FingerTec
www.fingertec.com

Kadex+ User Guide

Copyright Notice

Disclaimer

No person should rely on the contents of this publication without first obtaining advice from a qualified professional person. The company expressly disclaims all and any liability and responsibility to any terminal or user of this book, in respect of anything, and of the consequences of anything, done by any such person in reliance, whether wholly or partially, upon the whole or any part of the contents of this book.

TIMETEC COMPUTING SDN BHD

Contents

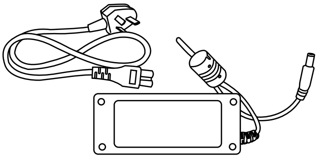
Chapter 1

Getting Started

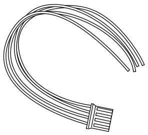
Viewing the User Guide in the Internet

The User Guide is available in the package when you purchase the terminal. The user guide is also available online at https://product.fingertec.com/userguide.php. The user guide on our website will support different languages, so you can also choose and download the user guide based on the language you prefer.

Terminal Included Accessories

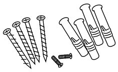


DC 12V Power Adapter

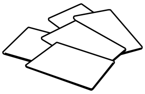


Connection Wires

Screwdriver



A Packet of Bolts



RFID Cards (5 pieces)

ITEM	FUNCTION
DC 12V Power Adapter	*Connect the power adapter to the terminal and plug it into a standard power outlet to power up the terminal.*
Connection Wires	*Connect the wires to door lock, doorbell and RS485, if required*
Screwdriver	*Special screwdriver to install terminal with the backplate.*
A Packet of Bolts	*For the terminal's back plate installation against a wall*
RFID Cards (5 pieces)	*For card enrollment and verification*

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 the Internet. In case you do not have an internet connection, you would need to do offline activation. You can do that by sending the serial number and models of your terminals to your local resellers or *support@fingertec.com* to request 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 24 month warranty protection.

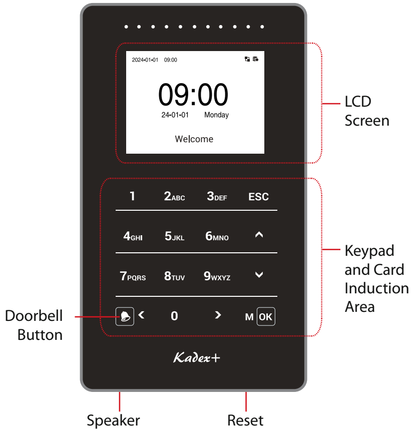
Chapter 2

Basics

Introduction to Terminal

Introducing Terminal, the latest product with Push technology (ADMS). A terminal can be used as both an attendance and access device. All data will be stored in the device and pushed to the server. Kadex+ supports both PC and cloud-based systems. For PC-based systems, Kadex+ will use Ingress AWDMS software as Attendance Mode or Access Mode. For a cloud-based system, Kadex+ instead uses TimeTec Attendance or TimeTec Access. In addition, the terminal accepts card verification as an added security measure. If you are looking for a contactless, hassle-free product, choose Terminal. You are good to go with one look!

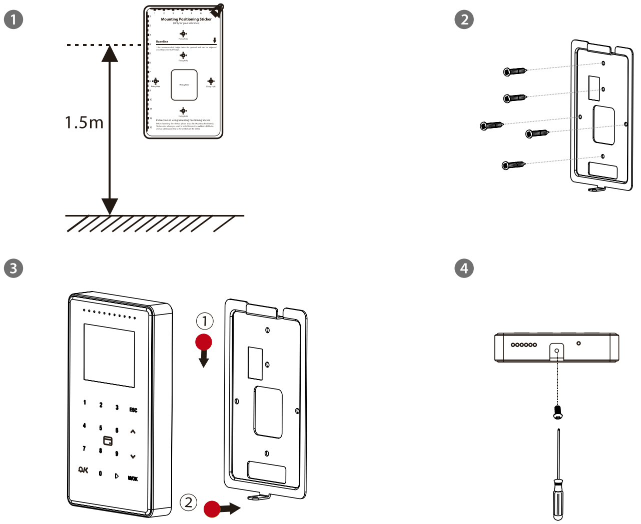
Terminal Overview



ITEM	FUNCTION
LCD Screen	*2.4” LCD screen to display visuals.*
Keypad	*For password verification and navigation on the device.*
Card Induction Area	*Area that reads cards.*
Speaker	*For terminal voice emission.*
Reset	*To restart the terminal as and when required.*
Doorbell Button	*For door bell purpose.*

Installation

FingerTec terminals offer several connections for power and communications. Installing FingerTec's terminals is as simple as ABC.



Firstly, measure the height accordingly and make relevant markings on the wall. Once you have your ideal height, drill the screws into the wall to secure the back plate. Attach the terminal to the back plate following the diagram above and finally tighten the screws.

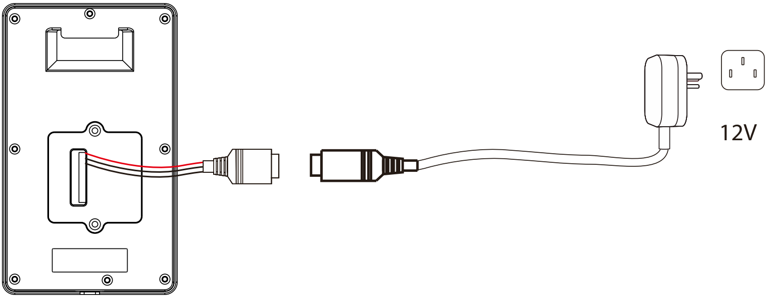
Installation tips:

The best installation location of the terminal should be:

1. Avoid direct or indirect sunlight.
2. 2 meters away from the light source i.e. ceiling fluorescent light.
3. Recommended 1.5m from the ground level.

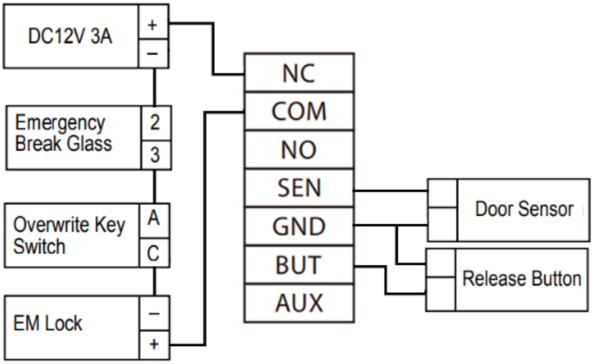
Wiring Diagrams

POWER CONNECTION



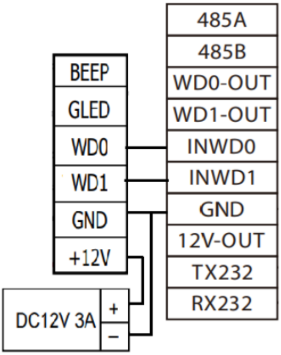
1. Recommended power supply 12V dc 3 A
2. Please use a separate power supply for lock purposes

Emlock, Emergency Break glass, Overwrite Key switch, Door sensor and push button.



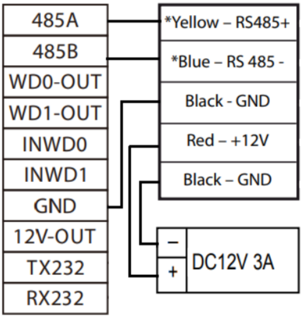
1. 12V Em lock will connect series to device NC and COM, 12V DC supply, Emergency break glass and Overwrite Key Switch.
2. The door sensor and Release Button will connect to SEN and BUT to GND as per the diagram above.

WIEGAND CONNECTION



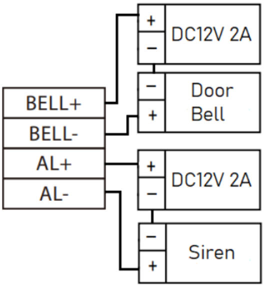
Model k-Kadex & i-Kadex

1. Wiegand connection is used for Slave connection. Fingertec i-Kadex, k-Kadex, or any master reader that supports Weigand Out will support a Master-Slave connection.
2. Kadex + will receive Weigand input as card number or user ID in Weigand 26 – 34-bit format.
3. It is recommended to use a separate power supply for the slave reader to avoid insufficient current supply.



Model R2c & R3c

RS 485 connection (Slave reader)-only for slave readers such as R2c & R3c

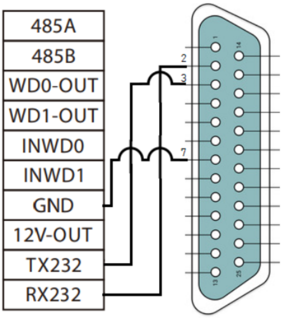


Bell

External Bell Schedule and External Alarm

Printer

1. TX 232 and RX 232 from Kadex + will connect to pin 2(TX232) and pin 3 (RX232) at DB-25
2. GND Kadex + will connect to pin 7 (Signal Ground) DB-25



Battery

Terminals operate using a power supply from a standard power outlet. Inside the terminal, there is an RTC battery to run the internal clock. You are recommended to charge the terminal for at least 3 hours straight before you start using it. When there is a huge delay in time or the clock keeps restarting, it is recommended to replace the RTC Battery. External power supply Mini UPS (uninterrupted power supply) 5V and mini UPS 12V provide mobile power supply to the terminals. Do charge the mini UPS sufficiently for optimum performance.

Refer to *http://accessory.fingertec.com* for more information about accessories.

Cleaning Terminal

To keep and maintain the terminal new, use a dry cloth to clean the terminal's body. Do not use any liquids, household cleaners, aerosol spray, solvents, alcohol, ammonia, or abrasive solutions to clean the body of the terminal as it might damage the terminal.

Restarting and Resetting Terminal

If a feature is not functioning as it should, try to restart or reset the terminals.

Restarting the Terminal: Push the reset button located at the bottom of the terminal to restart the terminal. If you cannot restart the terminal, or if the problem persists, you might want to reset it.

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

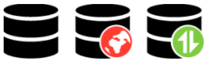
Device Icons

Alarm signal

Triggers when,

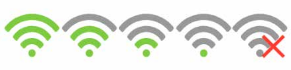
1. The device has been detached from the backplate.
2. The door is forced open.
3. The door did not close after the Door Sensor Delay(s) set amount of time
4. External alarm trigger

ADMS Server connection



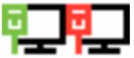
1. Show connected
2. Show disconnected, RED
3. Show data transfer, Green

WIFI Connection Status



1. Connected and signal strength is based on green bars.
2. Disconnected when a red cross is present.

Ethernet Connection

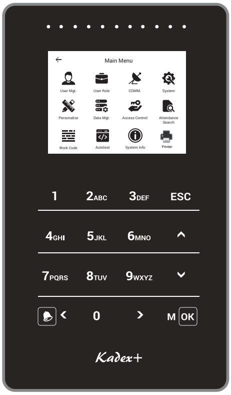


1. Green shows that the connection to Ethernet has been established.
2. Red shows that the Ethernet is disconnected.

Bell

Show when the Schedule Bell is set.

Main Menu



User Mgt
Enroll users/ manage user data.

User Role
Manage Privilege for User roles.

COMM.
Setup Device communication

System
Configure the terminal general to device type setting and reset the terminal.

Personalize
Adjust the User Interface, date/time, Voice, and bell schedule settings of the terminal.

Data Mgt
To delete data, backup and restore data.

Access Control
Configure door access settings in the terminal.

Attendance Search
Check attendance logs for specific users that are available in terminals.

Work Code
Create & manage workcode functionality.

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

System Info
View device capacity, device info, and firmware information.

Printer
Configure printer field and setting.

Chapter 3

Connection

Including Ethernet parameters such as IP address etc., serial Comm, PC connection, ADMS and Wiegand settings.

PC Connection Communication Key

Create a password for a specific terminal here. The security password known as COM Key is intended for extra security. To connect the terminal with the software, 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 > M/OK > Re-type the password > Confirm (OK) to Save > ESC to Exit

Configure TCP/IP connection

Kadex + supports Ethernet and WIFI connections. You need to connect to the network either by Ethernet or WIFI only as they support dynamic and static IP addresses. The default IP address of each terminal is 192.168.1.201.

To set the IP Address

Dynamic IP address: Menu > Comm. > Ethernet > enable DHCP > ESC to Exit

Or can setup a static IP address: Menu > Comm. > Ethernet > disable DHCP > set parameter as per Network required.

IP Address: The default Factory IP Address is 192.168.1.201 so please adjust it according to the actual network situation

Subnet Mask: Factory default is 255.255.255.0. 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 service dynamically allocates IP addresses for clients via server. If DHCP is enabled, IP cannot be set manually.

Display in Status Bar: Select to enable the display of the network icon on the status bar.

Configure WIFI Settings

A wireless connection (Wi-Fi) is available upon request. Kadex+ supports both 2.4 GHz and 5.0 GHz Wifi frequencies.

Only support Wi-Fi password encryption types WPA2PSK.

- **Step 1:** Menu > Comm. > Wi-Fi Settings > enable Wi-Fi connection.
- **Step 2:** Wait for the device to scan the SSID of your Wi-Fi network.
- **Step 3:** Select the SSID of the Wi-Fi network > OK to confirm.
- **Step 4:** Insert the Wi-Fi password > OK to confirm.
- **Step 5:** Select Advanced > disable DHCP > Manual assign IP or use DHCP as default
- **Step 6:** ESC to return to the main menu
- **Step 7:** The Wi-Fi icon appears on the main menu

Configure Cloud Server Connection

This setting is based on your software, either Fingertec Ingress AWDMS or TimeTec solution. Menu > COMM. > Cloud Server Settings

Ingress AWDMS (ATT and ACC mode)

Server mode = ADMS
Enable Domain Name = Disable, the domain name mode http://... will be used, such as *http://www.XXX.com.*

Server Address = Server PC IP Address or domain name installed with the AWDMS

Server Port = 8088(Default Port) - follow setting during AWDMS installation

Enable Proxy = Set the IP address and port number of the proxy server after enabling the proxy (based on server setup)

HTTPS = Enable if required (based on server setup).

TimeTec TA / Attendance

Server mode = ADMS

Enable Domain Name = Enable

Server Address = https://sg-push.zkclouds.com

Enable Proxy = Disable

HTTPS = Enable if required (based on server setup). Not required if https:// is included in the server address.

TimeTec Access

Server Address already predefined when selecting Best Protocol in Device Type Setting

Serial Comm

Serial Comm is used as a bridge between FingerTec devices and the Slave Unit or Printer

Master–slave: Serial port = Master Unit required for R2c, R3c or i-Kadex pairing.

Printer function: Serial Port = Print Function, Baudrate= 9600 – 115200, based on printer setting.

Enabling Wiegand

Wiegand is used as a bridge between FingerTec devices and third-party door Access Controller or connect with Slave Unit. Please disregard this section if you're not using a third-party door Access Controller or Slave Unit.

To configure the Weigand input parameter

🟥 **Step 1:** Menu > COMM. > Wiegand Setup > Weigand Input

🟥 **Step 2:** Configure the Weigand data settings.

Wiegand Format: Values range from 26 Bits, 34 Bits, 36 Bits, 37 Bits, 50 Bits and 66 Bits.

Wiegand Bits: Specify the number of bits occupied by the Wiegand data (based on Wiegand Format)

Pulse Width(us): The default Pulse width is 100 microseconds, which can be adjusted within the range of 20 to 400 microseconds.

Pulse Interval(us): The default value is 1000 microseconds, which can be adjusted within the range of 200 to 20000 microseconds.

ID Type: Select between User ID or card number, it will read the signal as User ID or Card Number

To configure the Weigand Output parameter

🟥 **Step 1:** Menu > COMM. > Wiegand Setup > Weigand Output

🟥 **Step 2:** Configure the Weigand data settings.

Wiegand Format: Values range from 26 Bits, 34 Bits, 36 Bits, 37 Bits, 50 Bits and 66 Bits.

Wiegand Output Bits: Specify the number of bits occupied by the Wiegand data (based on Wiegand Format)

Failed ID: If the verification fails, the system will send the failed ID to the device and replace the card number or personnel ID with the set value.

Site code: It is like the device ID. The difference is that a site code can be set manually, and repeatable in a different device. The valid value ranges from 0 to 256 by default.

Pulse Width(us): The default Pulse width is 100 microseconds, which can be adjusted within the range of 20 to 400 microseconds.

Pulse Interval(us): The default value is 1000 microseconds, which can be adjusted within the range of 200 to 20000 microseconds.

ID Type: Select between User ID or card number, it will send the signal as User ID or Card Number after successful verification.

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 a product key.

Installation and Setup of Ingress and AWDMS

Ingress and AWDMS need be to installed in the same PC and need to fulfil the hardware requirements below.

HARDWARE REQUIREMENT

Operating System: Windows 8, Windows 10, Windows Server 2012 and equivalent

Processor: Intel Core 2 Duo 2.5 GHz or Higher

Memory: Minimum 8GB of RAM or Higher

Refer to the links below for the Ingress and AWDMS installation user guide.

Ingress MySQL Installation Guide: *https://support.timeteccloud.com/portal/en/kb/articles/complete-guide-on-how-to-install-ingress-software-with-mysql-database*

AWDMS Installation Guide: *https://support.timeteccloud.com/portal/en/kb/articles/timetec-awd*

Setup Wizard will require you to do online activation before any connection is established between Ingress and the terminal(s).

Connecting The Terminals to software

The device can connect either to Ingress (AWDMS) or TimeTec solution. Thus, please make sure that you select your preferred Device Type Settings accordingly.

Ingress AWDMS

Example: Local Area Network for the PC installed with the software Ingress and AWDMS.

Server IP Address = 192.168.1.230
Server Port = 8088
HTTPS = no
Proxy = no

ATTENDANCE MODE (ATT)

■ **Step 1:** Device Type Setting (configure manually in the device setting)
Menu > System > Device Type Setting
Communication Protocol = Push Protocol
Device Type = T&A Push

■ **Step 2:** Cloud Server Setting (configure manually in the device setting)
Menu > COMM. > Cloud Server setting > configure the setting.
Server Mode = ADMS
Enable Domain Name = Disable
Server Address = 192.168.1.230
Server Port = 8088
Enable Proxy = Disable
HTTPS = Disable

■ **Step 3:** Ingress Software
Go to Device tab > Add device.
Device Type = Standalone Device
Device Name = Door 1 (Configure your preferred device name)
Communication Key = 0 (Device default value)
Communication Mode = AWDMS ATT
IP Address / URL = 192.168.1.201 (Device default IP Address value)
Serial Number = 1234567 (Configure your device serial number)

■ **Step 4:** Click Add

ACCESS MODE (ACC)

■ **Step 1:** Device Type Setting (configure manually in the device setting)
Menu > System > Device Type Setting
Communication Protocol = Push Protocol
Device Type = A&C Push

■ **Step 2:** Cloud Server Setting (configure manually in the device setting)
Menu > COMM. > Cloud Server setting > configure the setting.
Server Mode = ADMS
Enable Domain Name = Disable
Server Address = 192.168.1.230
Server Port = 8088
Enable Proxy = Disable
HTTPS = Disable

🟥 **Step 3:** Ingress Software
Device > Add device.
Device Type = Standalone Device
Device Name = Door 1 (Configure your preferred device name)
Communication Key = 0 (Device default value)
Communication Mode = AWDMS
Serial Number = 1234567 (Configure your device serial number)

🟥 **Step 4:** Click Add

TimeTec Attendance / TA

🟥 **Step 1:** Device Type Setting (configure manually in the device setting)
Menu > System > Device Type Setting
Communication Protocol = Push Protocol
Device Type = T&A Push

🟥 **Step 2:** Cloud Server Setting (configure manually in the device setting)
Menu > COMM. > Cloud Server setting > configure the setting.
Server Mode = ADMS
Enable Domain Name = enable
Server Address = https://sg-push.zkclouds.com
Enable Proxy = Disable
HTTPS = Disable

🟥 **Step 3:** Add device in TimeTec Attendance
Device > Terminal > Smart DBS (Fingertec) > click + > Insert Serial Number, Terminal ID, Terminal Group, Location, Timezone, Work Location > Click ✓ to save the changes to add the device > Click Refresh to sync device info

TimeTec Access

🟥 **Step 1:** Device Type Setting (configure manually in the device setting)
Menu > System > Device Type Setting
Communication Protocol = Best Protocol

🟥 **Step 2:** Add the device in TimeTec Access
Device > Terminal > Smart DBS (Fingertec) > click + > Insert Serial Number, Terminal ID, Location, Timezone > click + to save the changes > Click Refresh to sync device info

Access point > Manage Access point > Add Location > Assign/Create Building > Create Floor, Upload Floor plan and add Access Points to the respective building.

Assign devices that you prefer to be connected to the specific Access Points and configure the access settings for each access point then save all changes.

Chapter 4

Users

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.

User Role

By default, every user enrolled is a normal user, Kadex + offers three customizable user roles that can be set manually from the device. User role is important to have after the device is added to the software to make sure no unauthorized users are using the device.

Super Admin

At the top of the hierarchy, 'Super Administrators' have full access to all functions. It is compulsory to have at least a user assigned as Super Admin to enable the other user role.

Enroller

The rights of an Enroller are limited only to other enrollers or user add user, data enrolment and device info. The privilege only can be edited by the Super Admin after the Super Admin is assigned.

Normal User

Normal users have no access to any functions within the device.

For the Customizable User role, the permission can be edited according to the Super Admin's requirement.

Define User Role

You can define what the administrator is allowed to do on the device. You will be advised to create a Super Admin after clicking the enable bar. A maximum of three different role sets can be configured.

Menu > User Role > User Defined Role 1> Save > Exit

Enable Defined Role: Enable
Name: Name for User role
Define User Role

Assign Role

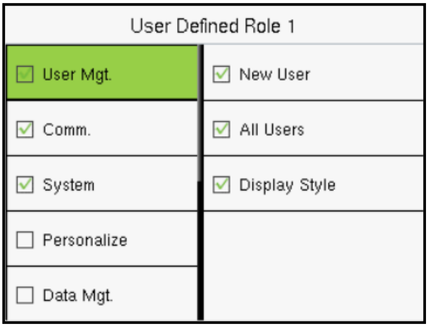
To define the role of new employees

- **Step 1:** Menu > User Mgt > New user > User Role
- **Step 2:** Select the role assigned to the employee > Save the changes.

To define roles for existing employees

- **Step 1:** Menu > User Mgt > All Users > Press M[OK] > Select the User ID > click Edit > User Role
- **Step 2:** Select the role assigned to the employee > Save the changes.

Permission is controlled by menu and submenu items in the device.



User Defined Role 1

☑ User Mgt.	☑ New User
☑ Comm.	☑ All Users
☑ System	☑ Display Style
□ Personalize	
□ Data Mgt.	

User Mgt (Add / Edit and Delete User)

Add New User

It is highly recommended to upload all users from more practical software. When creating a new user manually from the device, 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. You also cannot duplicate ID.

To add user(s)

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

Edit User

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

To edit user information

■ **Step 1:** Press Menu > User Mgt > All Users > find the User ID need to edit by scroll down or search button

■ **Step 2:** Select the User ID > Press OK Button > Select Edit

■ **Step 3:** Select the credentials to be edited > Save and Exit.

Delete User

To delete user information

■ **Step 1:** Press Menu > User Mgt > All Users > find the User ID need to delete by scrolling down or the 'search' button.

■ **Step 2:** Select the User ID > Press OK Button > Select Delete

■ **Step 3:** Select the details to be deleted either Delete User or Delete Card Number Only > click OK to confirm deletion > ESC to exit.

Method of Enrolment

Card Enrollment

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

Follow the steps below to enroll on 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 Number > click Edit > Wave card at the induction area > Screen displays the card ID > Press ESC to save

Password Enrolment

Password verifications have a lessened security presence in Attendance Reporting and Access control systems. Despite this, passwords are generally the primary preference for enrolment. 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 represents 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.

Verification Mode

Security can be enhanced with a terminal which offers the option of using multiple forms of verification methods. Select one of the following five verification modes.

- Password/Card
- User ID Only
- Password
- Card Only
- Password + Card

Chapter 5

System

Setup Date and Time

Menu > System > Date 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 on the home screen. You can choose the date and time format based on your preference.

To set a date and time

■ **Step 1:** Press Menu > System > Date Time > Set Manual Date and Time

■ **Step 2:** Set the Date and Time accordingly.

NTP Server: Enable the device to sync date and time with the NTP server. Users can manually set which NTP server to connect to.

Manual Date and Time: Set date and time manually as per user preference. By default, the device will sync the date and time with the software server time.

24-Hour Time: Select ON to display in 24-Hour format or OFF to display in 12-Hour format (with AM and PM)

Date Format: You can change the date format

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 the 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 on May 3rd at 22:15 hours and end on July 10th at 11:15 hours, 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 Sunday of the 2nd week of February at 1510 hours and ends on the 4th week of May at 1000 hours 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:** et 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 / Attendance Log settings

Press Menu > System > Access Logs Setting / Attendance Log settings

Duplicate Punch Period(m) *Attendance Mode Only: Within a set time (unit: minutes), the duplicated attendance record will not be reserved (value ranges from 1 to 999999 minutes).

Access Log Alert: When the record space of the attendance access reaches the maximum threshold value, the device automatically displays the memory space warning. Users may disable the function or set a valid value between 1 and 9999.

Periodic Del of Access Logs: When access logs reach their maximum capacity, the device can automatically delete older access logs. Users may disable the function or set a valid value between 1 and 999. If set to 100, when the device reaches max capacity it will delete the first 100 logs.

Authentication Timeout(s): The amount of time taken to display a successful verification message. Valid value: 1 to 9 seconds.

Device Type Settings

Please choose a device type according to your needs. You can either choose Fingertec Ingress or TimeTec solutions.

Menu > System > Device Type Setting

Ingress AWDMS (ACC mode)

Communication protocol = PUSH protocol.

Device type = A&C Mode

Ingress AWDMS (ATT Mode)

Communication protocol = PUSH protocol.
Device type = T&A Mode

TimeTec Attendance / TA

Communication protocol = PUSH protocol.
Device type = T&A Mode

TimeTec Access

Communication protocol = Best Protocol
Device type = not required

Reset Options

By resetting the device, you will restore the terminal to its factory settings.

To reset the options setting: Menu > System > Reset > Press OK.

A confirmation window will be promoted before the terminal resets. Kindly confirm and ensure that you are certain of resetting the device 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 9 languages preloaded into your device. Select the language that fits you best.
- Menu Screen Timeout: The device will return to the main screen if you remain inactive in the menu after a certain period. You can set the time duration for the time out between 60s to 99999s.
- Idle Time to Slide Show (s): The device will start to play slide shows (photos) on its screen when it is idle. You can set the idle time duration (range from 3s to 999s) before the slide show starts to play.
- Slideshow Interval (s): You can set the time interval between every image for the slide show. The interval ranges from 0-999s
- Idle Time to Sleep (m): You can set the idle time duration (range from 1 to 30 minutes) to make the device go into sleep mode. Pressing any buttons on the device will wake it and resume operations.
- Main Screen Style: You can select and show the different clock display styles and status keys on the main screen.
- Company Name: For printing purposes ** only available with Print Function*

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 Schedules

You can schedule the device to ring automatically during specific times. This is a reminder to notify employees about the start or end of their working hours or the start or end of the 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.
- Ringtone: Select the bells' preferred ring tone
- Internal Bell Relay: Specifies the time duration for the alarm to ring (ranges from 1s to 999s).
- External Bell Delay: Specifies the time duration delayed for the external 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 **only for ATT mode*

In the event you want your employees to choose an option to confirm his/her attendance status (for example Check-In, Overtime Check-Out, Taking a Break etc) before checking in, you can do so by enabling the punch state options from the device keypad's ESC, ∧, ∨, M/OK, and > buttons.

Here's how to set up the Punch State Mode:

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

- 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 options. The Shortcut Key Mappings menu will also become invalid.
- Manual Mode: Switch the punch state key manually, and the punch state key will disappear after Punch State Timeout.
- Auto Mode: Once this mode has been chosen, set the punch state key's switch time in Shortcut Key Mapping. The set punch state key will be switched automatically when the switch time is reached.
- Manual and Auto Mode: The main interface will display an 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 it timeouts.
- Manual Fixed Mode: The punch state key will remain unchanged until it is manually 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 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 **for ATT mode only*

You can assign five 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.

Here's how to set up the 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.

- Set the Switch Time: The switch time is set according to the punch state options. When the Punch State Mode is set to Auto Mode, users will need to set the switch time.

  On the Shortcut Key interface, tap Set Switch Time to set the switch time.
- Switch Cycle interface: Select the switch cycle (Monday, Tuesday, etc.).

Once the Switch cycle is selected, set the switch time for each day, and tap OK to confirm. If the function is set to Undefined, the device will not enable the punch state key.

Chapter 7

Data Manager

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

Delete Data

[Menu > Data Mgt > 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. Select Delete All or Delete by Time Range when deleting access records. Please ensure to set a specific time range to delete all data with the period if you select Delete by Time Range
- Delete All Data: Delete data related to IDs, passwords, card IDs and attendance records.
- Delete Access Control: Delete the access control setting.
- Delete Admin Role: Removes administrator privileges in your terminal. All employees who had the privilege will revert as normal users.
- Delete Wallpaper: Delete all saved wallpapers. Select Delete All Pictures or Delete Selected Picture
- Delete Screensavers: Delete screensavers. Select Delete All Pictures or Delete Selected Picture

Backup Data

[Menu > Data Mgt > Backup Data]

Back up the configuration data of the device internally > Select the local configuration items to be backed up to the device and save the selected items > Select Backup Start and tap M/OK

Restore Data

[Menu > Data Mgt > Restore Data]

Restore the data stored on the device internally> Select the Restore Data option on the Data Mgt. interface > Select the local configuration items you wish to restore to the device and save the selected items > Select Backup Start and tap M/OK

Chapter 8

Access Control

Access Control Options

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

To set 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. Lock Open duration turns to 1 sec. *Access Mode Only

- Door Lock Delay(s): This value is the time required for the door to lock again after it unlocks on successful verification. Valid value: 1-10s; 0s represent function disabled.
- Door Sensor Delay(s): This function only works if the door sensor is available. When a door is not closed after a specified time, the sensor will trigger the alarm system. This option is to specify the time required. 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 sensors available for door access which are None, Normal Open (NO), and Normal Closed (NC). Once a door sensor is available, you must choose the door sensor type. The default is None.
- Door Alarm Delays(s): When the state of the door sensor is inconsistent with that of the door sensor type, the alarm will be triggered after a time period; this time period is the Door Alarm Delay (the value ranges from 1 to 999 seconds)
- Retry Times to Alarm: When the number of failed verifications reaches the set value (value ranges from 1 to 9 times), the alarm will be triggered. If the set value is None, the alarm will not be triggered even after failed verification.
- Verification Mode: The supported verification mode includes Password/Card, User ID only, password, Card only, and Password + Card. *Access Mode only
- Door Available Time Period: Sets the time when the door is only accessible.
- NC Time Period: Sets the Time Period for Normal Closed mode, no one can gain access during this period. Time Period is Time Schedule
- NO Time Period: Sets the Time Period for Normally Open, the door will be unlocked during this period. Time Period is Time Schedule.
- Master Device: The status of the master can be set to Out or In
- Out: A record of verification on the Master device is a check-out record.
- In: A record of verification on the Master device is a check-in record
- Slave Device: The status of the slave devices. You can set the state of the slave as Out or In.
- Out: A record of verification on the slave device is a check-out record.

- In: A record of verification on the slave device is a check-in record
- Verify Mode by RS485: set the verification method used by R2c or R3c when the device acts as a master reader for R2c/R3c. since R2c / R3c does not support Password, please select Card Only.
- Speaker Alarm: When the 'Speaker Alarm' is enabled, the speaker will raise an alarm when the device is being dismantled.
- Reset Access Settings: To restore access control parameters. However, erased access control data in Data Mgt. is excluded.

Time Rule Settings

Menu > Access Control > Time Rule Settings

Time Rule Setting is the minimum period of access control settings, 50 time zones can be set in the system. Each time zone consists of 7 time period sections (a week), and each time period section is the valid time for access within 24 hours to set up the Time Zone

■ **Step 1:** Tap the input box of the Search Time 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 set the start and end time, then press Confirm (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 the Device's Door is open all day long

Holidays

Add New Holidays

Menu > Access Control > 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 is subject to the time zone set here.

Adding New Holidays

Menu > Access Control > Holidays > Add Holiday

- No. : Holiday ID
- Date: The date of the holiday setting start applies
- Holiday Type: select the access time period that the holiday will use

Edit Holidays

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

Delete Holidays

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

Access Groups *Attendance mode Only

Access Group is used to control users' access time zones, verification method and Holiday validity. When the group verification mode and the user verification mode overlap, the user verification mode takes priority. Each group can set a maximum of 3 time zones; as long as one of them is valid, the group can be successfully verified. The newly enrolled user is assigned to Access Group 1 by default but can be assigned to another access group.

- New Group: setup new group
- All Groups: to view and edit an existing group

Add / Edit Group

- No.: Group number to assign to user
- Verification mode: verification method for all users that follow group verification mode
- Time Period: The time period for group users valid for verification.
- Include Holidays: if enabled, users in the group can open the door only when the group time period overlaps with the holiday time period. If disabled, users in this group are not affected by holidays.

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: The 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 group.

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 groups (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 3 different access groups (group 3, group 5, and group 8).

To delete a door-unlocking combination:

Set all group numbers to 0 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 do not have verification. This setup can make sure that 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 inside and outside of the door. Two devices communicate via the Wiegand signal or RS485. 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:

Menu > 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 the 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 the 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 the record is a checkout; the user can check out if only the last status in the record is a check-in; otherwise, the alarm will be triggered.
- Null and Save: Anti-passback only affects attendance data and not access control *Attendance mode only

Device status and Slave status *attendance mode only
Attendance data from the device and slave reader will be counted as a set
Device status: in or out, Slave status: in or Out

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:

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): The alarm signal will not be transmitted until the alarm delay time has elapsed. Valid value ranges from 1 to 999s.
- Duress Password: Key in a 6-digit Duress password. This duress password will send out an alarm signal whenever a user enters it.

Chapter 9

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

Menu > Attendance Search > 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 a specific date and time at the User Defined > Press OK to see all records.

Chapter 10

Printer ** Upon Request*

Data Field Setup

You can select your preferred data field to be printed out and choose to enable/disable 'Paper Cut' in the printer options.

Menu > Print > Data Field Setup > ON or OFF your preferred field

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

Printer Options

Menu > Print > Printer Options > Enable / Disable Paper Cut

Chapter 11

Work Code **for ATT mode only*

A majority of FingerTec Terminals is incorporated with a feature which allows 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 do not contain any work codes

To add a Work Code:

Menu > Work Code > New Work Code > Key in the Work Code

- ID: Key in your work code ID.
- 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.

To view all work codes:

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:

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 work codes during verification, you must enable the function 'Work Code must be defined'. The terminal will reject work codes it cannot match in its current list

Chapter 12

Auto Test

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:

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

All Test

To autotest whether the LCD, audio, camera, and RTC are normal.

Test LCD

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

Test Voice

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

Test Keyboard

To autotest to examine whether the keyboard/keypad works normally and accurately.

Test Clock RTC

To 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 13

System Info

This option allows you to check your terminal’s storage, firmware, algorithm etc.

To access your system information:

Menu > System Info

Device Capacity

The number of enrolled users, administrators, passwords, cards, and attendance records will be displayed.

Device Info

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

Firmware Info

The Firmware version, Push Service, Standalone Service, Dev Service, System Version, Licdm Service, Mginit Service and Libopts Service will be shown in this section.

Chapter 14

Troubleshooting

Unable to Connect or search for the device

It means that the settings for the terminal and the Server are not properly done or got blocked through the network. Find out which method you are using to connect. The terminal offers LAN, and USB communication methods. Refer to Chapter 3 and Chapter 5 to further understand the topic. You may refer to your local network expertise.

'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 a normal user to access the Menu will prompt an 'Admin Affirm' message on the screen. In case the administrator has resigned from the company, kindly contact your FingerTec authorized reseller to access the terminal.

RFID Card Does Not Respond

Here are the 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 on the card. Refer to Chapter 4 User for card enrolment.

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

Without setting the terminal to show that you are under a group that supports the RFID card, the terminal would not read your card as a registered card.

No Sound

A few things could cause this problem:

The terminal voice mode is silent

Someone might have turned off the voice in your terminal or reduced its volume to 0%. To solve this, refer to Chapter 6 Personalization.

Speaker is damaged

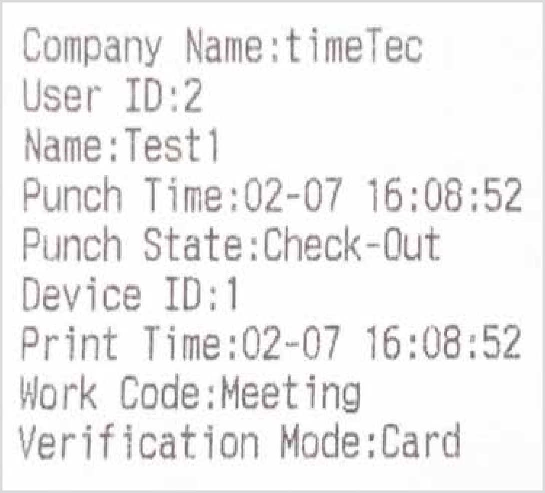
Once you have rectified the voice mode, if the problem persists, proceed to test the voice. Refer to Chapter 10 to do the test. If no voice is being emitted, contact your local reseller for support.

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

Chapter 15

Appendix

Ticket Sample from Thermal Printer – Refer to Chapter 10



```
Company Name:timeTec
User ID:2
Name:Test1
Punch Time:02-07 16:08:52
Punch State:Check-Out
Device ID:1
Print Time:02-07 16:08:52
Work Code:Meeting
Verification Mode:Card
```

timeTec
www.timeteccloud.com