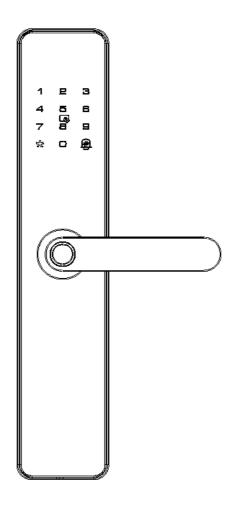
Semi-Automatic Smart door Lock User Manual

Handi Series

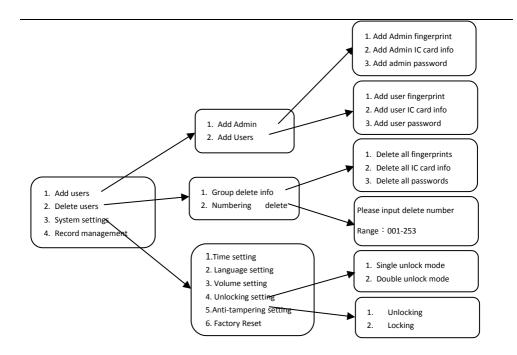
HD-103 (104,105,110) -A1



Smart Door Lock Basic Function

- 1. Three Unlocking Methods: Mifare-1 card, password, and fingerprint.
- 2. Touch Keypad with Voice Navigation: The system will automatically exit after 10 seconds if no operation is performed following activation.
- 3. Default Management Password: The factory/initialized/default administrator password is "123456". This password can be used to unlock the door.
- 4. User Identification: Each card, password, or fingerprint is assigned a unique 1 to 3-digit ID for easy individual deletion.
- 5. User Capacity: The system supports a total of 253 sets of unlocking credentials.
- Admin accounts: 5 sets (IDs 1–5)
- Regular user accounts: 248 sets (IDs 6–253)
- The combined total for cards, passwords, and fingerprints is 253 sets.
- 6. Decoy PIN Code Support: Random digits can be added before or after the valid password. Valid password length is 6–10 digits.
- 7. USB Charging Port: Equipped with a USB interface for emergency power supply.
- 8. Anti-Tampering Lockout: After 5 consecutive incorrect password, card, or fingerprint attempts, the system will lock the keypad for approximately 180 seconds.

Function Indication Diagram



Detailed Operation Instructions

- I. System Initialization
 - Remove the smart lock batteries.
 - 2. Press and hold the reset button on the back panel.
 - 3. Reinsert the batteries.
- 4. Wait for the 5-second system initialization countdown. A key tone will sound each second.
- 5. When the voice prompt says, "Restore factory settings, press the # key to confirm, press the * key to cancel," press the # key to enter the initialization process.
- 6. After a few seconds, when the voice prompt says "Initialization successful," the system reset is complete. All unlocking data is cleared. The system enters Demo Mode and proceeds to the startup process.

Note:

In Demo Mode, the default administrator password is "123456."

- Any Mifare-1 card can unlock the door.
- Any fingerprint can unlock the door.
- The default password "123456" can unlock the door.

★ After successful initialization, the lock must be reconfigured before use.

II. Adding an Administrator

1. If the lock is in sleep mode, touch any key (★ press and hold any number key for 0.5 seconds) to wake up the system. After the wake-up tone, press *+# to enter settings.

Voice Prompt: "Please enter the administrator password."

2. Enter correct administrator credentials (fingerprint, card, or password). In factory mode, enter "123456".

Voice Prompt:

- "Press 1 to add user"
- "Press 2 to delete user"
- "Press 3 for system settings"
- "Press 4 to check records"
- 3. Select 1 to enter the user addition menu.

Voice Prompt:

- "Press 1 to add administrator"
- "Press 2 to add normal user"
- 4. Select 1 to enter the administrator addition menu.

Voice Prompt:

- "Press 1 to add fingerprint"
- "Press 2 to add card"
- "Press 3 to add password"

(1) Administrator Fingerprint Setup:

- \bullet Press 1 \rightarrow Voice prompt: "Please place your finger, lift and place again."
 - After 5 scans, fingerprint registration is successful.

(2) Administrator Card Setup:

 Press 2 → Voice prompt: "Please swipe card." Hold the card near the sensor area → Voice prompt: "Setup successful."

(3) Administrator Password Setup:

• Press 3 \rightarrow Voice prompt: "Enter new password ******, press # to confirm" \rightarrow Re-enter password, press # \rightarrow Voice prompt: "Setup successful."

III. Adding a Normal User

1. Wake up the system by touching any key. After the wake-up tone, press *+#.

Voice Prompt: "Please enter the administrator password."

2. Enter correct administrator credentials or default password "123456".

Voice Prompt: Same as above

3. Select $1 \rightarrow$ Then select 2 to add a normal user.

Voice Prompt:

- "Press 1 to add fingerprint"
- "Press 2 to add card"
- "Press 3 to add password"

(1) Fingerprint Setup:

Same process as for administrator.

(2) Card Setup:

Same process as for administrator.

(3) Password Setup:

Same process as for administrator.

IV. Deleting Users by Group

- 1. Wake up system \rightarrow Press *+# \rightarrow Enter administrator credentials.
- 2. Voice prompt menu as before \rightarrow Press 2 to enter deletion menu.
- 3. Voice Prompt:
- "Press 1 for group delete"
- "Press 2 for delete by number"
- 4. Select 1 for group deletion (only non-administrators can be deleted this way).

Voice Prompt:

- "Press 1 to clear non-admin fingerprints"
- "Press 2 to clear non-admin cards"
- "Press 3 to clear non-admin passwords"
- 5. Confirm deletion:

Voice Prompt: "Press # to confirm, * to cancel" \rightarrow System: "Deletion successful"

V. Deleting by ID Number (Admin/User)

- 1. Wake up system \rightarrow Press *+# \rightarrow Enter admin credentials.
- 2. Press 2 for deletion menu \rightarrow Select 2 for delete by number.

Voice Prompt: "Enter ID number (001-253)" \rightarrow Press # to confirm.

Note: The admin currently accessing system settings cannot delete their own ID.

- VI. System Settings
- (1) Time Setting
- → Select 3 (System Settings)

Voice Prompt: "Press 1 for time settings..."

- → Enter year, month, day, hour, minute → "Setup successful"
- (2) Language Setting

→ Press 2

Voice Prompt: "Press 1 for Chinese, 2 for English"

- (3) Volume Setting
- → Press 3

Voice Prompt: "Press 2 to increase, 8 to decrease, # to confirm, * to exit"

- (4) Unlock Mode Setting
- → Press 4

Voice Prompt:

- "Press 1 for single unlock mode"
- "Press 2 for dual unlock mode"

In dual mode, two different user credentials are needed. Not applicable to admins.

- (5) Tamper Alarm Setting
- → Press 5

Voice Prompt: "Press 1 to enable, 2 to disable"

- (6) Restore Factory Settings
- → Press 6

Voice Prompt: "Press # to confirm, * to cancel"

→ "System initializing, please wait" → Wait for completion

VII. Access Record Inquiry

- 1. Wake up system \rightarrow *+# \rightarrow Enter admin credentials
- 2. Press 4 to access record log

Voice Prompt: "Press 2 for next, 8 for previous, * to exit"

VIII. Doorbell

Press the doorbell button in either verification or sleep mode \rightarrow Doorbell will chime twice.

IX. Low Battery Alarm

- 1. When battery is low, the system will say: "Battery power is low" after unlocking.
- 2. Backup Power: External USB power source can be connected for emergency use.

X. Lockdown Alarm

If incorrect unlock info is entered more than 5 times within 5 minutes, the system locks for 180 seconds.

XI. Tamper Alarm

If tamper button is triggered, a 30-second alarm sounds. Only valid unlock credentials can stop it.

XII. Battery Safety Instructions

- 1. Insert four AA smart lock-compatible 1.5V batteries into the back panel.
 - 2. For frequent use, replace batteries every 6–8 months.
 - 3. Use only manufacturer-approved batteries.
- 4. Do not expose batteries to high heat (sunlight, fire, microwave, oven).
 - 5. Do not disassemble, strike, crush, or cut batteries.
 - 6. Avoid low-pressure environments (may cause explosion/leak).
 - 7. Stop using swollen batteries.
 - 8. Do not swallow batteries—may cause chemical burns.
 - 9. If swallowed or inserted in the body, seek immediate medical help.
- 10. If battery compartment is not securely closed, keep the product away from children.
 - 11. Keep batteries (new or used) away from children.
- 12. Do not dispose of batteries in household waste—follow local disposal laws.
- 13. This product contains button batteries. Ingestion may cause severe internal burns or death within 2 hours.
 - 14. Use alkaline batteries. Do not mix brands or old/new batteries.

★ Special Reminder:

Each lock includes two emergency mechanical keys. Always store them outside the door in a secure location. If the key is locked inside, the manufacturer is not responsible.

User Safety Guidelines:

- 1. Before using the product, change the factory default admin password "123456."
- 2. It's recommended to set multiple admin fingerprints and one admin password.
 - 3. Emergency key must be hidden outside for backup use. If locked

inside, the company holds no responsibility.

4. Keep IC cards secure. Prevent loss or duplication.

Please read this manual carefully before installation and use!