HL.ACKPFP

Manuale d’istruzioni

TASTIERINO E LETTORE BIOMETRICO ANTIVANDALO
mono e/o bicanale, Standalone – Wiegand

Avvertenze importanti

Domotime Srl si riserva il diritto di apportare eventuali modifiche tecniche al prodotto senza preavviso; inoltre declina ogni responsabilità per danni a persone o cose dovuti a un uso improprio o a un'errata installazione del tastierino e lettore biometrico HL.ACKPFP.

Il presente manuale di istruzioni è destinato solamente a personale tecnico qualificato nel campo delle installazioni di automazioni.

Nessuna delle informazioni contenute all'interno di questo manuale è rivolta all'utilizzatore finale.

È consigliabile tenere un registro degli ID utenti aggiunti.

Per chiarimenti tecnici, o problemi di installazione, la ***Domotime Srl*** dispone di un servizio di assistenza clienti, che risponde al numero telefonico **+39 030 9913901**.

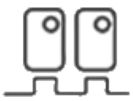
Presentazione del prodotto

Il tastierino e lettore biometrico HL.ACKPFP di DOMOTIME è un dispositivo di controllo degli accessi, ha un design semplice, operazioni facili e ha alta affidabilità.
Il circuito all'interno è resinato il che ne conferisce una totale resistenza all'acqua (IP 66).
Il dispositivo permette l'apertura o chiusura di un relè attraverso l'utilizzo di un codice PIN o il rilevamento di un'impronta digitale.
Consente di gestire fino a 3000 codici PIN o impronte digitali.

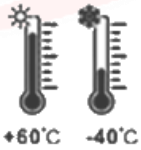
Di seguito alcuni esempi di campi in cui il lettore biometrico HL.ACKPFP può essere applicato:

1) Apertura cancello
2) Impianti di riscaldamento.
3) Attivazione o disattivazione impianto d'allarme.
4) Attivazione o disattivazione sistemi di supervisione e di monitoraggio.
5) Attivazione o disattivazione sistema di monitoraggio automatico.
6) Attivazione o disattivazione Distributori automatici.
7) Attivazione o disattivazione Stazioni di pompaggio.
8) Trasporti controllo alimentazione del veicolo.
9) Barche attivazione e disattivazione gruppo di alimentazione.
10) Attivazione o disattivazione valvole in genere esempio per oleodotti e gasdotti.
11) Automazione Industriale: Descrizione funzionamento vari.
12) Etc…

Uscita Standalone



Uscita Wiegand



Temperatura di esercizio

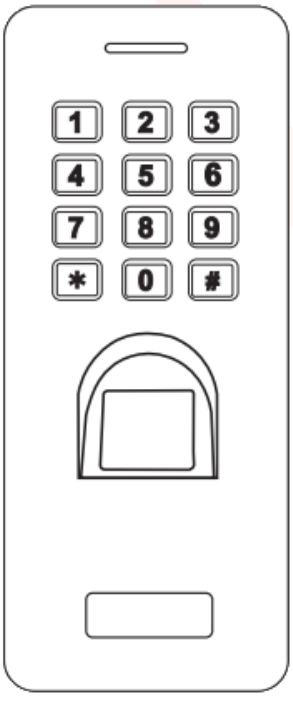
3000 Utenti

Grado di protezione

Dati tecnici

Alimentazione:	***12 Vdc ± 10%***	
Corrente assorbita:	***≤ 45 mA***	
Corrente di esercizio:	***≤ 150 mA***	
Risoluzione lettore d'impronte:	***500 DPI***	
Utenti registrabili:	***1000 Impronte digitali / 2000 codici PIN***	
Connessione cablaggio:	***Uscita relè (Standalone), Uscita Wiegand, Pulsante d'uscita, Allarme***	
Relè:	***Tempo chiusura relè:***	***Regolabile, da 1 a 99 secondi***
	Carico massimo output relè:	***2 Amp***
	Carico massimo output allarme:	***5 Amp***
Interfaccia Wiegand:	***26 bits output***	
Temperatura di esercizio:	***- 40° C / + 60° C***	
Umidità di esercizio:	***20% RH – 90% RH***	
Materiale:	***Lega di zinco***	
Grado di protezione IP:	***IP66***	
Dimensioni:	***137 x 58 x 26***	
Peso netto:	***400 g***	

Descrizione componenti



HL.ACKPFP

Diodo 1N4004 (per la protezione del relè)

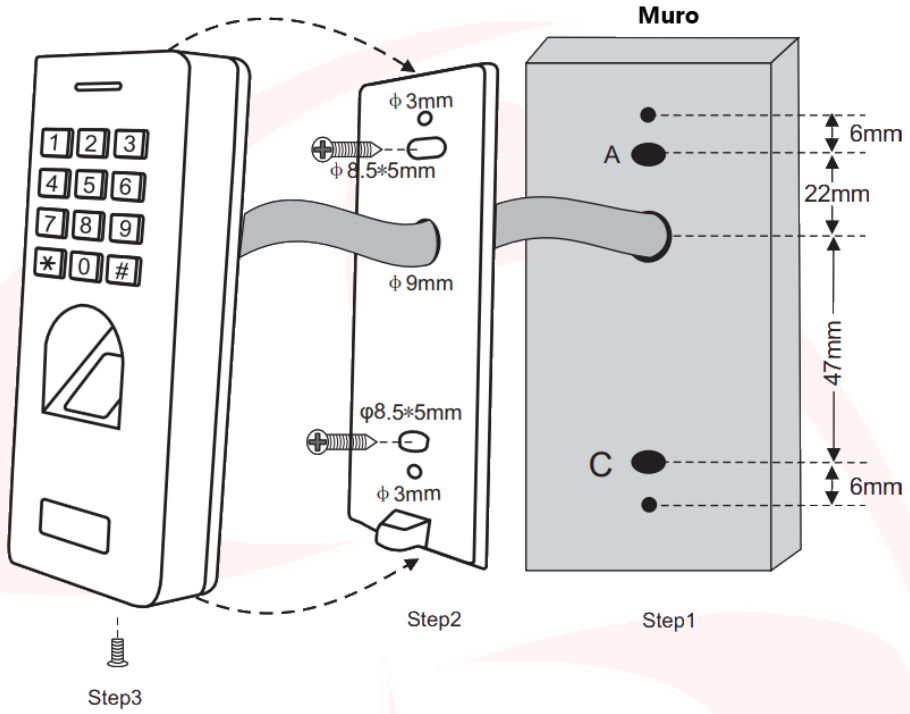
Fischer

Viti autofilettanti: Ø 4*25 mm

Cacciavite

Installazione

- Rimuovere la parte posteriore dell'unità
- Effettuare 2 fori (A, C) con il trapano per le viti
- Fissare saldamente il retro del lettore a muro con 2 viti a testa piatta
- Fissare il lettore sulla parte posteriore a muro.



Dettagli comunicazione

Il lettore biometrico HL.ACKPFP consente di comandare QUALSIASI DISPOSITIVO tramite i contatti puliti NO/NC, come ad esempio serrature, cancelli, pompe idrauliche, sistemi di sicurezza come allarmi, videosorveglianza o anti-intrusione, qualsiasi tipo di automazione, ecc., attraverso due tipi di comunicazione:

- **Standalone;**
- **Wiegand.**

La **modalità Standalone** permette al lettore biometrico di comandare QUALSIASI DISPOSITIVO attraverso i contatti NO/ NC e di utilizzare funzioni ausiliarie di comando e/o allarme direttamente dal dispositivo HL.ACKPFP (pagina 5).

La **modalità Wiegand** permette al HL.ACKPFP di commutare dei contatti NO/NC per comandare QUALSIASI DISPOSITIVO da remoto tramite una scheda di controllo.
Il lettore quindi non gestirà i contatti direttamente ma lo farà attraverso una scheda di decodifica garantendo affidabilità e sicurezza all'intero sistema: grazie alla comunicazione Wiegand una persona malintenzionata anche se dovesse manomettere il fingerprint esterno non riuscirebbe a comandare i contatti NO/NC e di conseguenza ad abilitare nessun dispositivo ad esso collegato (pagina 11).
Le schede per la decodifica di Domotime sono le seguenti:

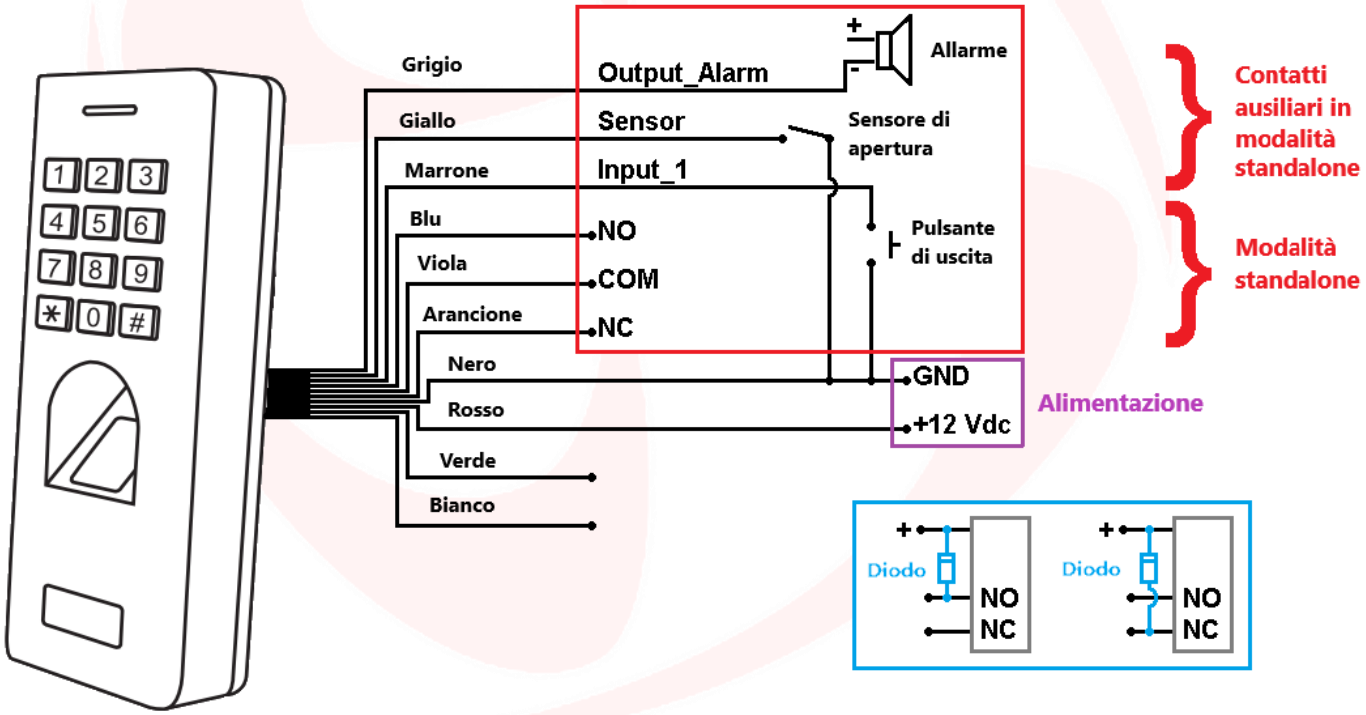
- HL.ACCB01: Scheda di decodifica con un uscita (MONOCANALE);
- HL.ACCB02: Scheda di decodifica con un uscita (MONOCANALE) – con Descrizione funzionamento Bluetooth;
- HL.ACCB03: Scheda di decodifica con due uscite (BICANALE) – con Descrizione funzionamento WiFi.

Modalità Standalone

La **modalità Standalone** permette al tastierino di comandare QUALSIASI DISPOSITIVO attraverso contatti puliti NO/ NC che ha a bordo e di utilizzare funzioni ausiliarie di comando e/o allarme direttamente dal dispositivo HL.ACKPFP.

Cablaggio

Colore cavo	Nome contatto	Funzione
Cablaggio modalità Standalone - Standard		
Rosso	+12 Vdc	12 Vdc – Polo positivo
Nero	GND	12 Vdc – Polo negativo
Blu	NO	Uscita relè – contatto normalmente aperto **(2 Amp max.)**
Viola	COM	Uscita relè – contatto comune **(2 Amp max.)**
Arancio	NC	Uscita relè – contatto normalmente chiuso **(2 Amp max.)**
Cablaggio modalità Standalone – Input e Output opzionali		
Giallo	Input_1	Pulsante per l'apertura/chiusura del relè
Grigio	Output_Alarm	Output - Polo negativo per allarme
Marrone	Sensor	Input - Sensore di apertura (normalmente chiuso)



ATTENZIONE:
Nella modalità **Standalone,** nel caso in cui l'alimentazione del nostro prodotto sia la medesima che va ad alimentare l'accessorio, sui contatti ausiliari di scambio si deve mettere il diodo, rappresentato in blu, fornito in dotazione.
Nella modalità **Standalone** non è obbligatorio collegare tutti i cavi del HL.ACKPFP, per esempio in assenza di bottone di uscita è possibile lasciare scollegato il cavo giallo ma non deve far contatto con gli altri cavi per evitare malfunzionamenti.

Programmazione

Informazioni generali di programmazione

Codice ID utente: ad ogni PIN di accesso o impronta digitale inserita viene associato un ID utente identificativo ed univoco.

L'ID utente può essere qualsiasi numero da 1 a 3000, da 1 a 1000 riservati alla gestione delle impronte digitali e da 1001 a 3000 riservati alla gestione dei PIN, eccetto i seguenti codici:

- Gli ID 999 e 1000 sono riservati alle impronte digitali autorizzatrici ovvero un utenza la cui impronta digitale permette di disabilitare/abilitare le altre utenze;
- Gli ID 2999 e 3000 sono riservati ai PIN autorizzatrici ovvero un utenza il cui PIN permette di disabilitare/abilitare le altre utenze;

Per poter modificare le impostazione del lettore biometrico è necessario accedere alla modalità programmazione, per poterlo fare è necessario essere a conoscenza del Master Code, un codice composto da 6 cifre che soltanto l'amministratore/installatore del dispositivo deve conoscere.

Valore Master Code predefinito: "123456". Si consiglia di modifcare il codice per una maggiore sicurezza.

Operazioni base

Modificare Master Code

Descrizione funzionamento	Combinazione tasti
Entrare nella modalità programmazione	* **(Digitare Master Code)** #
Modificare Master Code *(Master Code è qualsiasi numero composto da 6 cifre)*	0 **(Digitare Nuovo Master Code)** # **(Ripetere Nuovo Master Code)** #
Uscire dalla modalità programmazione	*

Aggiungere utenti

Aggiungere un codice PIN assegnandone un ID utente specifico

Descrizione funzionamento	Combinazione tasti
Entrare nella modalità programmazione	* **(Digitare Master Code)** #
Aggiungere un codice PIN assegnandone uno specifico ID utente. *ID Utente: qualsiasi numero da 1 a 1000* *Codice PIN: qualsiasi numero da 4 a 6 cifre*	1 **(Digitare ID utente)** # **(Digitare codice PIN)** #
Uscire dalla modalità programmazione	*

Aggiungere un'impronta digitale assegnandone un ID Utente specifico

Descrizione funzionamento	Combinazione tasti
Entrare nella modalità programmazione	* **(Digitare Master Code)** #
Aggiungere impronta digitale assegnandone uno specifico ID utente. *ID Utente: qualsiasi numero da 0 a 997*	1 **(Digitare ID utente)** # **(Appoggiare l'impronta digitale sul lettore) (Appoggiare l'impronta digitale sul lettore)**
Uscire dalla modalità programmazione	*

Aggiungere una o più impronte digitali utilizzando la "Master Add Fingerprint"

Descrizione funzionamento	Combinazione tasti
Entrare nella modalità programmazione	**Appoggiare l'impronta digitale "Master Add Fingerprint" sul lettore**
Aggiungere una o più impronte digitali	**Appoggiare l'impronta digitale da aggiungere sul lettore**
Uscire dalla modalità programmazione	**Appoggiare l'impronta digitale "Master Add Fingerprint" sul lettore**

Rimuovere utenti

Rimuovere un'impronta digitale o un codice PIN attraverso l'ID Utente

Descrizione funzionamento	Combinazione tasti
Entrare nella modalità programmazione	* **(Digitare Master Code)** #
Rimuovere un'impronta digitale o un codice PIN utilizzando l'ID utente	2 **(Digitare ID Utente)** #
Uscire dalla modalità programmazione	*

Rimuovere un'impronta digitale utilizzando l'impronta stessa

Descrizione funzionamento	Combinazione tasti
Entrare nella modalità programmazione	* **(Digitare Master Code)** #
Rimuovere un'impronta digitale utilizzando l'impronta stessa	2 **(Appoggiare l'impronta digitale sul lettore)** #
Uscire dalla modalità programmazione	*

Rimuovere una o più impronte digitali utilizzando la "Master Delete Fingerprint"

Descrizione funzionamento	Combinazione tasti
Entrare nella modalità programmazione	**Appoggiare l'impronta digitale "Master Delete Fingerprint" sul lettore**
Rimuovere una o più impronte digitali	**Appoggiare l'impronta digitale da rimuovere sul lettore**
Uscire dalla modalità programmazione	**Appoggiare l'impronta digitale "Master Delete Fingerprint" sul lettore**

Rimuovere tutti gli utenti

Descrizione funzionamento	Combinazione tasti
Entrare nella modalità programmazione	* **(Digitare Master Code)** #
Rimuovere tutti gli utenti	2 **(Digitare Master Code)** #
Uscire dalla modalità programmazione	*

Impostare modalità di apertura/chiusura relè

Questa funzione permette di impostare la modalità di accesso del dispositivo.
In particolar modo è possibile attivare/disattivare l'uscita collegata al lettore attraverso le seguenti opzioni:
Opzione 1) con la digitazione del SOLO codice PIN;
Opzione 2) con il rilevamento della SOLA impronta digitale;
Opzione 3) con il rilevamento dell'impronta digitale oppure con la digitazione del codice PIN *(Predefinito).*

Programmazione opzione 1)

Seleziona apertura/chiusura del relè con rilevamento SOLO codice PIN

Descrizione funzionamento	Combinazione tasti
Entrare nella modalità programmazione	* **(Digitare Master Code)** #
Selezionare apertura/chiusura del relè con digitazione SOLO codice PIN	4 0 #
Uscire dalla modalità programmazione	*

Utilizzo opzione 1)

Aprire/chiudere il relè con codice PIN

Aprire/chiudere il relè con carta/tag	**(Digitare codice PIN su HL.ACKPFP)** #

Programmazione opzione 2)
Selezionare apertura/chiusura del relè con rilevamento SOLO impronta digitale

Descrizione funzionamento	Combinazione tasti
Entrare nella modalità programmazione	* **(Digitare Master Code)** #
Selezionare apertura/chiusura del relè con rilevamento SOLA impronta digitale	4 1 #
Uscire dalla modalità programmazione	*

Utilizzo opzione 2)
Aprire/chiudere il relè con rilevamento impronta digitale

Aprire/chiudere il relè con impronta digitale	**(Appoggiare l'impronta sul lettore HL.ACKPFP)**

Programmazione opzione 3)
Selezionare apertura/chiusura del relè con rilevamento impronta digitale oppure con digitazione codice PIN

Descrizione funzionamento	Combinazione tasti
Entrare nella modalità programmazione	* **(Digitare Master Code)** #
Selezionare apertura/chiusura del relè con rilevamento impronta digitale oppure con digitazione codice PIN	4 2 #
Uscire dalla modalità programmazione	*

Utilizzo opzione 3)
Aprire/chiudere il relè con rilevamento impronta digitale o con codice PIN

Aprire/chiudere il relè con impronta digitale	**(Appoggiare l'impronta sul lettore HL.ACKPFP)**
Aprire/chiudere il relè con digitazione codice PIN	**(Digitare codice PIN)** #

Configurazione relè

Impostare modalità apertura relè: MONOSTABILE *(Predefinito)*

Descrizione funzionamento	Combinazione tasti
Entrare nella modalità programmazione	* **(Digitare Master Code)** #
Modalità monostabile *(Predefinito 5 secondi)* *Il tempo di apertura del relè può essere impostato da 1 a 99 secondi (1 = 50 mS)*	3 **(Digitare un numero da 1 a 99)** #
Uscire dalla modalità programmazione	*

Impostare modalità apertura relè: BISTABILE

Descrizione funzionamento	Combinazione tasti
Entrare nella modalità programmazione	* **(Digitare Master Code)** #
Modalità bistabile (*Impostare l'apertura/chiusura del relè in modalità ON/OFF)*	3 0 #
Uscire dalla modalità programmazione	*

Impostare modalità accecamento

La funzione “accecamento” si attiverà dopo 10 rilevazioni di utenti non abilitati, quindi di tentativi falliti. Questa funzione può essere impostata per negare l’accesso per 10 minuti ed essere disattivata solo dopo l’inserimento di un’impronta digitale o un codice PIN valido o il Master Code.

Accecamento: OFF *(Predefinito)*

Descrizione funzionamento	Combinazione tasti
Entrare nella modalità programmazione	* **(Digitare Master Code)** #
Accemento OFF (predefinito)	5 4 #
Uscire dalla modalità programmazione	*

Accemento: ON

Descrizione funzionamento	Combinazione tasti
Entrare nella modalità programmazione	* **(Digitare Master Code)** #
Accemento ON senza allarme *L’accesso sarà negato per 10 minuti a chiunque*	5 5 #
Uscire dalla modalità programmazione	*

Accecamento: ON con allarme

Descrizione funzionamento	Combinazione tasti
Entrare nella modalità programmazione	* **(Digitare Master Code)** #
Accemento ON con allarme *L’accesso sarà negato fino al rilevamento di un utente abilitato*	5 6 #
Uscire dalla modalità programmazione	*

Configurazione allarme

Allarme: ON *(Predefinito)*

Descrizione funzionamento	Combinazione tasti
Entrare nella modalità programmazione	* **(Digit Master Code)** #
Allarme ON *(Predefinito 1 minuto)* *Se la modalità accecamento è attiva, verrà attivato l’allarme quando ci saranno 10 tentativi errati, mentre se è disattivataverrà attivato solamente l’anti-tamper*	5 **(Digitare un numero da 1 a 3)** #
Uscire dalla modalità programmazione	*

Allarme: OFF

Descrizione funzionamento	Combinazione tasti
Entrare nella modalità programmazione	* **(Digit Master Code)** #
Allarme OFF *Attenzione: questa operazione disabiliterà la modalità accecamento con allarme*	5 0 #
Uscire dalla modalità programmazione	*

Apertura forzata porta aperta
Quando viene utilizzato con un contatto magnetico opzionale o un contatto magnetico incorporato nella serratura, se la porta viene aperta con la forza, il cicalino interno e l'allarme esterno (se presente) suoneranno entrambi. Possono essere arrestati da utenti abilitati, altrimenti continuerà a suonare per il tempo definito dall'allarme.

Imposta rilevamento apertura porta
Quando viene utilizzato con un contatto magnetico opzionale o un contatto magnetico incorporato della serratura, se la porta viene aperta normalmente, ma non chiusa dopo 1 minuto, il cicalino interno emetterà un segnale acustico automatico per ricordare alle persone di chiudere la porta. Il segnale acustico può essere interrotto chiudendo la porta o da utenti abilitati, altrimenti continuerà a suonare per il tempo definito dall'allarme.

Rilevamento apertura porta: OFF *(Predefinito)*

Descrizione funzionamento	Combinazione tasti
Entrare nella modalità programmazione	* **(Digit Master Code)** #
Disabilitare il rilevamento di apertura porta	6 0 #
Uscire dalla modalità programmazione	*

Rilevamento apertura porta: ON

Descrizione funzionamento	Combinazione tasti
Entrare nella modalità programmazione	* **(Digit Master Code)** #
Allarme OFF *Attenzione: questa operazione disabiliterà la modalità accecamento con allarme*	6 1 #
Uscire dalla modalità programmazione	*

Modalità Wiegand

La **modalità Wiegand** permette al tastierino di commutare dei contatti NO/NC per comandare QUALSIASI DISPOSITIVO da remoto tramite una scheda di decodifica.
Il lettore quindi non gestirà i contatti direttamente ma lo farà attraverso una scheda di decodifica garantendo affidabilità e sicurezza all'intero sistema: grazie alla comunicazione Wiegand una persona malintenzionata anche se dovesse manomettere il lettore biometrico esterno non riuscirebbe a comandare i contatti NO/NC e di conseguenza ad abilitare nessun dispositivo ad esso collegato.

Per poter utilizzare la modalità Wiegand del tastierino HL.ACKPFP è necessario collegarlo ad una scheda di decodifica remota.
Attenzione: Prima di poter aggiungere un utente sulla scheda di decodifica è necessario memorizzarlo sul lettore biometrico.

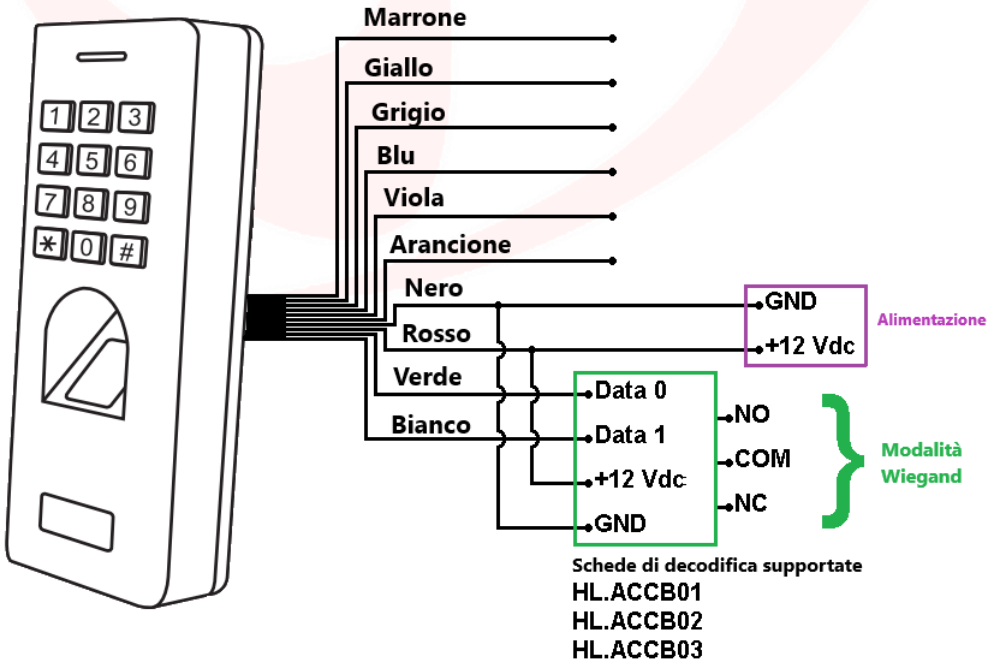
Scansiona il QR per le istruzioni di HL.ACCB01

Scansiona il QR per le istruzioni di HL.ACCB02

Scansiona il QR per le istruzioni di HL.ACCB03

Cablaggio modalità Wiegand

Colore cavo	Nome contatto	Funzione
Rosso	+12 Vdc	12 Vdc – Polo positivo
Nero	GND	12 Vdc – Polo negativo
Verde	Data 0	Uscita Wiegand – Data 0
Bianco	Data 1	Uscita Wiegand – Data 1



Aggiungere utenti

Aggiungere un codice PIN assegnandone un ID utente specifico

Descrizione funzionamento	Combinazione tasti
Entrare nella modalità programmazione	* **(Digitare Master Code)** #
Aggiungere un codice PIN assegnandone uno specifico ID utente. *ID Utente: qualsiasi numero da 1 a 1000* *Codice PIN: qualsiasi numero da 4 a 6 cifre*	1 **(Digitare ID utente)** # **(Digitare codice PIN)** #
Uscire dalla modalità programmazione	*

Aggiungere un'impronta digitale assegnandone un ID Utente specifico

Descrizione funzionamento	Combinazione tasti
Entrare nella modalità programmazione	* **(Digitare Master Code)** #
Aggiungere impronta digitale assegnandone uno specifico ID utente. *ID Utente: qualsiasi numero da 0 a 997*	1 **(Digitare ID utente)** # **(Appoggiare l'impronta digitale sul lettore) (Appoggiare l'impronta digitale sul lettore)**
Uscire dalla modalità programmazione	*

Aggiungere una o più impronte digitali utilizzando la "Master Add Fingerprint"

Descrizione funzionamento	Combinazione tasti
Entrare nella modalità programmazione	**Appoggiare l'impronta digitale "Master Add Fingerprint" sul lettore**
Aggiungere una o più impronte digitali	**Appoggiare l'impronta digitale da aggiungere sul lettore**
Uscire dalla modalità programmazione	**Appoggiare l'impronta digitale "Master Add Fingerprint" sul lettore**

Rimuovere utenti

Rimuovere un'impronta digitale o un codice PIN attraverso l'ID Utente

Descrizione funzionamento	Combinazione tasti
Entrare nella modalità programmazione	* **(Digitare Master Code)** #
Rimuovere un'impronta digitale o un codice PIN utilizzando l'ID utente	2 **(Digitare ID Utente)** #
Uscire dalla modalità programmazione	*

Rimuovere un'impronta digitale utilizzando l'impronta stessa

Descrizione funzionamento	Combinazione tasti
Entrare nella modalità programmazione	* **(Digitare Master Code)** #
Rimuovere un'impronta digitale utilizzando l'impronta stessa	2 **(Appoggiare l'impronta digitale sul lettore)** #
Uscire dalla modalità programmazione	*

Rimuovere una o più impronte digitali utilizzando la "Master Delete Fingerprint"

Descrizione funzionamento	Combinazione tasti
Entrare nella modalità programmazione	**Appoggiare l'impronta digitale "Master Delete Fingerprint" sul lettore**
Rimuovere una o più impronte digitali	**Appoggiare l'impronta digitale da rimuovere sul lettore**
Uscire dalla modalità programmazione	**Appoggiare l'impronta digitale "Master Delete Fingerprint" sul lettore**

Rimuovere tutti gli utenti

Descrizione funzionamento	Combinazione tasti
Entrare nella modalità programmazione	* **(Digitare Master Code)** #
Rimuovere tutti gli utenti	2 **(Digitare Master Code)** #
Uscire dalla modalità programmazione	*

Altre funzioni

Avvisi visivi e sonori

Il dispositivo è dotato di un LED e di un cicalino che permettono all'utente di ricevere avvisi visivi e sonori a seguito di ogni operazione.

Operazione	LED	Buzzer
Stand by	Luce rossa fissa	-
Entrare nella modalità programmazione	Luce rossa lampeggiante	1 beep
Dentro la modalità programmazione	Luce arancio fissa	1 beep
Operazione errata	-	3 beeps
Uscire dalla modalità programmazione	Luce rossa fissa	1 beep
Apertura/chiusura del relè	Luce rossa fissa	1 beep
Allarme	Luce rossa lampeggiante veloce	Beep continuo

Utenze autorizzatrici

Le impronte digitali i cui ID corrispondono a 999 e 1000 o le carte/tag i cui ID corrispondono a 2999 e 3000 possono inibire l'uso degli altri codici PIN o impronte digitali per attivare/disattivare l'uscita.
Una volta che il dispositivo legge un utenza autorizzatrice il led diventa rosso e lampeggia 4 volte.
Da quel momento le utenze valide sono disabilitate al controllo del dispositivo fino al momento in cui un'altra utenza autorizzatrice viene rilevata.
A quel punto il led verde lampeggerà 4 volte e tornerà alle normali funzioni.
Attenzione: Il bottone d'uscita potrà ugualmente attivare/disattivare l'uscita.

Ripristino delle funzioni di fabbrica e memorizzazione Master Cards

Attenzione: questa operazione riporterà le impostazioni a livello di fabbrica, non eliminirà le utenze già abilitate, per farlo è necessario eseguire la seguente operazione:

Rimuovere tutti gli utenti

Descrizione funzionamento	Combinazione tasti
Entrare nella modalità programmazione	* **(Digitare Master Code)** #
Rimuovere tutti gli utenti	2 **(Digitare Master Code)** #
Uscire dalla modalità programmazione	*

Attenzione: questa operazione eliminerà la "Master Add Card" e la "Master Delete Card".

Per ripristinare le funzioni di fabbrica è necessario togliere la tensione, premere il bottone di uscita e tenerlo premuto, accendere, attendere 2 beeps, dopodiché rilasciare il bottone, far leggere 2 impronte digitali:

- Alla impronta che il dispositivo leggerà verrà assegnato il ruolo di "*Master Add Fingerprint*", ovvero darà ad essa la possibilità di aggiungere altre impronte digitali.
- Alla seconda impronta che il dispositivo leggerà verrà assegnato il ruolo di "*Master Delete Fingerprint*", ovvero darà ad essa la possibilità di rimuovere impronte già abilitate.

Se non si desidera inserire impronte Master è necessario premere il bottone di uscita per almeno 10 secondi prima di rilasciarlo.

DECLARATION OF CONFORMITY

Domotime s.r.l.
Via Monico 9
25017 Lonato del Garda (BS) – ITALIA

DECLARE that the equipment described below:

Description:	Model:
Anti-vandalism fingerprint and keypad reader	HL.ACKPFP

Complies with the legislative regulations as in the following directives:

- EN 55022:2010+AC:2011
- EN 55024:2010+A1:2015

This statement is issued under the sole responsibility of the manufacturer and, if applicable, of his authorized representative.

DOMOTIME s.r.l.
Viale Michelangelo, 152/B
25010 DESENZANO D/G (BS)
C.f./P.I. n. Iscr. R.I. BS 02634[illegible]

Lonato, 19/02/2018

Via Monico, 9 25017 Lonato d/G (BS) – Italy - Tel: +39 030 9913901 - Fax: +39 030 2070611
Skype: domotime - email: info@domotime.com - www.domotime.com

HL.ACKPFP

User manual

ANTI-VANDALISM KEYPAD AND FINGERPRINT READER
single and / or dual channel, Standalone – Wiegand

Important warnings

Domotime Srl reserves the right to make any technical modifications to the product without prior notice; furthermore it declines all responsibility for damage to persons or things due to improper use or incorrect installation of the HL.ACKPFP keypad and fingerprint reader.

This instruction manual is intended only for qualified technical personnel in the field of automation installations.

None of the information contained in this manual is intended for the end user.

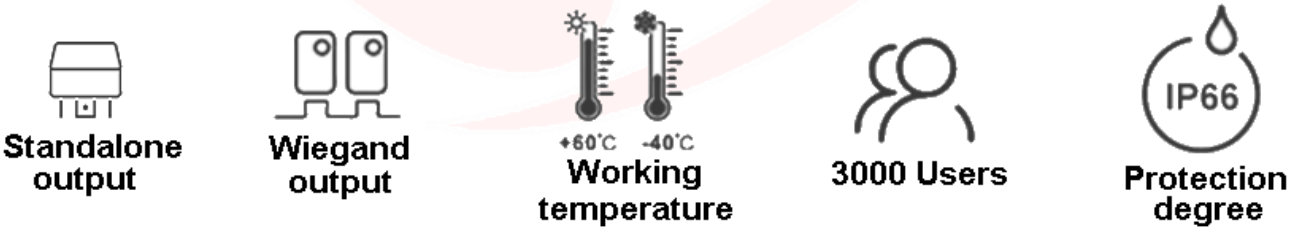
It is advisable to keep a record of added user IDs.

For technical clarifications or installation problems, ***Domotime Srl*** has a customer assistance service, which answers the phone number ***+39 030 9913901***.

Product overview

The DOMOTIME keypad and biometric reader HL.ACKPFP is an access control device, has a simple design, easy operations and high reliability.
The circuit inside is resined which gives it a total resistance to water (IP 66).
The device allows the opening or closing of a relay through the use of a PIN code or the detection of a fingerprint.
Manage up to 3000 PIN or fingerprint users.

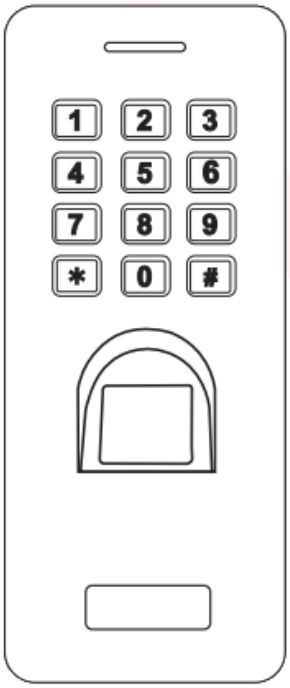
Here are some examples of fields in which the biometric reader HL.ACKPFP can be applied:
1) Gate open
2) Heating systems.
3) Activation or deactivation of the alarm system.
4) Activation or deactivation of supervision and monitoring systems.
5) Activation or deactivation of the automatic monitoring system.
6) Activation or deactivation of automatic dispensers.
7) Activation or deactivation of pumping stations.
8) Transport control of vehicle power supply.
9) Boats power supply activation and deactivation.
10) Activation or deactivation of valves in general, for example for oil and gas pipelines.
11) Industrial Automation: various commands.
12) Etc ...



Technical data

Power supply:	***12 Vdc ± 10%***	
Idle current:	***≤ 45 mA***	
Working current:	***≤ 150 mA***	
Fingeprint reader resolution:	***500 DPI***	
Users capacity:	***1000 fingerprints / 2000 keypad users***	
Wiring connections:	***Relay output, exit button, alarm, Wiegand output***	
Relay:	***Relay closing time:***	***Adjustable, from 1 to 99 seconds***
	Max load relay output:	***2 Amp***
	Max load alarm output:	***5 Amp***
Wiegand interface:	***26 bits output***	
Operating temperature:	***- 40° C / + 60° C***	
Operating humidity:	***20% RH – 90% RH***	
Material:	***Zinc-alloy***	
IP Protection rate:	***IP66***	
Dimensions:	***137 x 58 x 26***	
Net weight:	***400 g***	

Components description



HL.ACKPFP

Diode 1N4004 (For relay circuit protection)

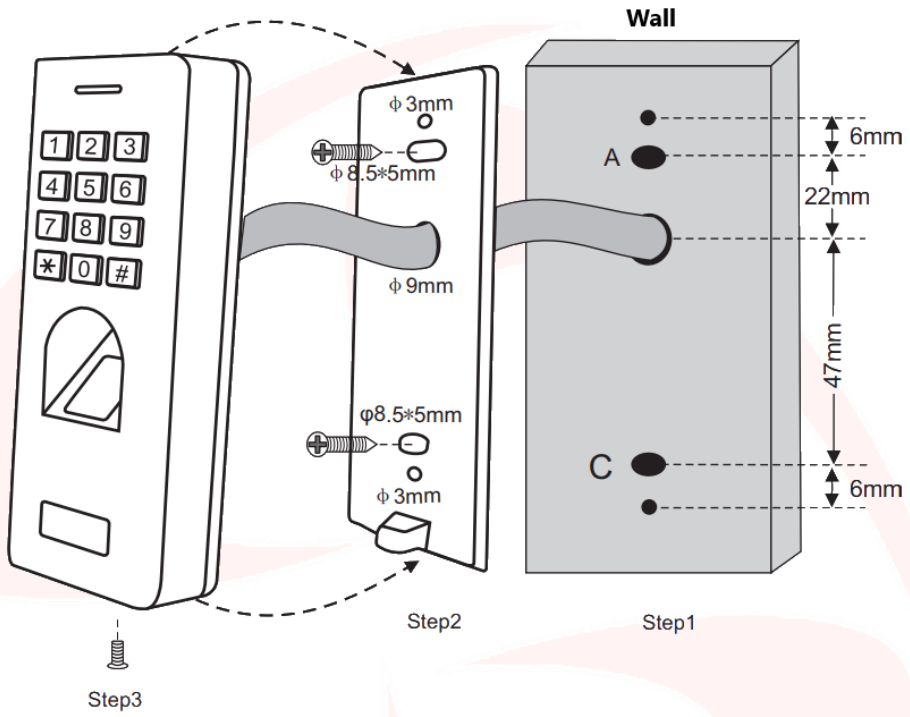
Fischer

Self Tapping Screws: Ø 4*25 mm

Screw Driver

Installation

- Remove the back cover from the unit;
- Drill 2 holes (A,C) on the wall for the screws and one hole for the cable;
- Fix the back cover firmly on the wall with 2 flat head screws (provided);
- Attach the unit to the back cover.



Communication details

The HL.ACKPFP reader allows you to control ANY DEVICE through one or more NO / NC dry contacts, such as locks, gates, hydraulic pumps, security systems such as alarms, video surveillance or anti-intrusion, any type of automation, etc. , through two types of communication:

- **Wiegand;**
- **Standalone.**

Standalone mode allows the device to command ANY DEVICE through the NO/NC contacts and to use auxiliary command and/or alarm functions directly from the HL.ACKPFP device (page 5).

Wiegand mode allows the HL.ACKPFP to switch NO/NC contacts to command ANY DEVICE.
The reader, however, will not manage the contacts directly but will do it through the decoding board ensuring reliability and security to the entire system: with the Wiegand communication a malicious person even if he tampers with the external fingerprint can not control the NO/NC contacts and consequently to enable any device connected to it (page 11).
The Domotime decoding cards are as follows:

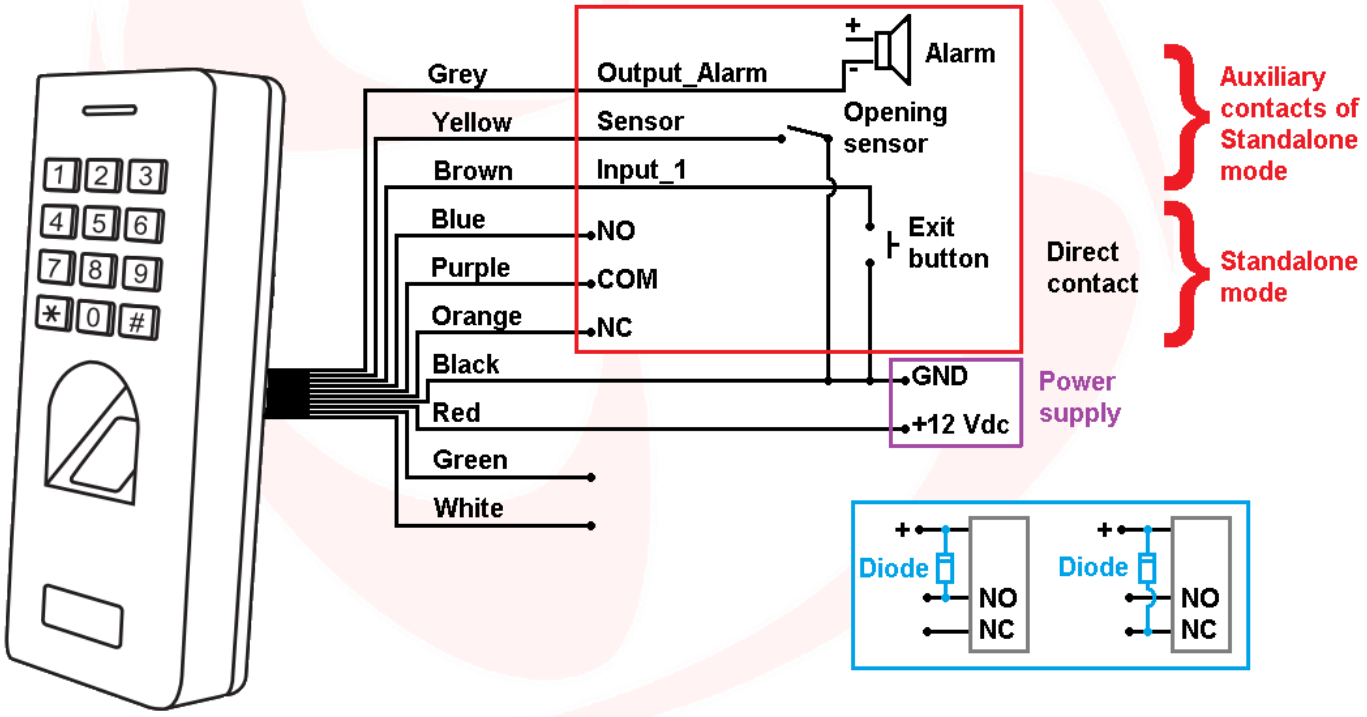
- HL.ACCB01: Decoding board with one output channel;
- HL.ACCB02: Decoding board with one output channel – Bluetooth control;
- HL.ACCB03: Decoding board with two outputs channel – WiFi control.

Standalone mode

Standalone mode allows the device to command ANY DEVICE through the NO/NC contacts and to use auxiliary command and/or alarm functions directly from the HL.ACKPFP device.

Connection diagram

Wire color	Contact name	Function
Standalone wirings – Standard		
Red	+12 Vdc	12 Vdc – Positive pole
Black	GND	12 Vdc– Negative pole
Blue	NO	Normally open relay output **(2 Amp max.)**
Purple	COM	Common connection for relay output **(2 Amp max.)**
Orange	NC	Normally closed relay output **(2 Amp max.)**
Standalone wirings – Optional Input and Output		
Yellow	Input_1	Button for opening / closing the relay
Grey	Output_Alarm	Output - negative pole for alarm
Brown	Sensor	Input - Opening sensor (normally closed)



WARNING:
In **Standalone** mode if the power supply of our product is the same that feeds the accessory on the exchange auxiliary contacts, you must put the diode marked in blue supplied.
In **Standalone** mode it isn't mandatory to connect all the cables of the HL.ACKPFP, for example in the absence of an exit button it is possible to leave the yellow cable disconnected but it must not make contact with the others to avoid malfunctions.

Programming

General programming information

User ID Number**:** it assigns an user ID number in order to keep track of the users of access PIN or fingerprints.
The user ID number can be any number from 1~3000. From 1 to 1000 reserved for fingerprints, from 1001 to 3000 reserved for PINs, with below exception:

- 999-1000 are reserved for the authorizer fingerprint that is an user whose fingerprint allows to disable / enable the other users.
- 2999-3000 are reserved for authorizer PIN that is an user whose PIN allows you to disable / enable the other users.

In order to be able to change the settings of the biometric reader, it is necessary to access the programming mode, to do so it is necessary to be aware of the Master Code, a 6-digit code that only the administrator / installer of the device must know.
Default Master Code value: "123456". We recommend modifying the code for greater security.

Basic setup

Changing Master Code

Programming Step	Keystroke Combination
Enter Setup Mode	* **(Digit Master Code)** #
Change Master Code *(Master Code is any 6-digit number)*	0 **（Digit New Master Code）** # **（Repeat New Master Code）** #
Exit Setup Mode	*

Add users

Add a PIN code by assigning a specific user ID

Programming Step	Keystroke Combination
Enter Setup Mode	* **(Digit Master Code)** #
Add a PIN code by assigning a specific user ID. *User ID: any number from 1 to 1000* *PIN code: any number from 4 to 6 digits*	1 **(Digit user ID)** # **(Digit PIN code)** #
Exit Setup Mode	*

Add a fingerprint by assigning a specific user ID

Programming Step	Keystroke Combination
Enter Setup Mode	* **(Digit Master Code)** #
Add fingerprint by assigning a specific user ID. *User ID: any number from 1 to 1000*	1 **(Digit user ID)** # **(Place the fingerprint on the reader) (Place the fingerprint on the reader)**
Exit Setup Mode	*

Add one or more fingerprints using the "Master Add Fingerprint"

Programming Step	Keystroke Combination
Enter Setup Mode	**Place the "Master Add Fingerprint" on the reader**
Add one or more fingerprints	**Place the fingerprint to be added on the reader**
Exit Setup Mode	**Place the "Master Add Fingerprint" on the reader**

Remove users

Remove a fingerprint or PIN code through the User ID

Programming Step	Keystroke Combination
Enter Setup Mode	* **(Digit Master Code)** #
Remove a fingerprint or PIN using the user ID	2 **(Digit user ID)** #
Exit Setup Mode	*

Remove a fingerprint using the fingerprint itself

Programming Step	Keystroke Combination
Enter Setup Mode	* **(Digit Master Code)** #
Remove a fingerprint using the fingerprint itself	2 **(Place the fingerprint on the reader)** #
Exit Setup Mode	*

Remove one or more fingerprint by "Master Delete Fingerprint"

Programming Step	Keystroke Combination
Enter Setup Mode	**Place the "Master Delete Fingerprint" on the reader**
Remove one or more fingerprints	**Place the fingerprint to be removed on the reader**
Exit Setup Mode	**Place the "Master Delete Fingerprint" on the reader**

Remove all users

Programming Step	Keystroke Combination
Enter Setup Mode	* **(Digit Master Code)** #
Remove all users	2 **(Digit Master Code)** #
Exit Setup Mode	*

Set open lock mode

This function allows you to set the device access mode.
In particular it is possible to activate / deactivate the output connected to the reader through the following options:
Option 1) by entering the ONLY PIN code;
Option 2) with ONLY fingerprint detection;
Option 3) with fingerprint detection or by entering a PIN code (*Default*).

Option 1 programming)

Select relay opening / closing with ONLY PIN code detection

Programming Step	Keystroke Combination
Enter Setup Mode	* **(Digit Master Code)** #
Select relay opening / closing with ONLY PIN code detection	4 0 #
Exit Setup Mode	*

Option 1 using)

Open / close relay with PIN code detection

Open / close relay with PIN code	**(Digit PIN code on HL.ACKPFP reader)** #

Option 2 programming)
Select relay opening / closing with ONLY fingerprint detection

Programming Step	Keystroke Combination
Enter Setup Mode	* **(Digit Master Code)** #
Select relay opening / closing with ONLY fingerprint detection	4 1 #
Exit Setup Mode	*

Option 2 using)
Open / close relay with fingerprint detection

Open / close relay with fingerprint	**(Place the fingerprint on the HL.ACKPFP reader)**

Option 3 programming)
Select relay opening / closing with fingerprint or PIN code detection *(Default)*

Programming Step	Keystroke Combination
Enter Setup Mode	* **(Digit Master Code)** #
Select relay opening / closing with fingerprint or PIN code detection	4 2 #
Exit Setup Mode	*

Option 3 using)
Open / close relay with fingerprint or PIN code detection

Open / close relay with fingerprint	**(Place the fingerprint on the HL.ACKPFP reader)**
Open / close relay with PIN code	**(Digit PIN code on HL.ACKPFP reader)** #

Relay configuration

Set relay output: MONOSTABLE mode *(Default)*

Programming Step	Keystroke Combination
Enter Setup Mode	* **(Digit Master Code)** #
Monostable mode *(Default 5 seconds)* *The relay opening time can be set from 1 to 99 seconds (1 = 50 mS)*	3 **(Digit a number from 1 to 99)** #
Exit Setup Mode	*

Set relay output: BISTABLE mode

Programming Step	Keystroke Combination
Enter Setup Mode	* **(Digit Master Code)** #
Bistable mode *(Set the relay opening / closing in ON / OFF mode)*	3 0 #
Exit Setup Mode	*

Set jamming mode

The “jamming alarm” will go off after 10 failed card attempts (factory default is OFF). It can be set to deny access for 10 minutes after wrong operation.
It can be put off after entering a valid fingerprint, PIN code or Master code.

Jamming mode: OFF *(Default)*

Programming Step	Keystroke Combination
Enter Setup Mode	* **(Digit Master Code)** #
Jamming mode OFF *(Default)*	5 4 #
Exit Setup Mode	*

Jamming mode: ON without alarm

Programming Step	Keystroke Combination
Enter Setup Mode	* **(Digit Master Code)** #
Jamming mode ON without alarm *Access will be denied for 10 minutes*	5 5 #
Exit Setup Mode	*

Jamming mode: ON with alarm

Programming Step	Keystroke Combination
Enter Setup Mode	* **(Digit Master Code)** #
Jamming mode ON with alarm *Enable alarm, need enter Valid PIN or Fingerprint to silence*	5 6 #
Exit Setup Mode	*

Alarm configuration

Alarm: ON *(Default)*

Programming Step	Keystroke Combination
Enter Setup Mode	* **(Digit Master Code)** #
Alarm ON (Default 1 minute) *If the Jamming mode is active, the alarm will be activated when there are 10 incorrect attempts, while if it is deactivated only the anti-tamper will be activated.*	5 **(Digit a number from 1 to 99)** #
Exit Setup Mode	*

Alarm: OFF

Programming Step	Keystroke Combination
Enter Setup Mode	* **(Digit Master Code)** #
Alarm OFF *Warning: this operation will disable the blinding with alarm mode*	5 0 #
Exit Setup Mode	*

Door Forced Open Detection

When use with an optional magnetic contact or built-in magnetic contact of the lock, if the door is opened by force, the inside buzzer and external alarm (if there is) will both operate, they can be stopped by master users or valid users, or else, it will continue to sound the same time with the alarm time set.

Set Door Open Detection

When use with an optional magnetic contact or built-in magnetic contact of the lock, if the door is opened normally, but not closed after 1 minute, the inside buzzer will beep automatically to remind people to close the door. The beep can be stopped by closing the door, master users or valid users, or else, it will continue to beep the same time with the alarm time set.

Set door open detection: OFF *(Default)*

Programming Step	Keystroke Combination
Enter Setup Mode	* **(Digit Master Code)** #
Disable door open detection	6 0 #
Exit Setup Mode	*

Set door open detection: ON

Programming Step	Keystroke Combination
Enter Setup Mode	* **(Digit Master Code)** #
Enable door open detection	6 1 #
Exit Setup Mode	*

Wiegand mode

Wiegand mode allows the HL.ACKPFP to switch NO/NC contacts to command ANY DEVICE.
The reader, however, will not manage the contacts directly but will do it through the decoding board ensuring reliability and security to the entire system: with the Wiegand communication a malicious person even if he tampers with the external fingerprint can not control the NO/NC contacts and consequently to enable any device connected.

In order to use the Wiegand mode of the HL.ACKPFP keypad it is necessary to connect it to a remote decoder board.
WARNING: Before being able to add a user to the decoder card, it must be stored on the biometric reader.

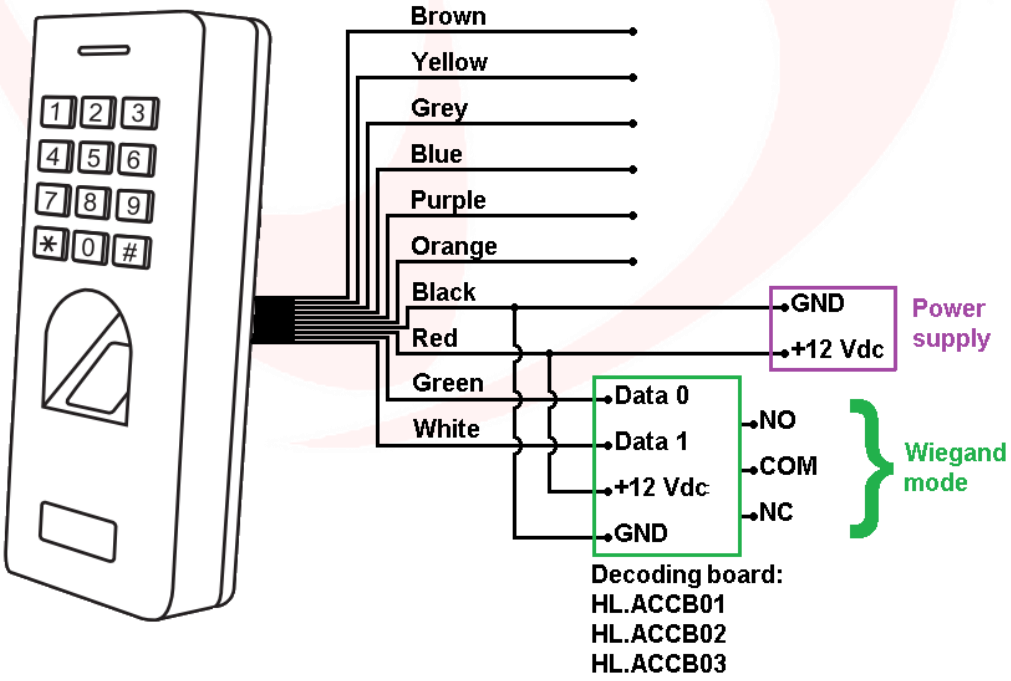
Scan the QR for the instructions of HL.ACCB01

Scan the QR for the instructions of HL.ACCB02

Scan the QR for the instructions of HL.ACCB03

Connection diagram

Wire color	Contact name	Function
Red	+12 Vdc	12 Vdc – Positive pole
Black	GND	12 Vdc – Negative pole
Green	Data 0	Wiegand output – Data 0
White	Data 1	Wiegand output – Data 1



Add users

Add a PIN code by assigning a specific user ID

Programming Step	Keystroke Combination
Enter Setup Mode	* (Digit Master Code) #
Add a PIN code by assigning a specific user ID. *User ID: any number from 1 to 1000* *PIN code: any number from 4 to 6 digits*	1 (Digit user ID) # (Digit PIN code) #
Exit Setup Mode	*

Add a fingerprint by assigning a specific user ID

Programming Step	Keystroke Combination
Enter Setup Mode	* (Digit Master Code) #
Add fingerprint by assigning a specific user ID. *User ID: any number from 1 to 1000*	1 (Digit user ID) # (Place the fingerprint on the reader) (Place the fingerprint on the reader)
Exit Setup Mode	*

Add one or more fingerprints using the "Master Add Fingerprint"

Programming Step	Keystroke Combination
Enter Setup Mode	Place the "Master Add Fingerprint" on the reader
Add one or more fingerprints	Place the fingerprint to be added on the reader
Exit Setup Mode	Place the "Master Add Fingerprint" on the reader

Remove users

Remove a fingerprint or PIN code through the User ID

Programming Step	Keystroke Combination
Enter Setup Mode	* (Digit Master Code) #
Remove a fingerprint or PIN using the user ID	2 (Digit user ID) #
Exit Setup Mode	*

Remove a fingerprint using the fingerprint itself

Programming Step	Keystroke Combination
Enter Setup Mode	* (Digit Master Code) #
Remove a fingerprint using the fingerprint itself	2 (Place the fingerprint on the reader) #
Exit Setup Mode	*

Rimuovere una o più impronte digitali utilizzando la “Master Delete Fingerprint”

Programming Step	Keystroke Combination
Enter Setup Mode	Place the "Master Delete Fingerprint" on the reader
Remove one or more fingerprints	Place the fingerprint to be removed on the reader
Exit Setup Mode	Place the "Master Delete Fingerprint" on the reader

Remove all users

Programming Step	Keystroke Combination
Enter Setup Mode	* (Digit Master Code) #
Remove all users	2 (Digit Master Code) #
Exit Setup Mode	*

Other functions

Sound and Light Indication

The device is equipped with an LED and a buzzer that allow the user to receive visual and audible warnings following each operation.

Operation Status	LED	Buzzer
Stand by	Red light bright	-
Enter into programming mode	Red light shines	One beep
In the programming mode	Orange light bright	One beep
Operation error	-	Three beeps
Exit from the programming mode	Red light bright	One beep
Open lock	Green light bright	One beep
Alarm	Red light shines quickly	Beep

Authorizer users

Fingerprints whose IDs correspond to 999 and 1000 or PIN codes whose IDs correspond to 2999 and 3000 can inhibit the use of other PIN codes or fingerprints to activate / deactivate the output.
Once the device reads an authorized user, the LED turns red and flashes 4 times.
From that moment the valid utilities are disabled to the control of the device until the moment in which another authorized user is detected.
At that point the green LED will flash 4 times and return to normal functions.
Warning: The exit button can also activate / deactivate the output.

Resetting to factory default & adding Master Cards

Warning: this operation will restore the factory settings, it will not eliminate the already enabled utilities, to do this it is necessary to perform the following operation:

Remove all users

Programming Step	Keystroke Combination
Enter Setup Mode	* **(Digit Master Code)** #
Remove all users	2 **(Digit Master Code)** #
Exit Setup Mode	*

To restore the factory functions it's necessary to switch off the voltage, press the exit button and hold it, switch on, wait for 2 beeps, then release the button and read as follows two different fingerprints:

- To the first fingerprint that the device will read twice, will be assigned the role of "*Master Add Fingerprint*", i.e. it will give to that fingerprint the possibility to add other fingerprints.
- The second fingerprint that the device will read twice, will be assigned the role of "*Master Delete Fingerprint*", i.e. it will give to that fingerprint the possibility to remove cards already enabled.

If you do not wish to insert Master cards, you must press the exit button for at least 10 seconds before releasing it.

Warning: this operation will restore the factory settings, it will not eliminate the already enabled users.
To eliminate all the users, the following operation must be performed:

DECLARATION OF CONFORMITY

Domotime s.r.l.
Via Monico 9
25017 Lonato del Garda (BS) – ITALIA

DECLARE that the equipment described below:

Description:	Model:
Anti-vandalism fingerprint and keypad reader	HL.ACKPFP

Complies with the legislative regulations as in the following directives:

- EN 55022:2010+AC:2011
- EN 55024:2010+A1:2015

This statement is issued under the sole responsibility of the manufacturer and, if applicable, of his authorized representative.

DOMOTIME s.r.l.
Viale Michelangelo, 152/B
25010 DESENZANO D/G (BS)
C.f./P.I. n. Iscr. R.I. BS 02634[illegible]

Lonato, 19/02/2018

Via Monico, 9 25017 Lonato d/G (BS) – Italy - Tel: +39 030 9913901 - Fax: +39 030 2070611
Skype: domotime - email: info@domotime.com - www.domotime.com