FINGERTEC

Face ID 5/TD Face ID 5

Face ID 5 Series

User Guide

Contents

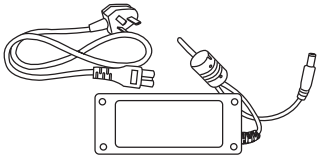
Chapter 1
Getting Started

Viewing the User Guide in the Internet

The User Guide is available in the package when you purchased the terminal. The User Guide is also available online at http://www.fingertec.com and http://user.fingertec.com. Choose the language that you prefer for your User Guide.

Terminal Included Accessories

Do not abuse the fingerprint sensor by scratching the surface, contacting the sensor's surface with heat, pressing hard during placement of fingerprint for verification. Clean the sensor occasionally with microfiber cloth to maintain the performance of the sensor.

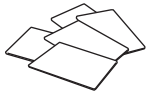


DC 12V Power Adapter

Connection Wires

Screwdriver

A Packet of Bolts



**RFID Cards (5 pieces)*

ITEM	FUNCTION
DC 12V Power Adapter	*Connect the power adapter to terminal and plug it into a standard power outlet to charge terminal*
Connection Wires	*Connect the wires to door lock, doorbell and RS485, if required*
Screwdriver	*Use the screwdriver to open the back plate of fingerprint terminal and to install the back plate against a wall*
A Packet of Bolts RFID	*Use the screws to hold the back plate of the terminal against a wall*
Cards (5 pieces)	*For card enrollment and verification * Only for Face ID 5*

Activating Terminal

Every FingerTec access control model comes bundled with a unique license key. To start using the terminal with Ingress, you must connect the terminal to Ingress and perform online activation. Ingress reads the serial number of your terminal and sends it for verification at the FingerTec server via Internet.

In case you do not have an Internet connection, you would need to do offline activation. Please send the serial number and models of your terminals to your local resellers or *support@fingertec.com* to request for a product key and activation key.

Registering Terminal

Make sure that you register your terminal's warranty with us at *http://www.fingertec.com/ver2/english/e_warranty.htm*.
for a 36 month warranty protection.

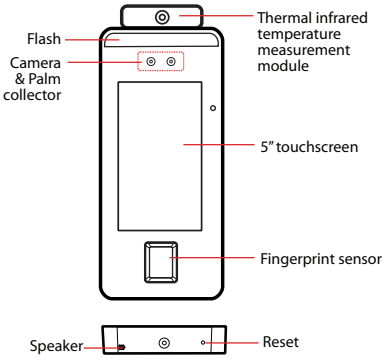
Chapter 2
Basics

Introduction to Terminal

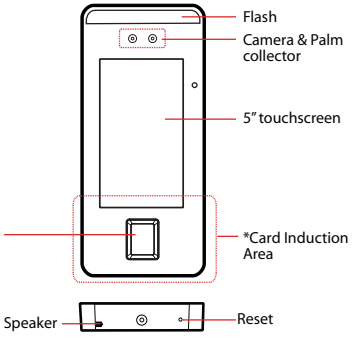
Introducing terminal, the latest biometrics product, face recognition technology product combined with fingerprint technology. Terminal can identify an identity in split seconds without any contact or hassle. Terminal only requires user to look at the machine to get verification. Terminal is loaded with powerful microprocessor that can process dual biometrics authentication methods for accurate personal identifications and for collection of precise data for time attendance and door access. In addition, the terminal accepts card verification as an added security measure. If you are looking for contactless, hassle free biometrics product, choose terminal. With one look you are good to go!

Terminal Overview

- **Face ID 5/TD**

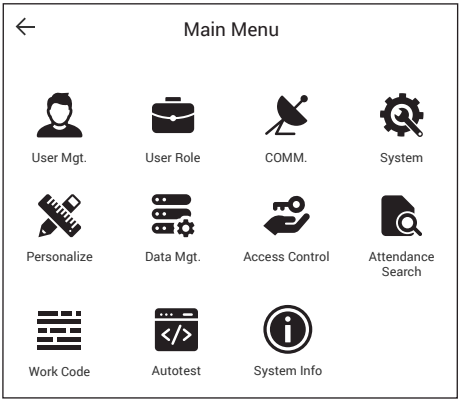


- **Face ID 5**



ITEM	FUNCTION
Thermal infrared temperature measurement module	*Infrared Temperature Measurementxxx*
Flash	*To facilitate the face recognition process in a dark environment*
Camera & Palm Collector	*Capture face images in few directions.*
5" Touchscreen	*Touch this screen to access into terminal system and do configuration.*
Fingerprint Sensor	*To scan finger for confirmation of identity.*
****Card Induction Area***	*Area that reads RFID cards. (Only for Face ID 5 model)*
Speaker	*For terminal voice emission.*
Reset Button	*To restart the terminal as and when required.*

Main Menu



User Mgt
Enroll users/ manage user data.

User Role
Assign privilege to users for data security.

COMM.
Setup FingerTec terminal communication with computer through LAN, RS232 and RS485. Set security password of the device for a secure data transfer.

System
Configure the settings of the FingerTec terminals from general to display setting to fingerprint, and reset the terminal to default settings.

Personalize
Adjust the date/time, Voice, bell schedules settings of the terminal.

Data Mgt
To delete/backup or restore data.

Access Control
Configure door access settings in terminal.

Attendance Search
Check attendance and transaction logs that are available in FingerTec terminals and perform housekeeping in the machine.

Work Code
Create & manage workcode functionality.

Autotest
Tests that can be done on the FingerTec terminal on various aspects.

System Info
View data capacity, device and firmware information.

Power On/Off Button

Use the power on/off button to turn the terminal on or off. You can disable the button to avoid accidental shut off of the terminal.

Battery

Terminals operate using power supply from a standard power outlet. Inside the terminal, there is an RTC battery for the running of the clock. Charge the terminal for at least 3 hours straight before you start using it. When there is a serious delay in time or the clock keeps on restarting, the RTC needs to be replaced.

Internal battery

The internal battery is provided as a separate accessory and it can last up to 5 hours. Refer to the battery icon on the terminal LCD for the status of the remaining power. Charge when necessary.

External power supply

Mini UPS (uninterrupted power supply) 5V and mini UPS 12V provide mobile power supply to the terminals. Charge the mini UPS sufficiently for optimum performance.
Refer to *http://accessory.fingertec.com* for more information about accessories.

Cleaning Terminal

Cleaning The Body

Use a dry cloth to clean the terminal's body. Do not use any liquids, household cleaners, aerosol spray, solvents, alcohol, ammonia and abrasive solutions to clean the body of the terminal because it could damage it.

Cleaning the Fingerprint Prism

Clean the fingerprint prism with a cellophane tape for (silicon coated prism).
View the video on how to clean the fingerprint prism at this link
http://www.fingertec.com/newsletter/enduser/cleanfinger.html.
For the non-coated prism, please use microfiber cloth.

Restarting and Resetting Terminal

If a feature isn't functioning as it should, try restarting or resetting the terminals

Restarting the Terminal

Push the On/Off button on the terminal to restart the terminal. If you can't restart the terminal, or if the problem persists, you might want to reset.

Resetting the Terminal

Resetting the terminal will cause all your settings to return to the original factory settings.

Chapter 3
Users

Introduction

FingerTec devices recognize users by face recognition, fingerprint, card access or a set of pin numbers. The Date, Time Data and User ID will be stored in its internal storage upon verification and will be used to generate reports in accordance with the user's attendance.

Privileges can be assigned accordingly based on individual permissions. Likewise, a System Administrator can have his rights restricted or be given full control. Access controls such as the ability to modify settings within the menu will be barred when a System Administrator has been assigned to a device. The role of an administrator plays a crucial role in the vitality of the data in these devices.

For example, Network Administrator(s) can be allowed to configure communication settings but not to enroll new users.

Three levels of authority govern each device:

- Super Administrator
  The top of the hierarchy, Super Administrators have, full access to all functions.
- Administrator
  The rights of an Administrator are limited by the permissions granted by the Super Administrator. For example, a Network Administrator can be allowed to configure communication settings but are not allowed to enroll users.
- User
  Normal users have no access to any functions within the device.

By default, every user enrolled is a normal user. Super Admin and Administrator roles are allocated from the list of normal users, either directly from the terminal or assigned via our software.

Voice Message

VOICE / MESSAGE	WHAT DOES IT MEAN?
"Verified"	*Identity verification is successful, the terminal stores the transaction logs and opens the door (if connected to door access)*
"Try again please"	*Identity verification is failed because the finger is not properly positioned, the template is not available in the terminal or the password is incorrect.*
"Admin Affirm"	*You are not an administrator of the system and you cannot access Menu page.*
"Duplicate Finger"	*This message only appears during registration when the finger that you want to enroll has been enrolled before. "FP Enrolled AIrd" will be displayed on the LCD screen.*
"Invalid ID"	*For 1:1 verification, User ID entered does not match with fingerprint.*

Methods of Enrollment

Fingerprint Enrollment

Please assign an enrollee as a Super Admin before you proceed to enroll any other credentials, as the menu options are only available to a Super Administrator.

It is recommended that all users enroll two fingerprints for each user ID. The first fingerprint will serve as a template for primary access where the other fingerprint will be used as a backup in the rare event that your first fingerprint is unreadable.

VERIFICATION METHOD	PROCESS
1:1 (One to One)	*You have to identify your User ID before inputting any biometrics feature for verification. For example, your user ID is 1008. One to one method requires you to key in user ID followed by your fingerprint to get verified.*
1:N (One to Many)	*You don't need to identify your User ID before inputting any biometrics feature for verification. Simply place your finger on the scanner for verification.*

1:N – Place your finger properly on the scanner and the terminal will verify your identity.
1:1 – 1:1 requires input of User ID before the terminal reads and verifies your identity.
Some precautions have to be taken to get a good read every time.

Users may attempt to verify their identities with 1:1 verification mode when they fail to gain access with 1:N authentication method.

- Make sure the center point of your finger is placed in the middle of the scanner for a good read.
- Recommended to use index finger. The terminal accepts other fingers but index is the most convenient.
- Make sure the finger is not wet, too dry, injured or dirty.
- Do not press hard on the sensor, just place it comfortably
- Avoid direct sunlight or bright light.

Center point

Prior to enrolling your fingerprint, please choose the fingers that will be used to enroll into the device. We recommend using both index fingers as opposed to your thumbs as their size may differ between individuals, which may not fit wholly on the scanner.

Follow the steps below to enroll a fingerprint:

- **Step 1:** Press Menu > User Mgt > New User
- **Step 2:** User ID > Key in User ID
  This is the unique ID number that represents the user in the devices and software. Make sure you do not use duplicated ID. The maximum length is 9-digits
- **Step 3:** Select Fingerprint > Press the corresponding number to select which finger(s) to enroll from the on screen image.
- **Step 4:** Press OK to start enrolling the fingerprint > Place your finger on the scanner 3 times > Screen will display the quality of image captured > Press OK to save > Press ESC to return to the main page
- **Step 5:** Press User Role > Select Role > Select Normal User > Press OK to save
  Select Super Admin or other defined role(s) you wish to assign to this user.

Refer to page 15 User Role for more details. Repeat Steps 3 and 4 to enroll the 2nd backup fingerprint.

Face Enrollment

During enrolment on terminal, please stand straight and do not move your face or body, and make sure that your face is calm with no extreme expression. For height between 150cm to 180cm, recommended distance between terminal and user is 0.5m.

1:N Facial Verification: Compare the acquired facial images with all face data registered in the device.

1:1 Facial Verification: Compare the face captured by the camera with the facial template related to the entered user ID.

If a user fails to verify, the screen will be prompted with a message “Please adjust your position!”.

Follow the steps below to enroll a Face:

- **Step 1:** Press Menu > User Mgt > New User
- **Step 2:** User ID > Key in User ID This is the unique ID number that represents the user in the devices and software. Make sure you do not use duplicated ID. The maximum length is 9-digits

- **Step 3:** Select Face > Follow the voice and interface prompts to move back and forth to place your eyes within the green box > Register Face success

- **Step 4:** Press User Role > Select Role > Select Normal User > Press OK to save

Cannot enroll duplicate face, otherwise device will show message 'Duplicated Face'

Palm Enrollment

Please place your palm parallel to the device with a distance of 30-50cm in the multi-mode collection area. Make sure to keep space between your fingers.

1:N Palm Verification mode: Compare the palm image collected by the palm collected with all the palm data in the device.

The device will automatically distinguish between the palm and the face verification mod, and place the palm in the area that can be collected by the palm collected, and the device will automatically detect the palm verification mode.

1:1 Palm Verification mode: Click the (x) button on the main screen to enter 1:1 palm verification mode. Input the user ID and press [OK].

If the user has registered the face and password in addition to his/her palm, and the verification method is set to palm/face/password verification, the following screen will appear. Select the palm icon (x) to enter palm verification mode.

Follow the steps below to enroll a Palm:

- **Step 1:** Press Menu > User Mgt > New User

- **Step 2:** User ID > Key in User ID This is the unique ID number that represents the user in the devices and software. Make sure you do not use duplicated ID. The maximum length is 9-digits

- **Step 3:** Select Plam > Follow the steps and stay still during the plam registration > Register Plam success

- **Step 4:** Press User Role > Select Role > Select Normal User > Press OK to save

Card Enrollment * Only for Face ID5

Please check the technical specifications of the device to ensure that this function is supported before continuing. The default card type is 64-bit, 125kHz RFID card. MIFARE and HID card systems are available upon request.

Follow the steps below to enroll a card:

- **Step 1:** Press Menu > User Mgt > New User
- **Step 2:** User ID > Key in User ID
  This is the unique ID number that represents the user in the devices and software. Make sure you do not use duplicated ID. The maximum length is 9 digits
- **Step 3:** Select Card > Wave card at the induction area > Screen displays the card ID > Press OK to save
- **Step 4:** Press User Role > Select Role > Select Normal User > Press OK to save
  Select Super Admin or other defined role(s) you wish to assign to this user.

Refer to page 15 for more details regarding User Role

Password Enrollment

Password verifications have a lessened security presence in Attendance Reporting and Access control systems. Despite this, passwords are generally the primary preference for enrollment. FingerTec devices can accept up to 8-digit passwords in numeric format.

Follow the steps below to enroll password:

- **Step 1:** Press Menu > User Mgt > New User
- **Step 2:** User ID > Key in User ID
  This is the unique ID number that represent the user in the devices and software. Make sure you do not use an existing ID. The maximum length is 9 digits
- **Step 3:** Select Password
- **Step 4:** Insert password for the 1st time > Press OK > Re-enter the password to confirm
- **Step 5:** Press User Role > Select Role > Select Normal User > Press OK to save
  Select Super Admin or other defined role(s) you wish to assign to this user.

Refer to page 15 for more details regarding User Role

Combined Verification

Security can be enhanced with terminal which offers the option of using multiple forms of verification methods.

Select one from the following fifteen verification combinations

- Password/Fingerprint/Face/Palm
- Fingerprint only
- User ID only
- Password
- User ID + Fingerprint
- Fingerprint + Password
- User ID +Fingerprint + Password
- Face Only
- Face + Fingerprint
- Face + Password
- Face + Fingerprint + Password
- Palm
- Palm + Face
- Palm + Fingerprint
- Palm + Face + Fingerprint

Verification may fail if the required verification information has not been registered before opting the combination verification mode.

Menu Options

Expiration Options

You can set the expiration options for each employee if required. Once the expiration period for the employee has been exceeded, access to the company will be restricted.

To turn on the function:

Step 1: Press Menu > System > Attendance > Expiration Rule > Press OK to turn it ON

Step 2: Press Menu > User Mgt > New User > Expiration Rule > Press OK to Enter

Step 3: Select the Expiration Options as below.

- ***Expired Date:*** You must set the employees' employment starting and ending date.
- ***Entries:*** You can set the number of transaction for the employee before their working duration expires. For example, once their attendance transaction reaches the limit, the employee's access will be marked as 'expired 'and will be barred from entering the premises.
- ***Expired Date and Entries:*** You can set both the expired date and entries for one employee. The settings will take effect when either option has been attained. For example if the expired date is set as 11th of January with the number of Entries set at 500, and the employee had his 500th verification on 9th of January, the expiration rule will take place on 9th of January.

You can also set for the user to be deleted or to remain in the system once the expiration options have been fulfilled. For more details on these settings, refer to refer to page 32 Expiration Rule.

Add User

During the initial registration, you can modify your ID - a user name may contain 17 characters and the user ID may contain 1-9 digits by default. Created IDs cannot be modified after registration. Duplicating ID is not allowed.

To add user(s):

- **Step 1:** Press Menu > User Mg > New User
- **Step 2:** Key in User ID and name > Press OK Button

Edit User

Name Change, user role, deletion or re-enrollment of fingerprints, card and/or passwords can be modified after the enrollment process. However the user ID is permanent and cannot be changed.

To edit user information:

- **Step 1:** Press Menu > User Mgt > All User > User ID
- **Step 2:** Key in User ID > Press OK Button > Select Edit
- **Step 3:** Select the credentials to be edited > Save and Exit.

Delete User

Only an administrator can perform user deletion at the terminal.

To delete user(s):

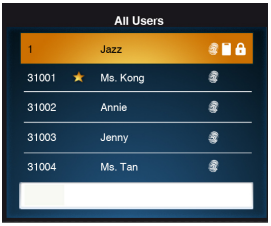
- **Step 1:** Press Menu > User Mgt > All User > User ID
- **Step 2:** Key in User ID > Press OK Button > Select Delete
- **Step 3:** Select Delete User, User Role, Fingerprint or Password
- **Step 4:** Press OK Button to delete > Select OK to confirm deletion > ESC to exit.

Display Option

Users can choose the display style of their credentials either to be in. Single Line, Multiple Line, Mixed Line, Single Line & Sort by Name, Multiple Line & Sort by Name and Mixed Line & Sort by Name.

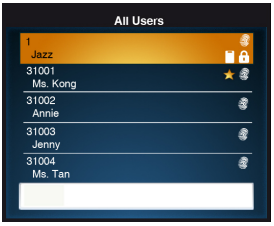
The different types of display are shown below:

Press Menu > User Mgt > Display Style > Select the type of Display > ESC to Exit

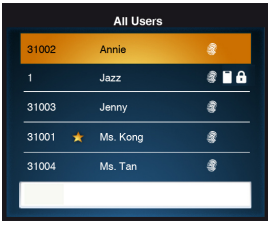


SINGLE LINE

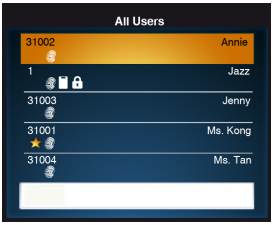
MULTIPLE LINE



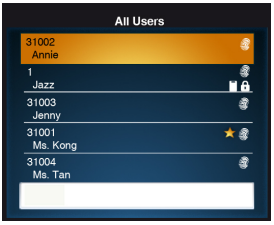
MIXED LINE



SINGLE LINE & SORT BY NAME



MULTIPLE LINE & SORT BY NAME



MIXED LINE & SORT BY NAME

User Role

Employees with Super Admin rights are granted limitless access to all settings and systems within the terminal in addition to the ability to enroll new users. Super Admin can also perform system Reset.

Employees with Normal User rights are only able to log in their attendance at a terminal. They are unable to access the menu to modify settings within the menu.

In addition to the three defined roles, you are given the option to configure 3 different subsets.

Refer to page 16 on details on how to configure the User Defined Role.

Define Role

You can define what the administrator is allowed to do at the device. You will be advised to create a Super Administrator first after clicking the enable bar. A maximum of three different role sets can be configured. For example, you create a role called Network Admin, and limit his access to the Network option only. Therefore, he is unable to enroll new users or configure device settings.

To set the define user role:

- **Step 1:** Press Menu > User Role
- **Step 2:** Select User Defined Role > Press OK > Press OK again to enable the selected Role
- **Step 3:** Rename the Role > Define User Role > Save and Exit.

Once these roles have been defined, they will appear in the Users tab where you can assign employees accordingly.

Assign Role

To define roles for new employees:

- **Step 1:** Menu > User Mgt > New User > User Role
- **Step 2:** Select the role to assign to the employee > Save and Exit.

To define roles for existing employees:

- **Step 1:** Menu > User Mgt > All Users > Press OK > Select the User ID > Press OK > Edit
- **Step 2:** User Role > Select the role to assign to the employee > Save and Exit

Search for Users

Search bar is available on the user list to enable quick search by entering the retrieval keyword (The keyword may be an ID, surname or full name.). The system will detect the input keywords and retrieve users' related information.

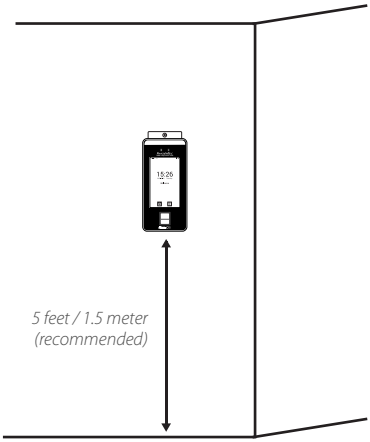
Chapter 4

Installations & Communication

Installations

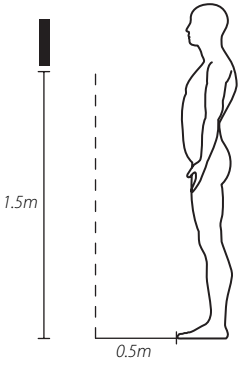
FingerTec terminals offer several connections for power and communications. Installations of FingerTec time attendance terminals are simple.

Mount On Wall



After measuring the height accordingly and make relevant marking on the wall, drill the screws into the wall to secure the back plate.

Attach the terminal to the back plate and tighten the screws.



Installation tips:

Best installation location of terminal must be

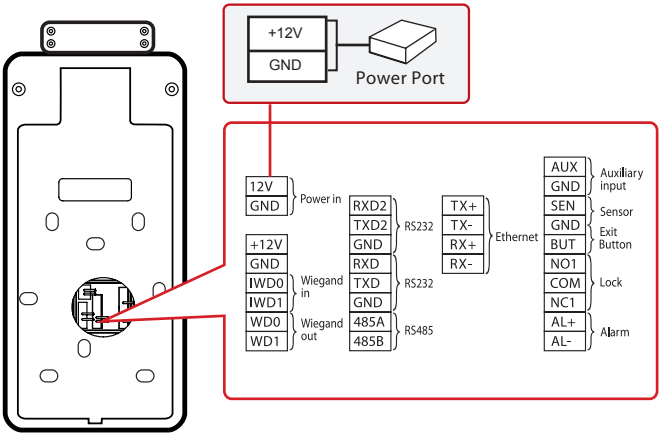
1 - Avoid from direct or indirect sunlight.

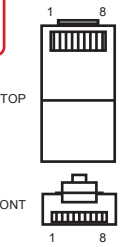
2 - 2 meters away from light source i.e. ceiling flourocent light

3 - Suggested 1.5m from the ground level (measure from ground to the face capturing camera)

Communications

Connection points for power and communication are available on top of the terminals. Refer to the following diagrams for the terminals you require.





TCP/IP Port

Connect with CAT 5 cable for LAN connection, one end to this port and another end to the computer's TCP/IP Port.

TCP/IP for Single Connection – Linking the terminal to a single computer using TCP/IP requires Ethernet 10/100Base-T Crossover Cable. The cable can be used to cascade hubs or to connect Ethernet stations back-to-back without a hub. It works with both 10Base-T and 100Base-TX.

JOINT 1 PIN		JOINT 2 PIN
TX+	1 — 3	RX+
TX-	2 — 6	RX-
RX+	3 — 1	TX+
RX-	6 — 2	TX-

TCP/IP for Network Connection – Linking the terminals to multiple computers using TCP/IP requires Ethernet 10/100Base-T Straight Thru Cable or "whips". The cable works with both 10Base-T and 100Base-TX, connecting a network interface card to a hub or network outlet.

CONNECTOR PIN		CABLE COLOR		CONNECTOR
TX+	1	White/Orange	1	TX+
TX-	2	Orange	2	TX-
RX+	3	White/Green	3	RX+
	4	Blue	4	
	5	White/Blue	5	
RX-	6	Green	6	RX-
	7	White/Brown	7	
	8	Brown	8	

Power Supply Port

Insert the Power Adapter point to this port for power.

RS485 & Wiegand Connection Port

RS485 Single Connection - Connection to a single computer using RS485 wire.
Wiegand Output – Connecting with third party connector or terminal(s)

Access Control Port

Linking Face ID terminal to door lock system.

External Alarm Port

Connect to External Siren for Door security

FingerTec devices offer several types of communication mediums for data transfer that allows you to share employee credentials across all devices within the network without re-enrolling users. Employee attendances are downloaded into our software for easy viewing, analysis and reporting.

We recommend that you delete the attendance records upon completion of the download process. The deletion process can be done manually at the device or commands via the software's interface.

This chapter will provide instructions to guide you in setting up the correct parameters to establish connection between your devices and the software. The available communication methods are listed below:

- TCP/IP
- WiFi (Wireless)*
- GPRS or 3G*
- Webster
- RS 232/RS 485
- USB drive

**This communication method is only available upon request*

Configuring your Device ID should be your first step before continuing with the above communication methods. It is crucial that each terminal's unique ID is identified and set apart. By default, all our Device IDs are set to "1", therefore you must change the Device ID manually if multiple devices are installed.

To change the Terminal ID:

Step 1: Menu > Comm. > PC Connection > Device ID > OK

Step 2: Insert new ID by pressing the keypad > OK to Save > ESC to Exit

COM KEY

Create password for a specific terminal here. The security password known as COM Key is intended for extra security. To conect the terminal with the sofgtware, the COM Key inserted in the Software must be the same as the one inserted in the terminal or else the connection will not be established even though the activation key and product key are correctly inserted.

To set the Comm. Key

- **Step 1:** Menu > Comm. > PC Connection > Comm. Key
- **Step 2:** Insert the password by pressing the keypad > OK to Save > ESC to Exit

Configure TCP/IP connection

Internet Protocol (IP) is a unique numeric designation of each device within a network. Without an assigned IP Address, it would make identifying a specific terminal difficult. The default IP address of each terminal is 192.168.1.201. Connect your terminal via a RJ45 (LAN cable) to connect to your local area network.

To change the IP address:

- **Step 1:** Menu > Comm. > Ethernet > IP Address > OK
- **Step 2:** Insert the IP Address > Press Down arrow to go to the next column

See below to understand every column.

- IP Address: Known as Internet Protocol Address, the default configuration is 192.168.1.201.
- Subnet Mask: Set to 255.255.255.0 by default, this is used to manage a specified network range. You may change the subnet mask if you have multiple networks in your company.
- Gateway: By default, it is configured as 0.0.0.0. Only configure the gateway if the device and PC are on different IP ranges.
- DNS: Domain Name System. By default, the DNS has been configured as 0.0.0.0. If you are using your own internal DNS servers, please change your DNS to ensure that it is reflected accordingly.
- TCP COMM Port: The default port is 4370. Only change the number if your network is unable to utilize this port.
- DHCP: Dynamic Host Configuration Protocol. It's used to allocate dynamic IP addresses to clients on a network.
- Display in Status Bar: Select to enable the display of the network icon on the status bar.

Configure Cloud Server Connection

This setting is used for connecting with the ADMS server.

To connecting with the ADMS server

Menu > Comm. Settings interface > Cloud Server Setting

Enable Domain Name > Server Address > Default domain name mode after enabling is ***"http://…", such as http://www.XYYZ.com.*** Once the mode is ON, the "XYZ" will be the indication of domain name.

Disable Domain Name > Server Address > IP address of the ADMS server.
Disable Domain Name > Server Port > Port used by the ADMS server.

Enable Proxy Server > Set the IP address and port number of the proxy server after enabling the proxy.

Configure WiFi

A wireless connection (WiFi) is an available hardware feature in some FingerTec devices. You can link up your devices with the software via a wireless connection.

To configure the WiFi connection:

- **Step 1:** Menu > Comm. > Wireless Network > enable WiFi connection > ESC to Save and Exit.
- **Step 2:** Wait for the device to scan the SSID of your WiFi network.
- **Step 3:** Select the SSID of the WiFi network > OK to confirm
- **Step 4:** Insert the WiFi password > OK to confirm
- **Step 5:** Select to use DHCP or Manual assign IP
- **Step 6:** ESC to return to the main menu
- **Step 7:** The WiFi icon appears on the main menu

RS232/RS485 serial Configuration

When TCP/IP, WiFi or GPRS/3G connections are unavailable, a serial connection is the preferred communication between the terminal and PC. RS 232 is a one-to-one connection between a device and a PC. The RS485 supports the network wiring by using the RS485 cable to associate multiple devices to a PC.

A data converter must be installed at the PC to switch the RS 485 data signal to a RS 232 signal that can then be processed by the PC.

To setup either RS 232 or RS 485:

Step 1: Menu > Comm. > Serial Comm. > Select RS232 or RS485 > OK to turn on.

Step 2: Configure the settings in the page as explained below:

- Baudrate: This is the communication speed for the serial connection. RS232 supports up to 115200 bps, while the RS485 supports up to 9600 bps to ensure no loss of data is incurred.

Enabling Wiegand

Wiegand is used as a bridge between FingerTec devices and 3rd party door Access Controller. Please disregard this section if you are not using a 3rd party door Access Controller.

FingerTec devices supports 26-bits Wiegand data for input and output. Refer to the steps below to pair your FingerTec device with your door controller or reader.

To configure the Wiegand input parameters:

Step 1: Menu > Comm. > Wiegand Setup > Select Wiegand In > OK.

Step 2: Configure the Wiegand data settings

- Wiegand Format: 26-bits
- Wiegand Bits: Specify the number of bits occupied by the Wiegand.
- Pulse Width: The default pulse width is 100 microseconds. It can be adjusted to between 20 and 100
- Pulse Interval: Is configured to 1000 by default. It can be adjusted to between 200 and 20000 microseconds.
- ID Type: Identifies the content of the data output by Wiegand (User ID and badge number)
- Format Details: Displays information from Wiegand

To configure the Wiegand output parameters:

Step 1: Menu > Comm. > Wiegand Setup > Select Wiegand Out > OK.

Step 2: Configure the Wiegand data settings

- SRB: Prevent the lock from being opened due to device removal.
- Wiegand Format: 26-bits
- Wiegand Output bits: Select one corresponding output digits in the Wiegand format.
- Failed ID: System will directly regenerate a new card number or personnel ID for failed IDs.
- Site Code: can be set manually and is repeatable in a different device. Valid value ranges from 0 to 256 by default.
- Pulse Width: The changes of quantity of the electric charge with high-frequency capacitance within a specified time.
- ID Type: Identifies the content of the data output by Wiegand (User ID and badge number)

Ingress Online Activation

Ingress is a genuine software by FingerTec. Every FingerTec time attendance model comes bundled with a unique license key. To start using the terminal with Ingress, you must connect the terminal to Ingress and perform an online activation. Ingress reads the serial number of your terminal and sends it for verification at the FingerTec server via the Internet.

In case you do not have an Internet connection, you need to do offline activation. Please send the serial number and model of your terminal to your local reseller or *support@fingertec.com* to request for a product key

Installation and Setup of Ingress

Install Ingress in a PC that fulfils the software's minimum requirements. Refer to *http://www.fingertec.com/customer/download/postsales/SUM-Ingress-E.pdf* for the Ingress user guide online. Setup Wizard will require you to do online activation before any connection is established between Ingress and the terminal(s).

Connecting The Terminals to Ingress

Determining Terminal Number

Identify the number of your terminals to differentiate them between one another. Ingress can connect up to 999 units of terminal.

- **Step 1:** Press Menu > Options > Comm Opt
- **Step 2:** PC Connection > Dev Num > Select the number

Using TCP/IP

IP address is important, as it is a unique address of the terminal in LAN. Without the IP address, locating the specific terminal is not possible.

To input the IP address of the terminal:

- **Step 1:** Press Menu > Comm. > OK to Enter
- **Step 2:** Ethernet > IP Address > Key in IP Address

Setting Up Netmask and Gateway

Determining the Netmask, Gateway and NetSpeed: For TCP/IP connection, please configure the netmask, gateway and netspeed for the terminal.

Setting Up Netmask

- **Step 1:** Press Menu > Comm.
- **Step 2:** Ethernet > Subnet Mask > Insert the numbers.

Setting Up Gateway

- **Step 1:** Press Menu > Comm.
- **Step 2:** Ethernet > Gateway > Insert the numbers.

Using RS232 Connection

For connection via RS232,baudrate is the determinant of communication speed between the terminal and the software. The higher the baudrate, the faster the speed is.

To turn on RS232 connection and set the baudrate:

- **Step 1:** Press Menu > Comm.
- **Step 2:** Serial Comm. > RS232 > Turn it On

To change baudrate:

- **Step 1:** Press Menu > Comm.
- **Step 2:** Serial Comm. > Baud Rate > Select the baud rate.

Using RS485 Connection

For connection via RS485, baudrate is also the determinant of communication speed between the terminal and the software but the speed must be according to the speed of theconverter. Check your converter for the speed.

To turn on RS485 connection and set the baudrate:

- **Step 1:** Press Menu > Comm.
- **Step 2:** Serial Comm. > RS485 > Turn it On

To change baudrate:

- **Step 1:** Press Menu > Comm.
- **Step 2:** Serial Comm. > Baud Rate > Select the baud rate.

PC Connection Communication Key

The Comm Key is used as a communication between the device and the PC to protect the security of data. If a Comm Key is set, the connection password must be entered before the device can be connected to the PC software.

Set the COMM key to zero:

- **Step 1:** Press Menu > Comm.
- **Step 2:** PC Connection > Comm. Key > Set to 0.

- Comm Key: Default Password: 0. The Comm Key may contain 1-6 digits.
- Device ID: Select identity number of the device between 1 and 254. Input this device ID if the communication method is RS232/RS485 in the software communication interface.

Chapter 5
System

FingerTec devices can be personalised according to preference. These settings include date/time, storage of in-out records and biometric verification rules. You can find the Reset option which allows you to program your devices to default factory settings, under this chapter.

Setup Date and Time

The Date & Time is a very crucial aspect for accurate logging of attendance and the record of door activity in each company. The date and time of the terminal will be displayed at the home screen. You can choose the date and time format based on your preference.

To set date:

- **Step 1:** Press Menu > System > Date & Time > Set Manual data and time
- **Step 2:** Set the Date accordingly.

You can change the Date format. To set the format:
Press Menu > System > Date & Time > Select the date format

To set time:

- **Step 1:** Press Menu > System > Date & Time > Set Time
- **Step 2:** Set the Time accordingly.

The time can be set by pressing the up or down arrow, or by pressing the number button.

You can change the display of time format. To set the time format:
Press Menu > System > Date & Time > 24-hour time

Select ON to display as 24-Hour format or OFF to display it in12-hour format (with AM and PM)

To use Daylight Savings Time (DLST)

Daylight saving time (DLST) is the practice of temporarily advancing clocks so that the daylight in the afternoon will be longer whereas morning will be shorter. Please disregard this if DLST does not apply to your country.

To set the DLST settings:

- **Step 1:** Press Menu > System > Date & Time > Daylight Saving Time > Press OK to enable
- **Step 2:** Select Daylight Saving Mode > Select either By date/time or By week/day > Configure details in Daylight Saving Setup

By Date/Time:

This option is recommended if you know the exact date the DLST begins. For example, if company A wants to set the DLST to begin from May 3rd 22:15 hour and ends on July 10th 11:15 hour, this setting should be chosen.

- **Step 1:** Set the month and date for the DLST to begin
- **Step 2:** Set the time (in HH.MM format) on when the DLST will begin.
- **Step 3:** Set the month and date for the DLST will end.
- **Step 4:** Set the end time of the DLST period.

By Week/Day:

This option is recommended if you want the DLST settings to take place on the exact week, month and day every year regardless of the date. For example, if company B wants to set the DLST to begin from the Sunday of the 2nd week of February at 1510 hour and ends on the 4th week of May at 1000 hour each year, this setting should be chosen.

- **Step 1:** Set the month for the DLST to begin.
- **Step 2:** Set the week for the DLST to begin.
- **Step 3:** Set the day for the DLST to begin.
- **Step 4:** Set the time (in HH.MM format) on when the DLST will begin.
- **Step 5:** Set the month for the DLST to end.
- **Step 6:** Set the week for the DLST will end.
- **Step 7:** Set the end day of the DLST period.
- **Step 8:** Set the end time of the DLST period.

Access Log Settings

Press Menu > System > Access Logs Setting

- Camera Mode: 5 modes to capture and save snapshot images during verification:
  No Photo: No photo will be taken during user verification.
  Take photo, no save: Photo will be taken but will not be saved during verification.
  Take photo and save: Photo will be taken and saved during verification.
  Save on successful verification: Photo will be taken and saved for each successful verification. Save on failed verification: Photo will be taken and saved during each failed verification.
- Display User Photo: Options to display the user photo whenever a user passes verification.
- Access Logs Warning: Display automatic remaining record memory warning when the record space reaches a set value. Select to disable or set a valid value between 1 and 9999.
- Circulation Delete Access Records: Set to automatically delete a set value of old access records once the access records have reached its full capacity. Select to disable or set a valid value between 1 and 999.
- Cyclic Delete ATT Photo: Set to automatically delete a set value of old attendance photos once the attendance photos have reached its full capacity. Select to disable or set a valid value between 1 and 99.
- Cyclic Delete Blacklist Photo: Set to automatically delete a set value of blacklisted photos once the blacklisted photos have reached its full capacity. Select to disable or set a valid value between 1 and 99.
- Confirm Screen Delay(s): Set a valid value between 1-9s for the length of time to display the message of successful verification.
- Face Comparison Interval(s): Set the facial template matching time interval as per required. Valid value ranges between 0-9s.

Attendance Record Storage Option

Each time a verification is performed on the device, a transaction log will be stored inside the terminal. These logs need to be managed to maintain the effectiveness of the devices. However, you can only setup rules to control attendance capturing and storage.

Press Menu > System > Attendance > Select type of rules to configure

Display User photo

You can set the device to display a photo of the employee after a successful verification. A success verified indicator will appear on the screen after his/her ID and name has been verified. You can transfer photos from the software to the device.

This should be enabled if you would like the device to display the employees' photo on screen.

Alphanumeric User ID

You can set employee IDs with alphanumeric entry for example, ENG1003 represents staff ID 1003 from the Engineering Department. This alphanumeric ID recommended for large organizations with multiple departments.The person in charge will know which department the employees belong to by referring to their ID. Only enable this if your company intends to separate employees from different departments.

Attendance Log Alert

You can set the device to prompt an alert message on screen every time it verifies an employee when its storage is approaching the limit. The value ranges from 1 to 99 (transaction counts). The device will always delete earlier records to free up space to save the latest record (FIFO, first in first out), if storage is full. By default, the value is 99. Change it if you want to apply another value.

Cyclic Delete ATT Data

You can set the device to delete a number of records when its storage is full. The value range is from 1 to 999 records. For example, you can set the value at 500 records and the device will delete the first 500 records to free up the space to store new records.

Cyclic Delete ATT Photo

You can set the device to delete a number of stored photos when its storage is full. The value range is from 1 to 99. For example, you can set the value to 50 and the device will delete the first 50 photos to free up slots to store new images.

Confirm Screen Delay(s)

You can set the time delay for the device to display verification results (ID, name and photo). The time range is from 1s to 9s.

Fingerprint Options

Threshold is the level of security during a fingerprint verification process. Threshold determines how many percent of minutiae points on a fingerprint template will be read by the system.

The higher the threshold level means the device will require additional minutiae points to verify an employee. Thus increasing its security. There are 2 sets of Threshold settings for different verification process:

- 1:1 Matching Threshold Value: 1:1 match is where one verification method is matched to only one template. Employee presses keypad to insert his/her ID followed by OK button and fingerprint verification
- 1:N Matching Threshold Value: 1:N (many) match is where the verification is compared against N templates. Employee presses finger on the scanner to verify.
- High Security: If high security is intended, the threshold value must be set to high. Do take note that if the threshold value is set to high, users may be inconvenienced due to the requirement may need multiple verifications of the fingerprint. For example: If security level is set to high, the chances of identifying the wrong person will be very low. However, you need to verify for a few times before your credentials are verified.
- Normal: This is the default setting where both the security and convenience level are in balance.
- Low Security: If high convenience is intended, the threshold value must be set to low. Do take note that if convenience level is high, the security level will be low, thus the chances of inaccurate identification will be high.

Below is the table for ease of setting.

Types	1:N	1:1
High Security	*45*	*25*
Normal	*35*	*15*
Low Security	*25*	*10*

- FP Sensor Sensitivity: You can set the sensitivity of the fingerprint prism to respond to the employee when he/she places finger on it. The default value is set at Medium. However, when the environment is dry, it is recommended to set the sensitivity to high and set to low if the environment is humid.

- 1:1 Retry Times: You can set the maximum number of attempts for 1:1 fingerprint verification or password verification. The device will trigger an alarm system when the limit has been reached.

Note: Both algorithms are not compatible with each other.

Fingerprint Image

Select to display the fingerprint image on the screen. Four choices are available:

- Show for enroll: Display the fingerprint image on the screen only during enrollment
- Show for match: Display the fingerprint image on the screen only during verification.
- Always show: To display the fingerprint image on screen during enrollment and verification.
- None: No display of any fingerprint image.

Face Parameters

Press Menu > System > Face

- 1:1 Matching Threshold Value
  1:1 match is where one verification method is matched to only one template. Valid value ranges from 55 to 120. The higher the thresholds, the lower the misjudgment rate, the higher the rejection rate, and vice versa. Default value: 63 is recommended.
- 1:N Matching Threshold Value
  1:N (many) matches are where the verification is compared against N templates. Valid value ranges from 65 to 120. The higher the thresholds, the lower the misjudgement rate, the higher the rejection rate, and vice versa. Default value: 75 is recommended.
- Face Enrollment Threshold
  Face enrollment opts 1:N comparison to determine the validity of a user (registered/no register). Registered facial templates will appear greater than the threshold.
- Face Pitch Angle
  The pitch angle tolerance of a face for facial registration and comparison. Once a face's pitch angle exceeds this set value, the algorithm will conduct a filtration. Any failure or ignorance by the terminal will not trigger any registration nor comparison interface.
- Face Rotation Angle
  Rotation angle tolerance of a face is used for facial template registration and comparison. Once a face's rotation angle exceeds this set value, the algorithm will conduct a filtration. Any failure or ignorance by the terminal will not trigger any registration nor comparison interface.

- Image Quality
  Image quality for facial registration and comparison. The higher the value, the clearer the image requires.
- Minimum Face Size
  The required size for facial registration and comparison. The object will not be filtered or recognized if the size of an object is smaller than this set value. This value can be understood as the face comparison distance. Stand and adjust a moderate distance to ensure the device captures the right face for comparison and algorithm processes. If the value is 0, the face comparison distance is not limited.
- LED Light Triggered Threshold
  Change to control the on and off of the LED light. The greater the value, the more frequently the LED light will be turned on.
- Motion Detection
  The measurement of the potential motion detection that wakes the terminal from static motion to the comparison interface. The greater the value, the higher sensitivity level the system would be. A larger value set can trigger the interface much easier and more frequently.
- Live Detection
  Determine if the source of a biometric sample. Prevent a spoof attempt using visible light images.
- Live Detection Threshold
  Set value to judge the visible image comes from an alive body. The greater the value, the better the visible light anti-spoofing performance.
- Anti-counterfeiting with NIR
  Identify and prevent fake photos and videos attack using near-infrared spectra imaging.
- Wide Dynamic Range (WDR)
  Balance light and extend image visibility under high contrast lighting scenes; Improve object detection under bright and dark environments.
- Anti-flicker Mode
  Can be used when WDR is turned off. Reduce flicker when the device screen is flashing at the same frequency as the light.

Note: Do not attempt to adjust the exposure or quality parameters as it may severely affect the overall performance of the device. Please adjust the exposure parameter under the guidance of our after-sales service personnel

Palm Parameters

Press Menu > System > Palm

- Palm 1:1 Matching Threshold
  Only if the similarity between the verifying palm and the user's registered palm is greater than this value to attain successful verification.
- Palm 1:N Matching Threshold
  Only if the similarity between the verifying palm and the user's registered palm greater than this value to attain successful verification.

Reset Options

In an event you want to restore the terminal back to the factory settings.

To reset options setting:

Menu > System > Reset > Press OK.

A confirmation window will prompt you before the terminal is reset. Ensure that you are certain of performing the task before proceeding to avoid irreversible data loss.

Chapter 6

Personalization

You can manage the display style of your FingerTec device according to your preference. These include the user interface, voice, bell schedules, punch state options, and shortcut key mapping.

User Interface

The user interface is designed as such so that users can interact with the device. These include the appearance of the device, response time, and the content that is presented to the user.

To setup the display of the User Interface:

Go to Menu > Personalize > User Interface > Press OK to Enter > Press arrow and OK button to enable or disable the options:

- Wallpaper: You can choose which wallpaper to be displayed on the screen
- Language: There are 8 languages preloaded into your device. Select the language that fits your environment
- Lock Power Key: You can disable the ON/OFF button to prevent people from toying with the power button causing the terminal to shut off
- Menu Screen Timeout: The device will return to main screen if you remain inactive in the menu after a certain period of time. You can set the time duration for the time out between 60s to 99999s.
- Idle Time to Slide Show (s): Device will start to play slide shows (photo) on its screen when it is idle. You can set the idle time duration (range from 3s to 999s) before the slide shows start to play.
- Slide Show Interval (s): You can set the time interval between every image for the slide show. The interval ranges from 0-99
- Idle Time to Sleep (m): You can set the idle time duration (range from 1 to 30min) to make the device to go into sleep mode. Pressing any buttons at the device will make it resume operations.
- Main Screen Style: You can select to show clock display style and status key on the main screen.
- Company Name: You can insert your company name into this section. The name will be displayed at on the receipt from the thermal receipt printer after employees report attendance.

Read more regarding receipt printing in chapter 9.

Voice

You can choose to enable or disable the voice prompts, keyboard sound or adjust the volume of the device.

To enable or disable the options:

Go to Menu > Personalize > Voice > Press OK to Enter > Press arrow and OK button

- Voice Prompt: You can choose to disable or enable the voice greetings or feedback during the operations.
- Keyboard Prompt: You can choose to enable or disable the beeping sounds when pressing on the keys
- Volume: You can adjust the volume of the voice greetings/feedback and keyboard beeps

Bell

You can schedule the device to ring automatically during specific times. This is a reminder to alert the employees to start/end work, start/end of break time etc.

To activate this function, you have to create a new bell schedule:

Go to Menu > Personalize > Bell Schedules > Press OK to Enter > New Bell Schedule > Set the option accordingly:

- Bell Status: To turn the bell on or off.
- Bell Time: Set the time for the bell to ring automatically.
- Repeat: Set the bell to repeat on certain days or every day.
- Bell Type: You can set for the bell to be triggered from the internal bell or from an external bell that is wired to the device.
- Ring Tone: Select the bells' preferred ring tone
- Internal Bell Relay: Specifies the time duration for the alarm to ring (ranges from 1s to 999s).

Edit and Delete a Preset Schedule

Once you have created a bell schedule, you can edit or delete the schedule entirely.

Editing the function is similar to adding a new schedule:

Go to Menu > Personalize > Bell Schedules > Press OK > All Bell Schedule > Press OK > Press Down arrow to select the bell schedules > Press OK > Press Edit to edit the existing schedule or Delete to delete the schedule.

Punch State Options

In the event you want your employees to press a button to confirm his/her attendance status (for example Check-In, Break starts etc) you will need to set the punch state from your keyboard's F1 to F8 buttons.

Punch State Mode

Set the display of the status keys:

Go to Menu > Personalize > Punch State Options > Press OK > Punch State Mode > Select one from below:

- Off: To disable the punch state key function. Employees are not required to press any buttons to report their attendance. The screen will not display any Status key. Short-cut Key Mappings menu will also become invalid
- Manual Mode: Switch the punch state key manually, and the punch state key will dis-appear after Punch State Timeout.
- Auto Mode: Once this mode has been chosen, set the punch state key's switching time in Shortcut Key Mapping. The set punch state key will be switched automatically when the switching time is reached.
- Manal and Auto Mode: The main interface will display auto-switching punch state key under this mode while it also supports manually switching the punch state key. The manually switching punch state key will become an auto-switching punch state key after timeout.
- Manual Fixed Mode: The punch state key will remain unchanged until it is being man-ually switched on the next time.
- Fixed Mode: Only a fixed punch state key will be displayed and the status cannot be switched.

Punch State Required

You can set the device to only accept verification after an employee presses the status key to validate their attendance status. The device will not respond to attempts if the employee fails to validate their attendance status.

To enable punch state required:

Go to Menu > Personalize > Punch State Options > Press OK > Punch State Required > Press OK to enable or disable it.

Shortcut Key Mappings

You can assign six shortcuts as attendance or functional keys. On the main interface, when the shortcut keys are pressed, the corresponding attendance status or function interface will display.

To shortcut key mappings setting:

Go to Menu > Personalize > Shortcut Key Mappings > Press OK to Enter > Select the appropriate key by pressing the down arrow > Press OK to choose the corresponding action

Note: When the Attendance Status shortcut key is selected, you can also set the 'Auto Switch' parameter (refer to page 37 regarding Auto Mode).

Chapter 7

Data Manager

Data stored in the terminal can be utilized to establish management rights or have specific logs removed.

To manage your data:

Go to Menu > Data Management > Press OK to Enter

Delete Data

Data stored in the terminal can be deleted within your Data Management function. Below is a list of available options in your terminal:

- Delete Attendance Data: Delete all attendance records.
- Delete Attendance Photo: Delete all employees' attendance images.
- Delete Blacklist Photo: Delete photos of employees' captured during a failed verification attempt.
- Delete All Data: Delete data related to face & fingerprints templates, IDs, passwords, card ID and attendance records.
- Delete Access Control: Delete access control records.
- Delete Admin Role: Removes administrator privileges in your terminal. All employees who had the privilege will identify as a normal user.
- Delete User Photo: Delete all photos.
- Delete Wallpaper: Delete all saved wallpapers.
- Delete Screen Savers: Delete screensavers.

Select Delete All or Delete by Time Range when deleting access records, attendance photos or blacklisted photos. Please ensure to set a specific time range to delete all data with the period if you select Delete by Time Range.

Access control

Access Control options is used to set the Door Lock setting, Time Zone, Holidays and Access Group.

Access Control Options settings

To set the parameters of the Door Lock and related equipment

To setup the Access Control:

Press Menu icon > Access Control > Access Control Options

- Gate Control Mode
  Select to turn on the gate control mode. If ON is selected, the interface will remove the Door lock relay, Door sensor relay and Door sensor type function.
- Door Lock Delay(s)
  This value is the time period for the door to lock again after it unlocks on successful verification. Valid value: 1-10s; 0s represents function disabled.
- Door Sensor Delay(s)
  This function only works if the door sensor is available. When a door is not closing for a specified time, the sensor will trigger the alarm system. Specify the time of the delay. The valid value of Door Sensor Delay ranges from 1 to 255 secs. Choose your preference.
- Door Sensor Type
  There are three types of door sensor available for door access which are None, Normal Open (NO), and Normal Closed (NC). Once a door sensor is available, you have to choose the door sensor type. Dault is None.
- Verification Mode
  The supported verification mode includes password/face, User ID only, password, face only, and face + password.
- NC Time Period
  To set the time period for Normal Closed mode, so that no one can gain access during this period.
- NO Time Period
  To set the time period for Normally Open, so that the door is always unlocked during this period.
- Speaker Alarm
  When the 'Speaker Alarm' is enabled, the speaker will raise an alarm when the device is being dismantled.
- Master Device
  The status of the master can be set to exit on enter when setting up the master and slave terminals.

  Exit: The record verified on the host is the exit record
  Enter: The record verified on the host is the entry record
- Reset Access Settings
  To restore access control parameters. However, erased access control data in Data Mgt. is excluded.

Time Zone

Time Zone is the minimum time period of access control settings, there are 50 Time Zone can be set for the system. Each Time Zone consistof 7 time period section(a week), and each time period section is the valid time for access within 24 hours

To setup the Time Zone

Press Menu icon > Access Control > Time Zone

- **Step 1:** Tap the input box of Search Rime Zone.
- **Step 2:** Enter the number of the time zone (50 in total) to be searched.
- **Step 3:** Tap the date on which time zone setting is required.
- **Step 4:** Press Up and Down to se the start and end time, then press Confirem (OK)

Note:

1. Valid Time Zone: 00:00 ~ 23:59 (Whole day valid) or when the end time is greater than the start time
2. Invalid Time Zone: When the end time is smaller than the start time
3. The default time zone 1 indicates that Device's Door is open all day long

Holidays

The concept of holiday and festival is introduced into Access Control. On holidays or festivals, special access control time may be required, but changing everyone's access control time is very tedious. Therefore, the access control time on holidays, which applies to all staff, can be set. If the access control time on holidays is set, the opening or close period of Lock on Holidays subjects to the time zone set here.

Adding New Holidays

Press Menu > Access Control > Holidays > Add Holiday

- No. : Holiday ID
- Start Date : Date of the holiday setting start applies
- End Date : Date of the holiday setting ends
- Time Zone : select Access time period that the holiday will use

Edit Holidays

Press Menu > Access Control > Holidays > All Holidays > select Holiday > Edit

Delete Holiday

Press Menu > Access Control > Holidays > All Holidays > select Holiday > Delete

Combined Verification Settings

Strengthen the security by arranging the access groups into different door-unlocking combinations. This can be achieved via multiple verifications.

Door-unlocking combination: Range of the combined number N is: $0 \leq N \leq 5$, and the N amount of members may belong to one or more than one different access groups.

Go to Menu > Access Control > Combined Verification

Examples,

If the door unlocking combination 1 is (01 03 05 06 08), this combination has a total of 5 users. These users are 5 individuals from 5 different access control groups (AC group 1, group 3, group 5, group 6 and group 8, respectively).

If the door unlocking combination 2 is (03 05 08 00 00), this combination has a total of 3 users. Users are from AC group 3, AC group 5, and AC group 8.

To delete a door-unlocking combination

Set all group numbers to 0 in order to delete the door-unlocking combinations.

Anti-passback Setup

This function is optional and can be activated to resolve existing security problems. Often, users may be followed by some outsiders while entering the door and these outsiders are without verification. This setup can make sure the all check-in record matches the check-out record with traceable door access activities.

To enable this function, two devices must work together: A master device and a slave device must be installed at the inside and the outside of the door. Two devices communicate via the Wiegand signal. The Wiegand format and Output type (User ID/Badge Number) adopted by the master device and slave device must be consistent.

To enable the Anti-passback Setup:

Press Menu icon > Access Control > Anti-passback Setup

- No Anti-passback: By disabling this function, all successful verification via master or slave device can unlock the door. The attendance state is not saved.
- Out Anti-passback: The user can check-out only if the last status in record is a check-in; otherwise, the alarm will be triggered. This mode allows users to check-in without restriction.
- In Anti-passback: The user can check-in only if the last status in record is a check-out; otherwise, the alarm will be triggered. This mode allows users to check-out without restriction.

- In/Out Anti-passback: The user can check-in if only the last status in record is a check-out; the user can check-out if only the last status in record is a check-in; otherwise, the alarm will be triggered.

Duress Options Settings

By activating the duress verification function with specific authentication method(s), the device will still unlock the door, however, a signal will be sent to trigger the alarm if a user is performing authentication under coercion.

To enable the Duress Options Settings:

Press Menu icon > Access Control > Duress Options

- Alarm on Password: An alarm signal will be generated whenever a user uses the password verification method.
- Alarm Delay(s): Alarm signal will not be transmitted until the alarm delay time is elapsed. Valid value ranges from 1 to 999s.
- Duress Password: Key in 6-digit duress password. This duress password will send out an alarm signal whenever a user enters it.

Access Group Setting

To define group and time period for registered users:

■ **Step 1:** Menu > Access Control Role > Access Group

■ **Step 2:** Menu > Access Control Role > Time Period

User access control allocates the group and the time period that a user belongs to.

New users will be automatically grouped under Group 1 by default and can be reassigned to other groups. Face ID 5 device supports up to 99 access control groups.

- NO. : Acces Group ID
- Verification Mode : Verification type for users in this Group
- Time Zone: valid access time for user is this Group
- Include Holidays : Enabling this mean this group will use the Holiday's settings and Time Zone

Edit Access Group

Press Menu > Access Control > Access Group > All Groups > select Group ID > Edit

Delete Access Group

Press Menu > Access Control > Access Group > All Groups > select Group ID > Delete

Chapter 8

Attendance Search

The device stores attendance records, which can be processed by our software to produce payroll calculations and other reports. This search function is an easy to use module that allows you to check and browse records at your convenience at any time.

You can choose to display photos together with attendance records.

To use this browser:

Go to Menu > Attendance Search > Press OK > Insert the user ID to search (leave blank if you want to see all employees) > Press OK > Select the time range from the list or enter specific date and time at the User Defined > Press OK to see all records

Chapter 9

Work Code

A majority of FingerTec Terminals is incorporated with a feature which allow users to select a reason for re-entry during verification by selecting a work code (for example, work code 13 – Onsite at Customers).

Adding a Work Code

By default, our terminals does not contain any workcodes.

To add a workcode:

Go to Menu > Work Code > New Work Code > Key in the workcode

- ID: The work code ID supports 1 digit to 8 digits in length.
- Name: Short description of the work code.

All Work Codes

All work codes can be viewed, deleted or edited (with the exemption of modifying the ID number) in the All work codes tab. The process of editing a work code is similar to adding a work code as explained in 10.1.

To view all work codes:

Go to Menu > Work Code > All Workcodes > Select the Workcode > Press OK to Select either to Edit or Delete the selected Work Code.

Work Code Options

The option to use work codes must be enabled before it can be utilized.

To turn on Work Code:

Go to Menu > Work Code > Work Code Options > Work Code Required > Press OK to turn it ON

Note: If you wish to bar employees from entering new workcodes during verification, you must enable the function "Work Code must be defined". The terminal will reject work codes it cannot match to in its current list.

Chapter 10

Diagnostic

The Diagnostics page allows you to analyze the condition of your terminal(s) by utilizing a series of tests. Only administrators are authorized to perform these tests. To view the status of your terminal, you can select Go to Menu > Autotest:

Autotest

To automatically test whether all modules in the device function properly, which include the LCD, audio, camera and real-time clock (RTC).

All Test

Autotest whether the LCD, audio, camera and ETC are normal.

Test LCD

Autotest the display effect of the LCD screen by displaying full-colour, pure white, and pure black.

Test Voice

Autotest the voice quality of the audio files and if they are of completed versions.

Test Fingerprint Sensor

Examine the clarity of the acquired fingerprint image by pressing a finger on the scanner. The fingerprint image will display on the screen.

Camera Testing

Examine the proper camera functions by checking the clarity of the taken pictures.

Test Clock RTC

Test the RTC. To examine if the clock works normally and accurately with a stopwatch. Tap on the screen to start counting and tap it again to stop counting.

Chapter 11

System Info

This option allows you to check your terminals storage, firmware, algorithm etc.

To access your system information:

Go to Menu > System Info

Device Capacity

The number of enrolled users, administrator, passwords, total fingerprint and attendance records will be displayed.

Device Info

The Device name, serial number, MAC address, Fingerprint Algorithm, Platform Information, MCU version, Manufacture and Manufactured Date and Time will be shown in this section.

Firmware Info

The Firmware version, Bio Service, Push Service, Standalone Service and Dev Service is available from this tab.

Troubleshooting

“Unable to Connect” Appears

When this message appears, it means that the settings for the terminal and the computer are not properly done. Find out which method you are using to connect. The terminal offers LAN, RS232, RS485 and USB communication methods. Refer to Chapter 4 to further understand the topic.

“Admin Affirm” Appears

You are not the administrator of this terminal. Only an authorized administrator of the system is allowed to access the Menu. Any attempt of normal user to access the Menu will prompt “Admin Affirm” message on the screen. In case the administrator or he/she has resigned from the company, kindly contact your FingerTec authorized reseller to access the terminal.

Difficult to Read Finger

Five things could be the cause of this:

Enrolment is not properly done

Enrolment is the most important process to ensure that the terminal captures the best quality of your fingerprints. Refer to chapter 3 for how to do a good enrollment.

The location of the terminal is not conducive

The scanner does not work well in bright-lighted area. Cover the scanner a little if this is the cause of the difficulty. Shift the location area for a better performance.

Finger is not properly placed

To get a good read, make sure that your finger’s center points are located at the middle of the scanner. Adjust the position of your fingerprint as you see it onscreen.

The scanner is not cleaned or it is scratched

Check the quality of the scanner. If the scanner is dirty, please clean it with a microfiber cloth. If it is scratched, contact your local reseller for a replacement.

Did anything happen to your finger lately?

Make sure that the finger is not injured, cut or bruised which could cause it difficulty to read. The algorithm reads the minutiae points of your fingerprint, the more it can read, the better the result.

"Duplicate Finger" Appears

FingerTec terminals are intelligent. It will not accept the same fingerprint twice into its system. If you have registered a finger into the terminal, the system would prompt "duplicate finger" when you try to enroll that finger for another time. Choose a different finger to proceed.

RFID Card Doesn't Respond

Two possibilities for this problem

Have you registered the card to the terminal?

The card must be registered to the terminal before it can read the information in the card. Refer to chapter 3 User for card enrolment.

Have you assigned the user ID to the verification group that supports RFID card?

Without setting the terminal to show that you are under a group that supports RFID card, the terminal wouldn't read your card.

No Sound

A few things could cause this problem:

The terminal voice mode is silent

Perhaps someone has turned off the voice in your terminal or reduced its volume to 0%. Refer to Chapter 6 Personalization.

Speaker is damaged

Once you have rectified the voice mode, if the problem persists, proceed to test the voice. Go to Chapter 10 to do the test. If no voice is being emitted, contact your local reseller for support.

For more troubleshooting, go to *http://user.fingertec.com/*