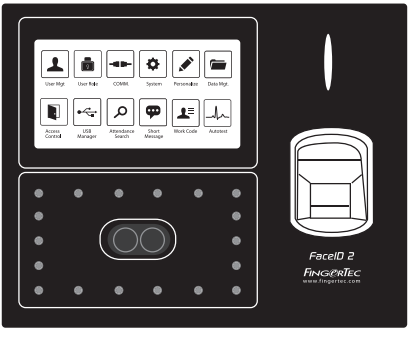
FINGERTEC



Face ID 2 FMM

User Guide

Contents

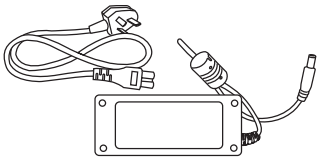
Chapter 1
Getting Started

Viewing the User Guide in the Internet

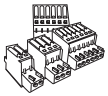
The User Guide is available in the package when you purchased the terminal. The User Guide is also available online at http://www.fingertec.com and http://user.fingertec.com. Choose the language that you prefer for your User Guide.

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.

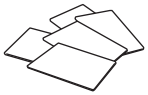


DC 12V Power Adapter



Connection Wires

Screwdriver



RFID Cards (5 pieces)

A Packet of Bolts

Measurement Tape

Diode

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*
RFID Cards (5 pieces)	*For card enrollment and verification*
A Packet of Bolts	*Use the screws to hold the back plate of the terminal against a wall*
Measurement Tape	*Measuring installation height to achieve optimum performance for terminal*
Diode	*For installation of door lock system, allowing electrical current to pass through it in one direction only; can be thought of as a check valve*

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

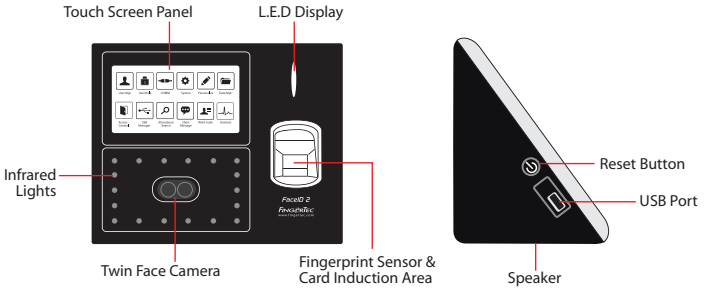
Make sure that you register your terminal's warranty with us at *http://www.fingertec.com/ver2/english/e_warranty.htm*.
for a 36 month warranty protection.

Chapter 2
Basics

Introduction to Terminal

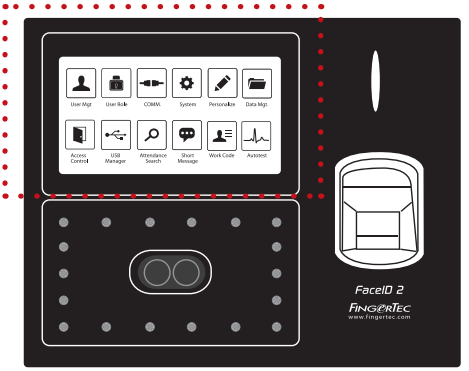
Introducing Face ID 2, the latest biometrics product, face recognition technology product combined with fingerprint technology. Face ID 2 can identify an identity in split seconds without any contact or hassle. Face ID 2 only requires user to look at the machine to get verification. Face ID 2 is loaded 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 Face ID 2 terminal accepts card verification as an added security measure. If you are looking for contactless, hassle free biometrics product, choose Face ID 2. With one look you are good to go!

Terminal Overview



ITEM	FUNCTION
Touch Screen Panel	*Touch this screen to access into terminal system and do configuration.*
Infrared Lights	*Enhance facial image in poorly lighted areas.*
Twin Face Camera	*Capture face images in few directions.*
Fingerprint Sensor	*To scan finger for confirmation of identity.*
Card Induction Area	*Area that reads RFID cards.*
LED Light Indicator	*Indicate the status of terminal.* *• Green indicates terminal is on standby or verification is successful.* *• Red indicates problem or verification is fail.*
Speaker	*For terminal voice emission.*
USB Port	*To upload/download users information, password and transaction logs via USB disk.*
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.

USB Manager
Upload and download data and information to and from FingerTec terminal using a USB flash disk.

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

Short Message
Create & manage Short Message display.

Work Code
Create & manage workcode functionality.

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

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.

- 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 16 User Role for more details. Repeat Steps 3 and 4 to enroll the 2nd backup fingerprint.

Face Enrollment

During enrolment on Face ID 2, 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 Face ID and user is 0.5m.

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'

Card Enrollment

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 16 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 16 for more details regarding User Role

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.

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):

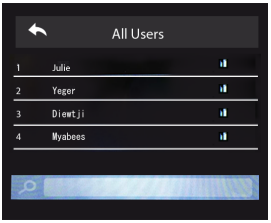
- **Step 1:** Press Menu > User Mgt > All User > User ID
- **Step 2:** Key in User ID > Press OK Button > Select Delete
- **Step 3:** Select Delete User, User Role, Fingerprint or Password
- **Step 4:** Press OK Button to delete > Select OK to confirm deletion > ESC to exit.

Display Option

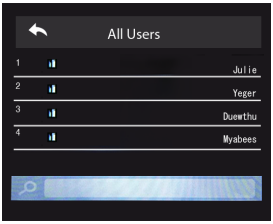
Users can choose the display style of their credentials either to be in. Single Line, Multiple Line & Mixed Line.

The different types of display are shown below:

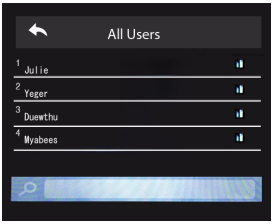
Press Menu > User Mgt > Display Style > Select the type of Display > ESC to Exit



SINGLE LINE



MULTIPLE LINE



MIXED LINE

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.

Define Role

You can define what the administrator is allowed to do at the device. 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

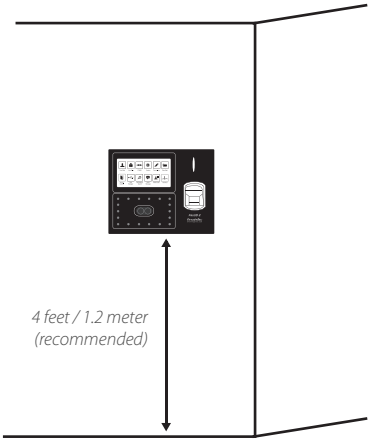
Chapter 4

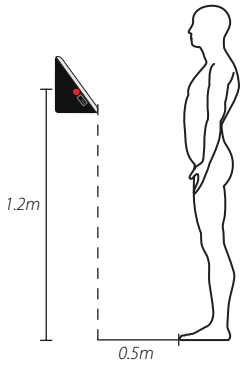
Installations & Communication

Installations

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

Mount On Wall





Installation tips:

Best installation location of Face ID 2 must be

1 - Avoid from direct or indirect sunlight.

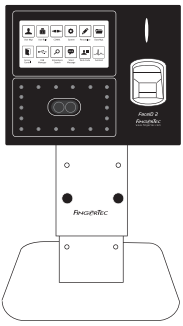
2 - 2 meters away from light source i.e. ceiling flourocent light

3 - Suggested 1.2m from the ground level (measure from ground to the face capturing camera)

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.

DIY Display Stand



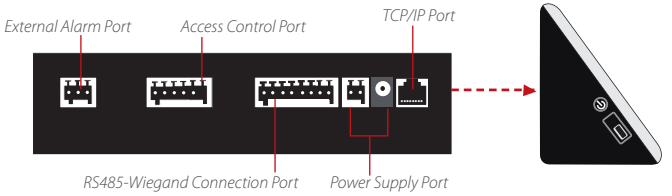
If your Face ID 2 is used for only time and attendance purpose, and not for access control, you may consider this specially designed Face ID 2 Display Stand.

With its DIY concept metal structure, it easily installs your FingerTec Face ID 2 model, adjustable to the desired height for ease of face or fingerprint verification. It is portable too, allowing you to place it anywhere on your reception desk or entrance, the best location to record time and attendance of your staff.

View DIY display stand at *http://accessory.fingertec.com*

Communications

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

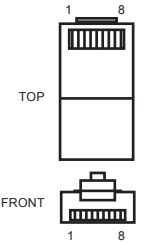


USB Port

Linking with USB flash disk for remote data transfer.

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.

Configure USB Flash Disc

USB drives can be utilized to transfer data between FingerTec devices and software if a cable is unavailable. You can export employees' attendance records (transaction logs) from the device to the USB drive, and import the data from the drive directly to your management software and vice versa.

Download

To copy data from a device into a USB drive. Attach the USB drive to the devic.

To download the data:

Go to Menu > USB Manager > Download

You can select the following data type to copy into the USB drive:

- Download Attendance Data: Download attendance data.
- Download User Data: Download employees' data (face/fingerprint templates, password, card ID, names).
- Download User Portrait: Download employees' photos.
- Download Attendance Photo: Download photos captured while an employee is successfully verified. The photos are in JPEG format.
- Download Blacklist Photo: Download the photo (captured while employee fails to verify at the device) into USB device. The photos are in JPEG format.
- Download Work Code: Download the work code ID.
- Download Short Message: Download the short message.

Upload

Uploading is the process of copying data from a USB drive into a device. The data has to be copied from the software to the USB Drive. To begin uploading your data, connect the USB to your device

To uploading the data:

Go to Menu > USB Manager > Upload

- Upload User Portrait: Upload employees' photos.
- Upload Work Code: Upload the work code ID.
- Upload Short Message: Upload the short message.
- Upload Screen Saver: Upload photos (used as a slide show) in JPEG format into the device. The name of file must start with "ad_" .
- Upload Wallpaper: Upload a photo (used as wallpaper at the main screen) in JPEG format into your device. An example of the file's naming convention - "1-10.jpg".

Download Options

You can configure your device to encrypt data and transaction logs when downloading onto a USB drive to avert alterations made by staff members. Logs can be chosen for deletion after being downloaded into your USB drive to free up disk space.

Go to Menu > USB Manager > Download Options > Press OK to Enter > Select either Encrypt Attendance Data or Delete ATT data > Press OK to either turn the function on or off.

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 > OK to 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

Configure GPRS/3G Connection

FingerTec devices with built-in GPRS or 3G modules can be installed remotely, in the situation where no other forms of connection are available. Devices with GPRS or 3G connections can only be used in conjunction with the FingerTec Webster or TimeTec Cloud server services.

To configure GPRS or 3G:

- **Step 1:** Menu > Comm. > Cellular Data Network > OK to enable the function > ESC to save and exit.
- **Step 2:** Configure the settings

- Cellular Data Network: Enable this to use GPRS/3G
- APN Setup: Access Point Name is the gateway between a GPRS, 3G or 4G mobile network and another computer. You can edit the APN name, dial number, username and password on this tab.
- APN: Access Point Name, used to identify GPRS type
- Dial Number: GPRS Access Number
- Username and Password: To access the network if you have the correct credentials.
- Heartbeat Server: Enter the public IP address of your Webster or TimeTec Cloud server. The device frequently sends status and data updates to Webster or TimeTec Cloud. In the rare case that the connection to the server drops out, the device will perform an automatic restart.
- Details: This includes information about the connected mobile devices such as network mode, Telco operator, IP address and the total data sent and received.

Configure Webster

FingerTec Webster is a web storage application for managing content that are sent from your devices. The contents include information pertaining to user verification credentials, transaction logs and device settings. You will be required to assign an IP address to the server to connect all devices via an Internet connection. The public IP address must be entered into the device to allow a connection.

To configure Webster

Locate the submenu "ADMS". The options within this submenu are used to connect all Webserver settings such as the Webserver IP Address, port and proxy settings.

Step 1: Menu > Comm. > ADMS > Press OK to enable the domain name.

Step 2: Configure all related settings in the page.

- Enable Domain Name: You can access Webster using a domain name in the format of "http://" once you have enabled this function. Alternately, you can enter the IP address to access Webster
- Server Address: Webster's Public IP address
- Server Port: Webster's server port number
- Enable Proxy Server: If you choose to enable this function, you must set the IP address and port number of the proxy server. You may choose to enter the proxy IP address of your proxy server for Internet access.

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.

Configure a USB connection

You can use a USB cable to connect your device directly to a PC. This is similar to a RS232 connection.

To setup a USB cabled connection:

- **Step 1:** Menu > Comm. > Serial Comm > USB > OK to switch it on.
- **Step 2:** USB > Select Yes to enable
- **Step 3:** Configure speed of data transfer at USB Baudrate

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 and 34-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:

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

Step 2: Configure the Wiegand data settings

- Wiegand Format: Select both 26-bits and 34-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 1000
- ID Type: Identifies the content of the data output by Wiegand (Card / Password ID)
- Format Details: Displays information from Wiegand

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.

Communication Key

Since the software is controlled by an activation code and a product key.

Set the COMM key to zero:

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

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 Date
- **Step 2:** Set the Date accordingly.

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

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.

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

Duplicate Punch Period (m)

In the event that you want to consider all clocking activities within the predefined time interval as a single clocking, you can use this setting. For example, if the IN time is 9:00am and the time interval is 15 minutes, any verification done by the same ID within the 15 minutes will be considered as a same record, taking the first time he/she clocks in. The maximum number of minutes that can be entered is 60.

Press the number button to insert the value.

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.

Save Illegal Verification Record

You can set a time range to allow employees to verify for access, for example from 9:00 am to 6:00pm. Employees will be able to verify at the device before and after this time range, but no access will be granted. However the device will record the employees ID and attempted time of access. You can set the device to ignore these records to save storage.

Expiration Rule

You can set limits for the device to verify an employee, either by number (for example 100 times) or specific date (for example 1st of June). Employees exceeding the limit can no longer verify at the device or gain access. You can set the device to take any of the action below when the limit has been reached:

- Keep User, No Audit Future Punch: Device keeps employee data but will not save any attendance records.
- Keep User, And Audit Future Punch: Device keeps employee data and attendance records.
- Delete User: Device removes all employee data

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.
- Fingerprint Algorithm: You may choose to use either VX9.0 or VX10 for fingerprint algorithm.

Note: Both algorithms are not compatible with each other.

- Fingerprint Image: You can select to display or not to display the fingerprint image during verification or enrolment.

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 Status key function. Employees are not required to press any buttons to report their attendance. The screen will not display any Status key
- Manual Mode: By default the device does not display any status key. Press the Status Key to view and select your attendance status. The status key will revert to Check-In mode after an employee has reported their attendance.
- Auto Mode: The Status Key switches to a specified status according to the predefined schedule. Employees cannot press the key to change their attendance status. He/she can only report attendance according to the predefine schedule. You can set the time under Shortcut Key Mapping.
- Manual and Auto Mode: The Status Key switches to specific status according to the predefined time. Employees can verify their attendance without pressing the button. However you are still able to select alternative attendance statuses.
- Manual Fixed Mode: The device tends to show the last attendance status reported by the previous employee, for example Check Out. The employee must press to change to Check-In if he/she reports to start work.
- Fixed Mode: Device will only display a Check-in status. Employees cannot change the status by pressing other keys.

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.

Backup Data

Losing valuable data can be discouraging and damaging. Our FingerTec terminal(s) offer the option of backing up your configurations to a file within the terminal itself, allowing for seamless restorations. However you can choose to save the file onto a USB drive to perform restorations on other terminals.

To initiate a backup:

Go to Menu > Data Management > Press OK to Enter > Backup Data > Press OK to Enter > Select either Backup to Device or Backup to USB Disk > Select the items to be backup > Backup Start

Restore Data

Restore the data stored in the device or from the USB drive:

Go to Menu > Data Management > Press OK to Enter > Restore Data > Press OK to Enter > Select either Restore from Device or Restore from USB Disk > Select the data to be restored > Start Restore

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

- Door Lock Delay(s): This value is the time period for the door to lock again after it unlocks on successful verification. Default value is 10 second and the range is between 1-10
- Door Sensor Delay(s): This function only works if door sensor is available. When a door is not closing for a specified time, the sensor will trigger alarm system. Specify the time of the delay. Default value is 10s, the range is 0-99s. Choose your preference.
- Door Sensor Type: There are two types of door sensor available for door access which are Normally Open (NO) and Normally Close (NC). Once a door sensor is available, you have to choose the door sensor type. Default is None.
- Door Alarm Delays(s): This function only works when there is alarm system installed with Face ID. You can adjust the time before Face ID triggering an alarm system if the door is not closed. A tap on the value will prompt a keypad. Input the value in seconds. The default value is 30s.
- Retry Times To Alarm: When the nummber of failed verification reaches the set value (value ranges from 1 to 9), the alarm will be triggered. If the set value is None, the alarm will not be triggered after failed verification.
- NC Time Period: To set the time period for Normmally 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.
- Valid Holidays: To set if NC Time Period or NO Time Period settings are valid in set holida time period. Choose ON to enable the set NC or NO time period in holiday
- Speaker Alarm: When the 'Speaker Alarm' is enabled, the speaker will raise an alarm when the device is being dismantled.
- Reset Access Settins: To restore access control parameters

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

Access Group Setting

Adding New Access Group

Press Menu > Access Control > Access Group > New Group

- 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
Receipt Printing

You can attach your FingerTec devices to a thermal receipt printer. When an employee reports for work, the terminal will send a ping to the printer to have a receipt printed, consisting of the employees' ID, date and time during the verification process.

Data Field Setup

You can adjust the information that you want to print on a receipt. This function has to be turned on using the Function Tool.

Go to Menu > Print > Press OK to Enter > Data Field Setup > Set the criteria accordingly.

- Company Name: You can choose to disable or enable the display of your company name in the attendance record. Do take note that you have to configure the company name before it can be displayed.

Refer to chapter 4 User Interface on how to set the company name.

- User ID
- Name
- Punch Time
- Punch State
- Device ID
- Print Time
- Work Code
- Verification Mode

Printer Option

To enable printing, select ON. If your printer is equipped with a paper cutting function, turn Paper Cutting ON to automate the service.

Chapter 10

Short Message Display

Displaying public or private short message(s) is a function available on some terminals. Private messages will be displayed at the bottom of the screen only after specific recipients have been verified at the terminal. A mail icon at the top of the screen will appear when a message is available.

Add a Short Message

To enter a short message:

Go to Menu > Short Message > New Message > Message > Enter the message > Press OK to save.

Note: Press * to display the input method. Press # to enter a space between words. Press Esc to exit the input method.

Set the date and time for the Short Message to take effect and expire:

- **Step 1:** Go to Menu > Short Message > New Message > Start Date > Enter the date or press Up/Down Button to select the date > Press OK to Save.
- **Step 2:** Set the start time for the message to begin to take effect.
- **Step 3:** Set the expiry time in minutes for the message to stop appearing in the screen. Range from (1-99 minutes).

Note: Public messages will only be available on screen for the time period as configured in your settings . Press OK to acknowledge the message to return back to the menu. (refer to page 44-message option on how to set the display duration).

Select Message Type

There are 3 types of message that you can set it to.

- Public: Message is viewable by everyone.
- Personal: Message is for designated individuals.
- Draft: You can save the message in draft first before assigning them to public or personal at a later time.

Go to Menu > Short Message > New Message > Message Type > Select the preferred message type > Press OK to save.

Public, Personal and Draft List

View, edit or delete messages in their respective list:

Go to Menu > Short Message > Select either Public, Personal or Draft from the list > Select the appropriate actions.

Note: The operations of the 'edit' function are similar to that of adding a short message (refer to page 43)

Message Option

Set the active duration of a message before it is removed from the screen:

Go to Menu > Short Message > Message Options > Select the preferred delayed time or define it yourself > Press OK to save.

Chapter 11

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 12

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:

All Test

This option will assess the quality of the terminals LCD Display, Voice, Keyboard and Biometric Sensors.

LCD Test

This will perform an evaluation test of your terminals' display by gauging its effects under all colors, including pure white and black. Press OK to continue to the next test or Esc to Stop.

Test Voice

Select this function to ensure the quality of your voice files are clear and complete. Pressing OK to continue to the next test or Esc to Stop.

Test Keyboard

This function tests the keypad on your terminal. Press any key on the keypad to verify the key shown on the display matches your input.

Test Fingerprint Sensor

To determine the condition of the fingerprint sensor, place your finger on the scanner when a white square is displayed. If you are able to see your fingerprint within the white square, your sensor is functioning.

Test Camera

This will determine if the photos taken by the camera are clear and acceptable.

Test Clock RTC

The RTC test will accurately examine the time & date to ensure the time logged is accurate. Click OK to start the test. Every 10ms passed will be displayed as 1s.

Chapter 13

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 4 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.

The LED is Blinking All The Time

You have nothing to worry about unless the blinking light is red. The green blinking light is indicating that the terminal is under its standby mode. Red blinking light may signal problem in the terminal. Contact your reseller for consultation.

"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 5 System under Voice to rectify.

Speaker is damaged
Once you have rectified the voice mode, if the problem persists, proceed to test the voice. Go to Chapter 8 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/*