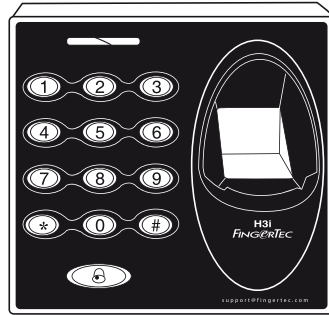# FINGERTEC
www.fingertec.com

H3i
Stand-alone Fingerprint &
Card Access Control System

User Guide

This guide serves as an important document for consumers to operate H3i. Keep this guide intact for your future reference.

For any problems, kindly contact **support@fingertec.com** for assistance.

IMPORTANT

VERIFY YOUR ADMIN PASSWORD
Default Password: 1234
Operation: Press * > LED goes off > Buzzer emits long beep > Press # > Insert the Admin password > Green LED blinks > Buzzer emits long beep again > Admin password verified successfully

Note: The admin password must be inserted before the start of any operation in H3i.

CHANGING ADMIN PASSWORD
It's recommended that you change the default Admin password to your very own 4-digit unique password. If you want to use less than 4 digits, hash (#) symbol is permitted. I.e.: 123 will be keyed in as 123#.

Operation: Verify default Admin password > Press 8 > Insert new Admin password > Repeat new Admin password > Green LED blinks > Buzzer emits long beep > Admin password changed successfully

ENROLLMENT

H3i assigns user IDs automatically. It ranges from 1 to 65534. Record the details of enrollment using a form for future reference. Enroll fingerprints and cards as desired.

ENROLLING FINGERPRINTS
Operation: Verify your Admin password > Press 1 > Scan finger 3 times > Green LED blinks > Buzzer emits long beep > Continue to enroll another fingerprint > Press * to end process

ENROLLING CARDS
Operation: Verify your Admin password > Press 1 > Wave card once > Green LED blinks > Buzzer emits long beep > Continue to enroll another card > Press * to end process
Note: H3i will blink its red LED and it'll beep twice if the fingerprint or card data had already been enrolled before or you registered a bad fingerprint. Ensure the fingerprint quality before enrollment.

ENROLLING A BATCH OF CARDS
Operation: Verify your Admin password > Press 6 > Wave the 1st card once > Insert the total number of cards (i.e. 50) > Press # if the total number is less than 3-digits for example 81#, 99# > Green LED blinks > Buzzer emits long beep > Press * to end process
Note: All cards must have running card number in sequence.

SETTING PASSWORDS
H3i supports 8 sets of passwords. Any of the predefined passwords can unlock the device. Get ready with the passwords before you register them in H3i.

For **example:**

SET	PASSWORD
1	2331
2	4563

ENROLLING PASSWORDS
Operation: Verify your Admin password > Press 3 > Green LED blinks > Buzzer emits long beep > Press the number of password(s) set, e.g. 1 > Insert the password > Insert the same password again > Green LED blinks > Buzzer emits long beep again > Press * to end process

*Note: If you want to continue enrolling more passwords, do not press *, which will end the process. Instead, continue by inserting the new set number and its new password. Maximum set of passwords allowed is 8. Press # to fill in the gap if your chosen password is less than 4-digits. I.e.: 123 will be keyed in as 123#.*

DELETING USER INFO ✖

DELETING USER ID

Operation: Verify your Admin password > Press 2 > Green LED blinks > Buzzer emits long beep > Insert the user ID for deletion > Press # if the ID is less than 5-digits > Buzzer emits long beep again > Press * to end process

*Note: You can delete more users by inserting their user ID after the long beep. Only press * after you have finished deleting the users you want. In case the red LED blinks after you've inserted the user ID, that particular ID is not available in H3i.*

DELETING FINGERPRINT

Verify your Admin password > Press 2 > Green LED blinks > Buzzer emits short beep > Place the enrolled fingerprint on scanner > Buzzer emits long beep again > Press * to end process

DELETING CARDS

Operation: Verify your Admin password > Press 2 > Green LED blinks > Buzzer emits long beep > Wave the enrolled card at the induction area > Buzzer emits long beep again > Press * to end process

DELETING PASSWORDS

Operation: Verify your Admin password > Press 3 > Green LED blinks > Buzzer emits long beep > Insert the set number, for example 2 > Insert 0000 > Insert 0000 one more time > Green LED blinks > Buzzer emits long beep again > Press * to end process

*Note: Only press * after you've finished deleting the fingerprint, card or password data. In case the red LED blinks after you've inserted one of the data, that particular user data is not available in H3i.*

DELETING DEVICE INFORMATION

Operation: Verify your Admin password > Press 9 > Green LED blinks > Buzzer emits long beep > Press 9 again > Green LED blinks > Red LED blinks Buzzer emits one beep

Note: This deletion will not affect the passwords stored in H3i. The password(s) must be deleted one by one.

OTHER OPERATIONS ❓

RESET TO DEFAULT FACTORY SETTINGS

You can reset the device back to its default factory settings (including the default admin password, 1234).

Operation: Dismantle device > Look for the tamper switch at the back of device > Wait for 30s > Buzzer emits long beep > Press and release the tamper switch 3 times > Install the device back to its position > Press the RESTART button (at the bottom of device)
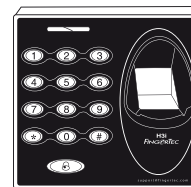
UNLOCK DOOR ADMIN PASSWORD

On top of using the admin password as a key to start any operation, you can also use the admin password to unlock doors.

Operation: Verify your Admin password > Press 0 > Green LED blinks > Buzzer emits long beep > Press 0 > Green LED blinks > Buzzer emits long beep > Door unlocked successfully

ENABLE/DISABLE LED BLINKS DURING IDLE MODE

The LED on H3i will blink during verification. However, you can disable the LED blinks of the device during other operations.

Operation: Verify your Admin password > Press 0 > Green LED blinks > Buzzer emits long beep > Press 3 > Press 0 (to disable) or 1 (to enable) > Green LED blinks > Buzzer emits long beep > Changes done successfully

FINGERTEC
www.fingertec.com

H3i
Stand-alone Fingerprint & Card Access Control System

Fingerprint Password Card

SPECIFICATIONS	
MODEL	H3i
SURFACE FINISHING	Acrylonitrile Butadiene Styrene (ABS)
TYPE OF SCANNER	Non-coated optical scanner
MICROPROCESSOR	400 MHz
MEMORY	32MB flash memory
ALGORITHM	BioBridge VX 10.0
PRODUCT DIMENSION (L X W X H), mm	88 x 25 x 88
STORAGE	
• Fingerprint template	200
• Cards	500
• Passwords	8 sets (max length 4-digits per password)
ENROLLMENT & VERIFICATION	
• Methods	Fingerprint (1:N), card & password
• Recommended fingerprint per user ID	1
• Fingerprint placement	Any angles
• Password length (digits)	Max 4
• Verification time (sec)	< 1
• FAR (%)	< 0.0001
• FRR (%)	< 1
CARD TECHNOLOGY	
• RFID: 64-bit, 125kHz	Yes
• MIFARE: MFIS50/S70, 13.56MHz	Made to order
OPERATING ENVIRONMENT	
• Temperature (°C)	0 ~ 45
• Humidity (%)	20 ~ 80
• Power input	DC 12V 3A
ACCESS CONTROL	
• EM lock driving output	12VDC / relay output
• Alarm output	NO only
• Door sensor	Yes (NO/NC)
GROUP VERIFY TYPE	
• Password only	Yes
• Card only	Yes
• Fingerprint only	Yes
• Fingerprint/card/password	Yes
• Card and password	Yes
• Fingerprint and password	Yes

*NOTE: Specifications are subject to change. Check **http://product.fingertec.com** for latest product information.*