FA600 Series Facial Recognition Terminal

User Manual

Original operating instructions Version 1.1 / 09-2015

EN

General Notice

Although every care has been taken to ensure that this manual is reliable and accurate, Hanvon Corporation (here after referred to as Hanvon) provides it ‘as is’ and without express, implied, or limited warranty of any kind. In no event shall Hanvon be liable for any loss or damage caused by the use of this manual.

This manual describes FA600 facial recognition terminal
in detail and contains full operating instructions.

Hanvon reserves the rights to change the specifications and information in this document without notice. The information contained herein is proprietary to Hanvon. Release to third parties of this publication or of information contained herein is prohibited without the prior written consent of Hanvon.

Copyright © Hanvon, 2015

Content

1. About this document 4

2. Product Features 5

2.1 Appearance View 5

2.2 Installation Guide 6

2.3 Connection Port 7

2.4 Power up terminal 8

3. Operating Guide 9

3.1 Admin. Management 9

3.2 User Management..... 11

3.3 Data Management..... 15

3.4 USB Management..... 17

3.5 System Settings 21

3.6 System Info. 34

3.7 Auto Test..... 35

4. Appendix.....38

Appendix1. Product Specification.....38

Appendix2. Caution 39

1. About this document

Validity

These instructions are valid for the FA600 Facial Recognition Terminal.

Target group

The target group for this document comprises the terminal operator and technical personnel.

Content and purpose

These user manual describe the FA600 facial recognition terminal installation and operation information to users.

Supplementary documents

N/A

Abbreviations

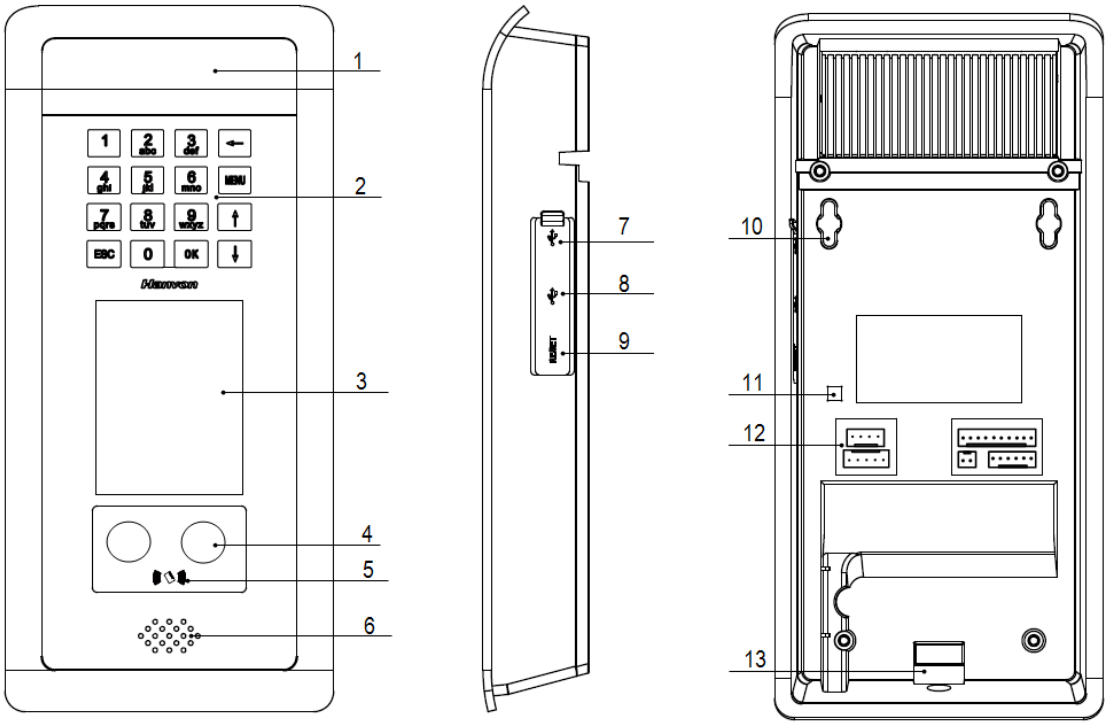
Hanvon	Hanwang Technology Co., Ltd Brand
Face ID	Hanwang Technology Co., Ltd Brand
FA600	FA600 Facial Recognition Terminal

Danger categories and warning symbols

	DANGER
	Danger Operation!
	NOTE
	Application tips, useful information

2. Product Features

2.1 Appearance View



1. LED lights
2. Keypad

   ← key: backplace

   MENU key: enter to main menu

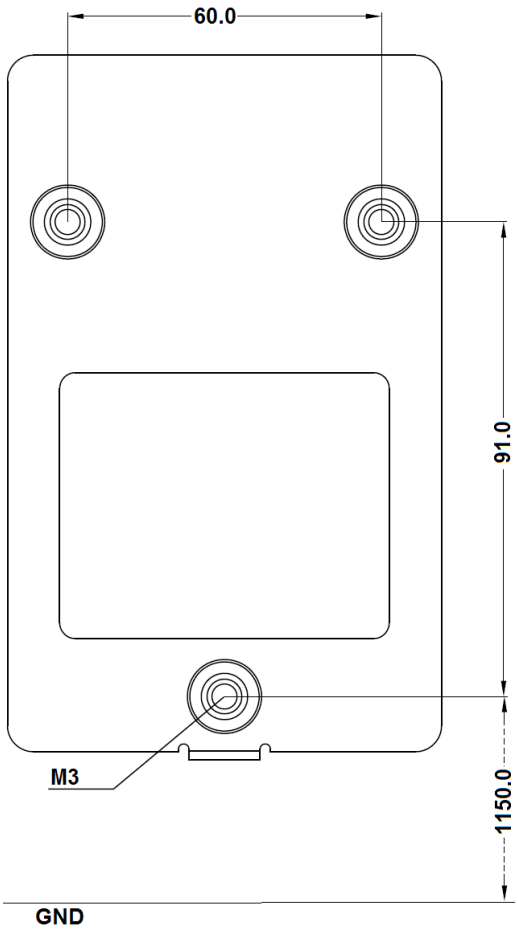
   ↑/↓ key: move to previous or next field

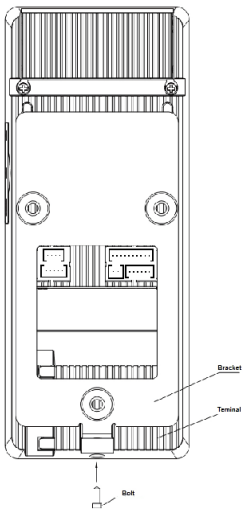
   OK key: confirm current process

   ESC key: cancel current process

3. LCD screen
4. Dual Sensor Cameras
5. RFID area
6. Speaker
7. Mini USB port: factory debugging use
8. USB port(Just for data transmission)
9. Reset port
10. Mounting holes
11. Tamper alarm trigger
12. Terminal blocks
13. Installation hole

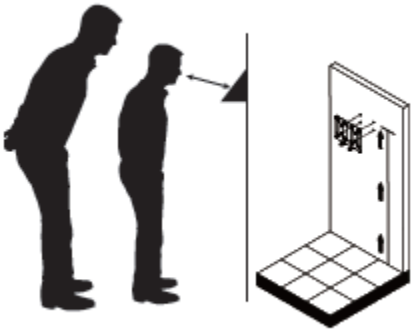
2.2 Installation Guide





User can drill the holes according to the mounting diagram. Use the 3 wall mount, screws to mount the bracket to the wall.

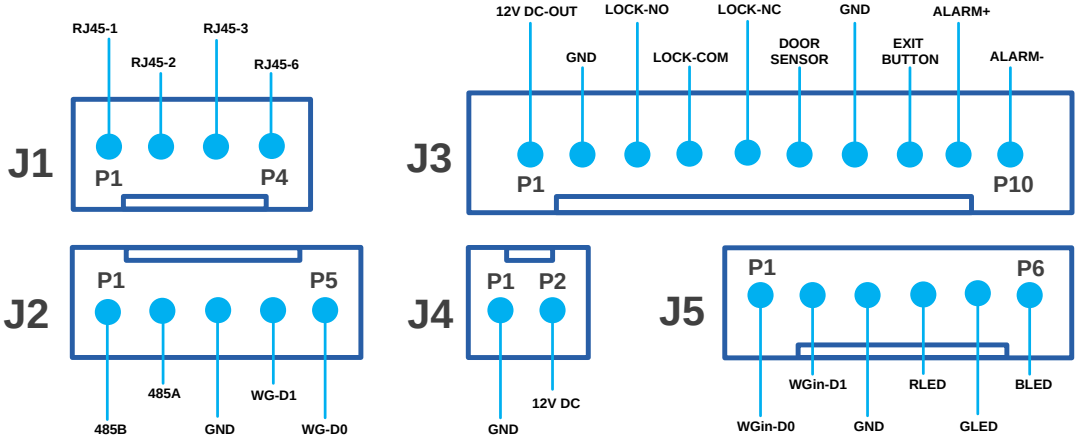
Use the 1 bracket screws on the bottom of the bracket. Be careful not to pinch the AC cord. When finished, plug the Power Adapter into the AC wall outlet.



User also could mount the terminal by choosing your “shortest” users and have them stand in front of the device.

Hold the terminal on the wall that employee can comfortably center their face in the LCD display window.

2.3 Connection Port



PIN	Definition	Feature
J1.1	RJ45-1	Network
J1.2	RJ45-2	
J1.3	RJ45-3	
J1.4	RJ45-6	
PIN	**Definition**	**Feature**
J2.1	485B	RS485
J2.2	485A	
J2.3	GND	Ground
J2.4	WG-D1	Wiegand Output
J2.5	WG-D0	
PIN	**Definition**	**Feature**
J3.1	12V DC-OUT	12V Power Supply (Output)
J3.2	GND	Ground
J3.3	LOCK-NO	Door Lock

J3.4	LOCK-COM	
J3.5	LOCK-NC	
J3.6	DOOR SENSOR	Magnetic Sensor
J3.9	GND	Ground
J3.8	EXIT BUTTON	Door Switch
J3.9	ALARM+	Alarm/Bell Output (Relay2)
J3.10	ALARM-	
PIN	**Definition**	**Feature**
J4.1	GND	Ground
J4.2	12V DC	12V Power Supply (Input)
PIN	**Definition**	**Feature**
J5.1	WGin-D0	Wiegand Input
J5.2	WGin-D1	
J5.3	GND	Ground
J5.4	RLED	Red LED
J5.5	GLED	Green LED
J5.6	BEEP	Buzzer

2.4 Power up terminal

Select a proper language when the terminal boot first time. The terminal will provide several language options for customers:

- English
- Simplified Chinese

3. Operating Guide

3.1 Admin. Management

- **Admin. Management Main Menu**

- If no admin. in system, then press **<MENU>** to enter the main menu.
- If there has enrolled admin. in system, then press **<MENU>** to enter admin. verifying process. While the verification is correct, then the system enter to the main menu.
- Press **<↑/↓>** to move selection to **<Set Admin>**, and press **<OK>** to enter into admin. Menu

Press 1-7 digital buttons on the keypad to enter the corresponding functions directly.

- **Set Admin.**

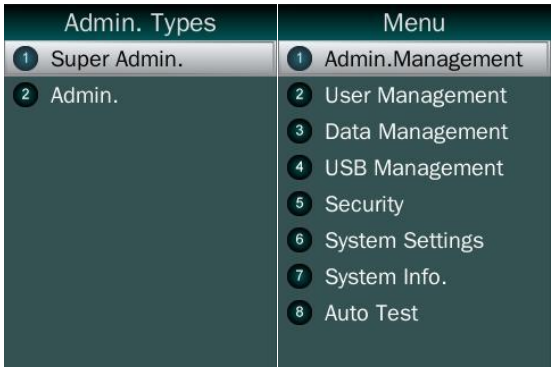
- There are total 8 admin. accounts. A **<Null Admin.>** sign will display for unset admin. accounts. Choose a **<Null>** account to register an admin.

- Input Admin. ID: Input an ID for admin. If the ID is in the database, then the terminal displays admin.'s name.

Admin ID uses natural sequence numbers.
Admin.ID can't be duplicated and start with "0".

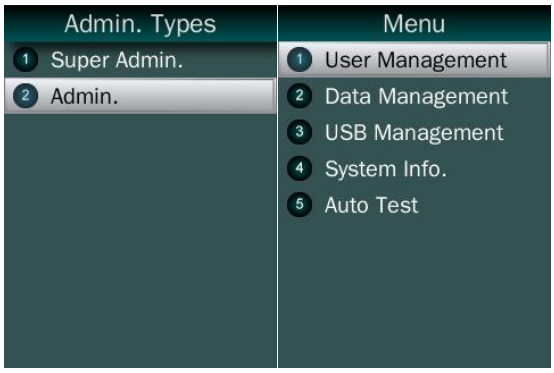
- Input Admin. Name: Press **<MENU>** to switch character inputting mode between **<Upper Case>**, **<Lower Case>** and **<Digital>**.

- **Admin. Types**



- Super Admin. can operate all functions and normal administrators.

⚠ The first administrator must be super admin and can't be deleted in system.



- Normal Admin. can operate User/Data/USB Management function, check system info. and auto test function.

- Verification modes:

ID and Pin: Use ID and password sequentially as a verification method.

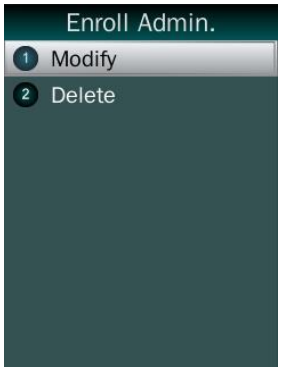
ID and Face: Use ID and face sequentially as a verification method.

Card and Face: Use card and face sequentially as a verification method.

Card: Use card as a verification method.

- **Admin Verification**
  - After set an admin. account, then press **<MENU>** to activate admin verification process.
  - Input admin. ID (or using registered RFID card)
  - Input corresponding password or using face verification, according to the mode during admin registration, after verification is successful, then the system enter to the main menu.

- **Modify & Delete Admin account**

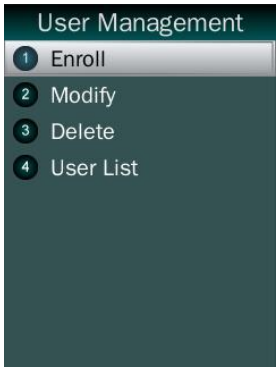


- Select a registered admin. account to modify or delete this account.
- Modify admin. name
- Change verification mode:
- Modify password
- Re-enroll face template
- Re-register RFID card

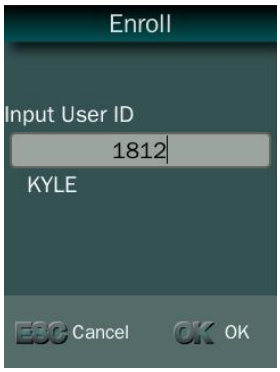
⚠ Delete the certain admin. account: If only one registered admin. account with in the system, then it will be banned to delete.

3.2 User Management

- **User Management Main Menu**



- **User Enroll**



- Input User ID

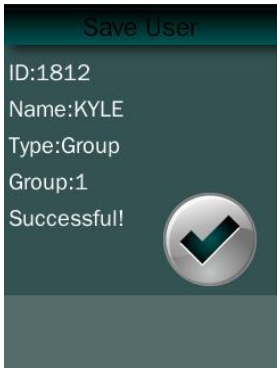
⚠ The range of User ID is from 1-99,999,999,999,999.

- Input name

ℹ Press to **<MENU>** will switch character inputing mode between **<Upper Case> <Lower Case>** and **<Digital>.**

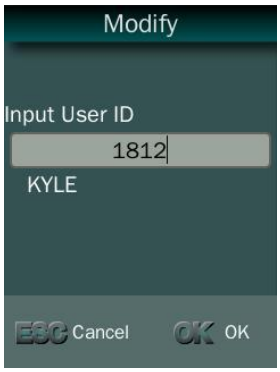
⚠ User Name can contain 18-bit characters totally.

- Select a verification mode
  - **Face:** Use face as a verification method.
  - **Card and Face:** Use card and face sequentially as a verification method.
  - **Card or Face:** Use card or face separately as a verification method.
  - **Card:** Use card as a verification method.



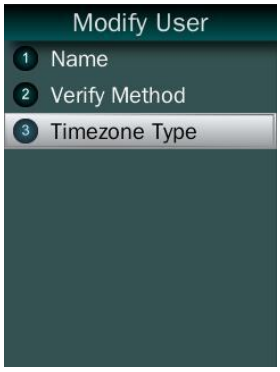
- User registering finished.

- **Modify User**



- Input User ID

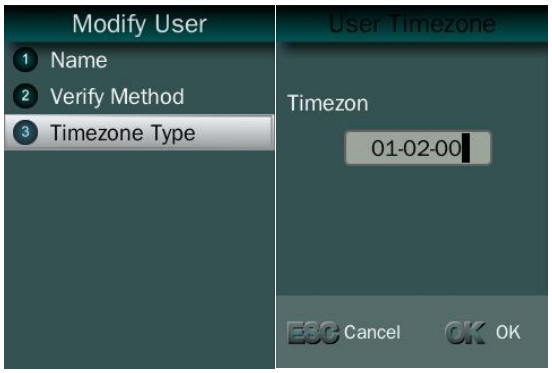
- Following the procedure to change user name, **<Verify Method>** and **<Timezon Type>**.



- Timezone Type includes Group Timezone and User Timezone

- Select a group number for this user

Use **<Group>** function to create group first.

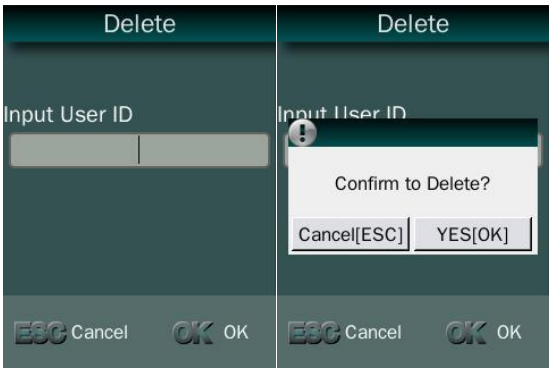


- Select 3 timezones for this user

Each user can set 3 user timezones.

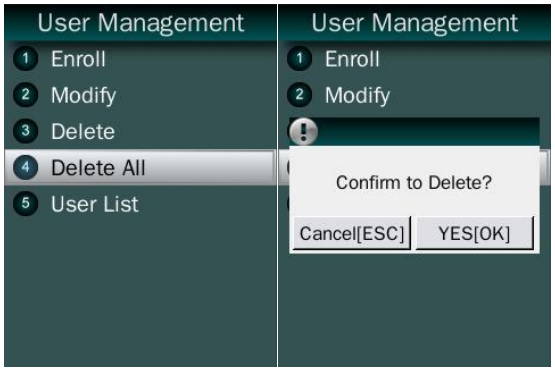
Use **<Group>** function to create group first.

- **Delete User**



- Input an User ID
- Press **[OK]** (or **[ESC]**) to confirm (or cancel) this process.

- **Delete All Users**

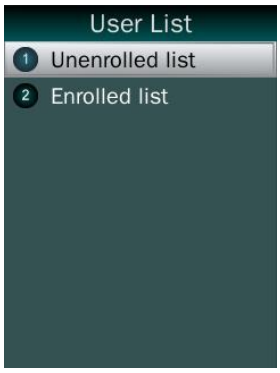


- Press **[OK]** (or **[ESC]**) to confirm (or cancel) this process.

All user's ID, name and templates will be erased.

This step is irreversible. Not affect Admin data and records.

- **User List**



- Enter user list to check Un-enrolled and Enrolled list.
- Press **[OK]** (or **[ESC]**) to confirm (or cancel) this process.

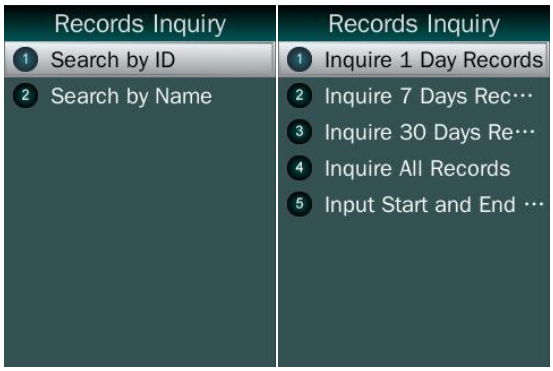
<User List> provides enroll, modify and delete users directly

3. 3 Data Management

- **Data Management Main Menu**

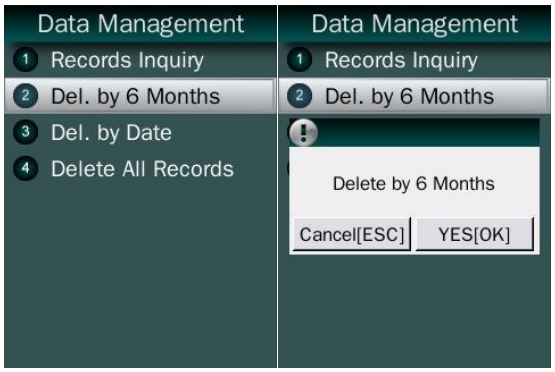
- **Records Inquiry**

- Record Inquiry: User records can be inquiry by User ID/Name.



- Select a search mode to inquiry user records.
- User can view 1 day / 7 days/ 30 days / All records, or all records in indecated periods

Delete 6 Months Records

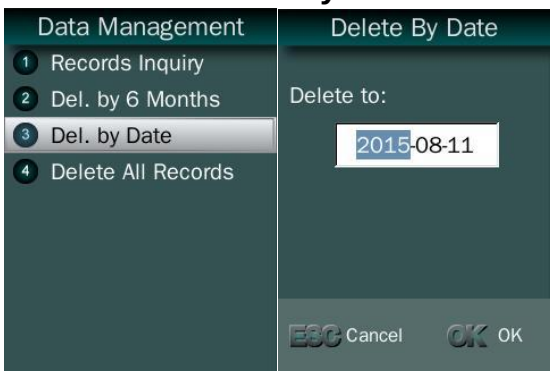


- Del. by 6 months

⚠ Before 6 months records will be erased. This step is irreversible.

ℹ Backup all user data before doing this step.

Delete Records by Date

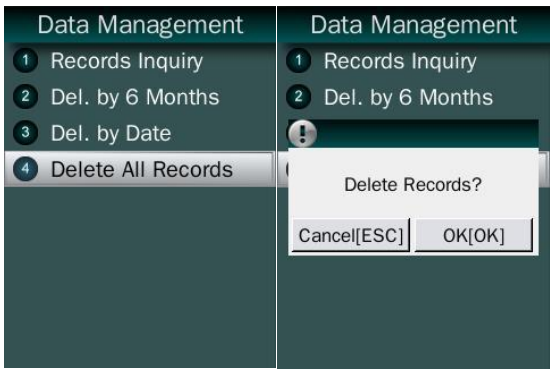


- Del. by Date: Delete all records before indicated date (including this day) .

⚠ All records will be erased. This step is irreversible.

ℹ Backup all user data before doing this step.

Delete All Records



- Delete All Records

⚠ Before 6 months records will be erased. This step is irreversible.

ℹ Backup all user data before doing this step.

3.4 USB Management

- **USB Management Main Menu**

Don't remove USB Disk while data transferring.

Try other USB Disk, if the terminal doesn't recognize it.

- **Export Management**
- **Export Admin**

- Expt. Admin.: Export all admin. data into a file which named as MANAGER.TXT file.

- **Export Part Users**

- Expt. Part Users: Export part user's data into a file which named USER.DAT file.
- Continue to input User ID to add them into the export list.
- Press **<ESC>** to finish adding a user and export all users in export list.

Export All Users

- Expt. All Users: Export data of all users.

Data is stored into a USERALL.DAT file.

Export All Records

- Expt. All Records: Export all user records into a file, which named as **"TIME+SN.TXT"**.

For example, TIME095.TXT, "095" is the last 3 bits of SN of the terminal.

Export Admin. Logs

- Expt. Admin. Log: Export all admin operating logs.

Data is stored into a MANAGERLOG.TXT file.

- **Export Security Photo**

- Expt. Security photos: Set a time duration of exporting security photos

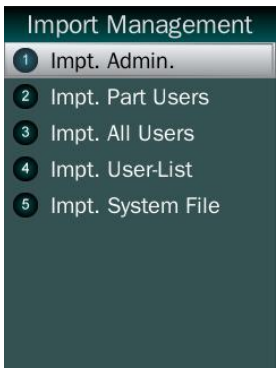
Security photos are saved in security folder

- **Export System File**

- Expt. System File: Export all system settings and parameters

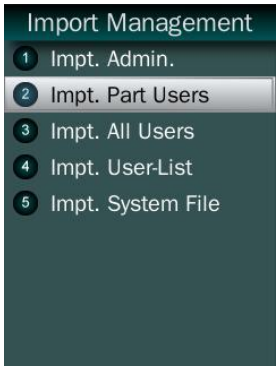
Data is stored into a sys.dat file.

- **Import Management**
- **Import Admin**



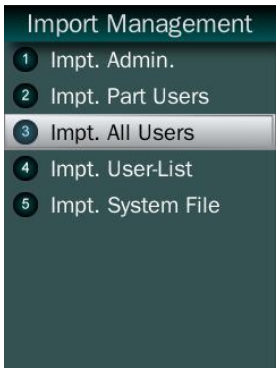
- Impt. Admin.: Import all admin. data from a MANAGER.TXT file.

Import Part Users



- Impt. Part Users: Import part user's data from USER.DAT file.

Import All Users



- Impt. All Users: Import data of all users from a USERALL.DAT file.

Import User-List

- Impt. All Users: Import all ID and name information of users from a USERLIST.TXT file.

The contents of USERLIST.TXT file are list of **<ID>+<TAB Key> + <Name>**.

The range of user ID is from 1-99,999,999,999,999.

Import System File

- Impt. System File: Import all system settings and parameters from a sys.dat file.

Update Wallpaper

- Update the new wallpaper on a terminal.

⚠ 240 * 320pix BMP/JPG file, and named to **<idlepicture.bmp>** or **<idlepicture.jpg>**.

Update Prompt Voice

- Update Successful and Failed prompt audio on a terminal.

⚠ PCM, 16000Hz, 16bit, stereo wave file, and named to **<granted.wav>** and **<deny.wav>**

ℹ Keep audio length less than 1 second.

Firmware Upgrade

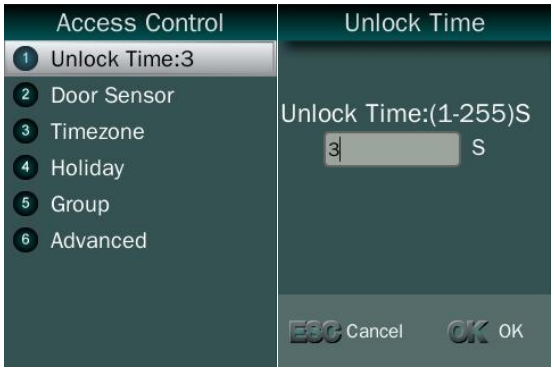
- Upgrade a new firmware for a terminal.

⚠ Firmware files are **<FA600.BIN>** and **<FA600.TXT>**

3.5 Security

- **Security Main Menu**

- **Unlock Time**



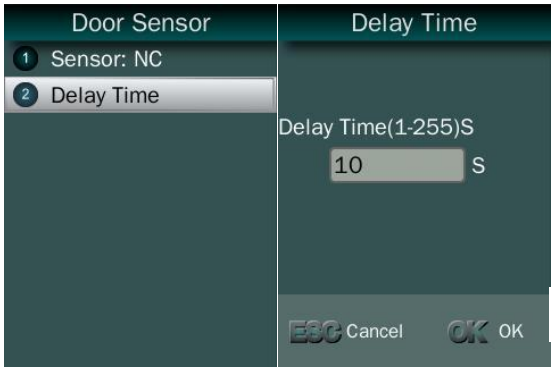
- **Unlock Time:** User can set duration time of unlock.

The default duration is 3 seconds.

The duration range is 1~255 seconds.

- **Door Sensor**

- Door Sensor has 3 status: **None, Normally Open (NO), Normally Close (NC)**

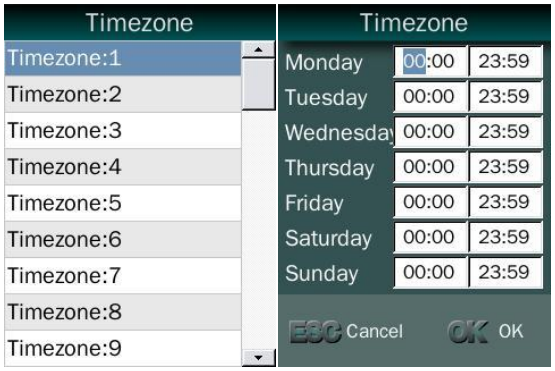


- **Delay Time:** Set a time period for the door sensor. In the indicated period, the sensor will not detect singal.

The default duration is 10 seconds.

The duration range is 1~255 seconds.

Timezone

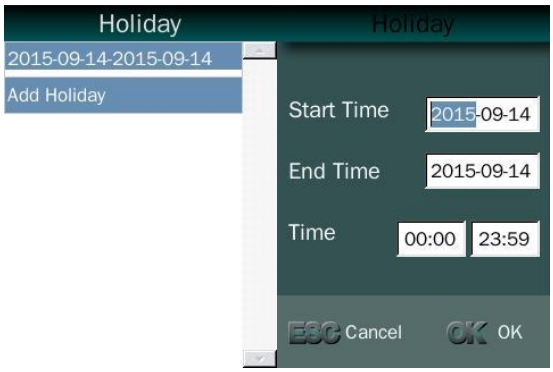


- **Timezone:** limit user access within a indicated period (start time & end time).
- Start time is earlier than end time, then access is granted, for example: 00:00-23:59
- Start time is later than end time, then access is nenied, for example: 06:00-06:00 or 06:00-05:50

Total 50 Timezone can be set.

Each timezone allows user to set for access limitied from Monday to Sunday.

Holiday



- **Holiday:** a special access period which works independently from timezone fucntion.
- Start time is earlier than end time, then access is granted, for example: 00:00-23:59
- Start time is later than end time, then access is nenied, for example: 06:00-06:00 or 06:00-05:50

Total 24 holidays can be set.

Group

- **Group:** each group can set 3 different timezones.
- Holiday can be enable (1) or disable (0) for this group.

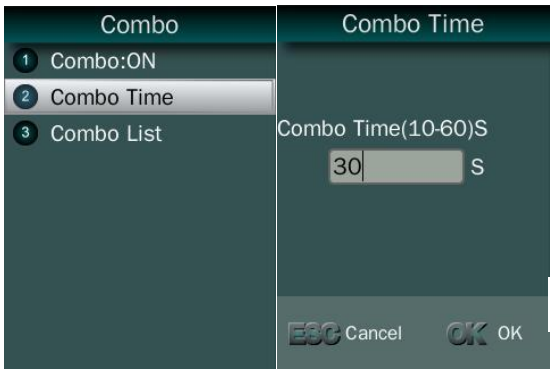
Total 99 groups can be set.

Advanced

- **Combo:** Combination Access, it combines several users from the selected group to gain one access priviliege.
- **Anti-Passback (APB):** check each IN and OUT status and determine an access priviliege for users.

Combo and **Anti-Passback** fucntion cannot be used together.

Combo



- **Combo Time:** a total time for one combination access process. If time is out, the process is failed.

The default duration is 30 seconds.

The duration range is 10~60 seconds.

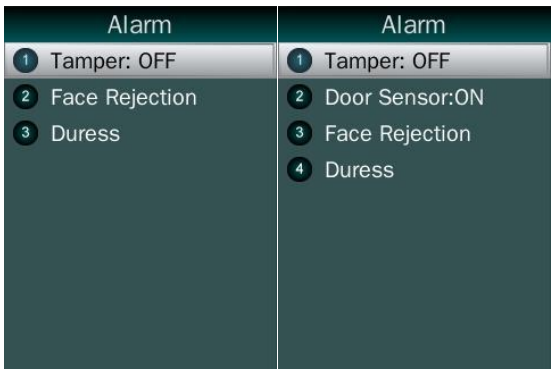
- **Combo list:** Create or modify Combination access group.

Total 10 combo groups.

Anti-Passback (APB)

- **Anti-Passback:** has 4 mode, None, OUT, IN and IN+OUT.
- **OUT mode:** to gain valid and authorized OUT access priviliege, user's previous record must be correct and matched IN access.
- **IN mode:** to gain valid and authorized IN access priviliege, user's previous record must be correct and matched OUT access.
- **IN+OUT mode:** combine both OUT and IN mode together.

Alarm Main Menu



- 4 types alarm: **tamper alarm**, **door sensor alarm**, **face rejection alarm** and **duress alarm**.

Door Sensor alarm will appear only if door sensor turn on in Security setting.

Tamper Alarm

- Tamper alarm is on, the alarm will activate by the tampler trigger on a device

The default is OFF.

Door Sensor Alarm

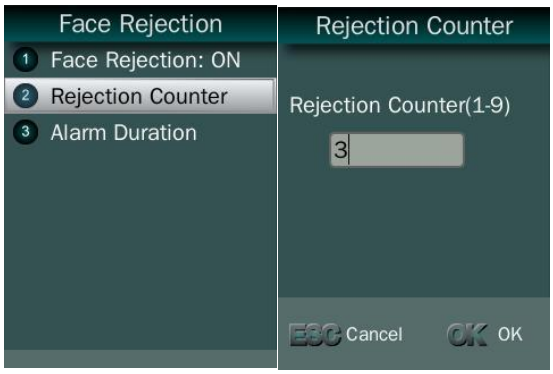
- **Door Sensor** alarm is on, the alarm will activate by the door sensor status

Door sensor funciton can be set in **Security** function.
The default is OFF.

Face Recjection Alarm

- **Face Rejection** alarm is on, the alarm will activate after the verifying rejection of one user exceed limit value.

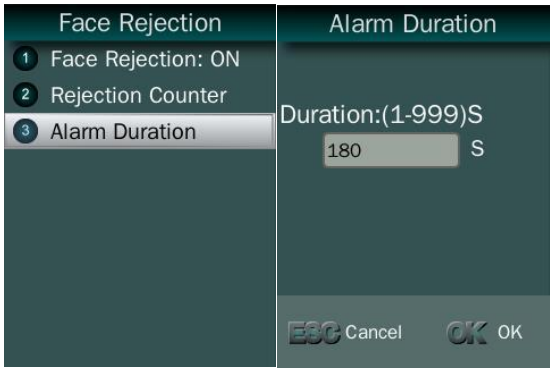
The default is OFF.



- Total rejected verification times

The default duration is 3 times.

The range is 1~9 times.



- Total duration of rejection alarm

The default duration is 180 seconds.
if value is 999, the alarm will alert endless until an admin to operate it.

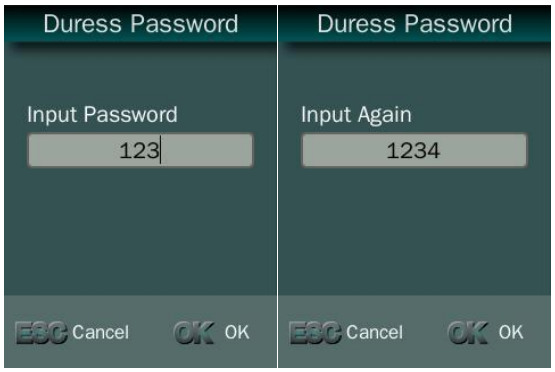
The range is 1~999 seconds.

Duress Alarm

- **Duress** alarm is on, the alarm will activate after a user enter duress password during verficiation.

The default is OFF.

Duress alarm will only provide a signal for the network via SDK. It will not activate alart on device.



- Duress password: a special password for users to enter as they meet threat during verficiation.

The range is 8-bit digitals from 1~99999999.

Duress Workflow

- As Duress function is enabled, the device will ask password (user ID) after each verification.
- Input **User ID** for password, the device provide normal access.
- Input **druess password**, the device sends Alart message via SDK.

3.5 System Settings

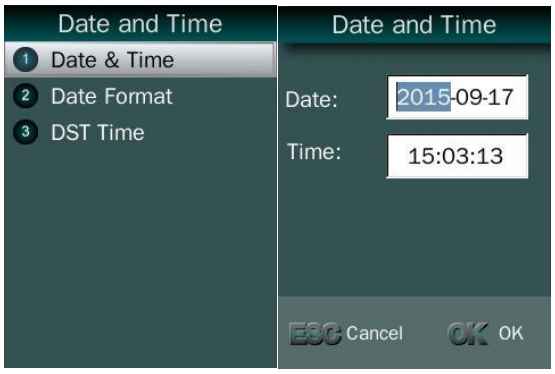
- **System Main Menu**

- **Basic Main Menu**

- **Language**

- English and Simplified Chinese

Date and Time



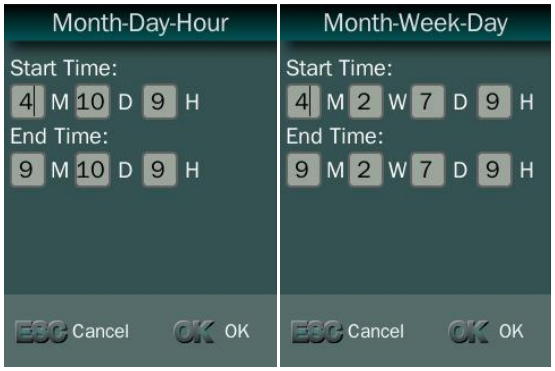
- **Date and Time:** System date and time can be set with this function

- **Date Format:** System date format can be set in 9 formats.

Day-light Saving TIme

- **DST Time:** Set daylight saving time.
- Select proper DST format according to DST rule of your region.

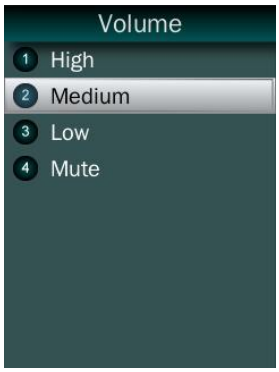
Default is off.



- **Mode1 (Month-Day-Hour):** DST begins with April 10 on 9am, and end to Sept. 10 on 9am.
- **Mode2 (Month-Week-Day):** DST time begins with 2nd Sunday, April on 9am, and end to 2nd Sunday, Sept on 9am.

Mode2: 1D: Monday - 7D: Sunday.

- **Volume**



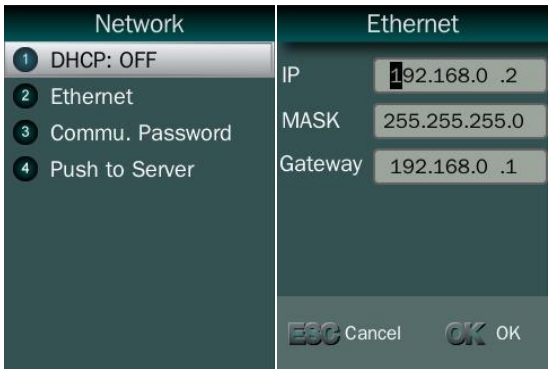
- Set Volume: terminal support 4 modes to customers.

The default is medium.

- **Communication**

- Communication: Network and Wiegand setting.

- **Network**
- **DHCP**



- DHCP turns on, the device will allocate IP/MASK/Gateway automatically from a router. User doesn't need to operate them
- DHCP turns off, user set the IP /MASK/Gateway manually.
- Ethernet: Set IP /MASK/Gateway for a device

- **Communication Password**

- Encrypt commucnication channel by password.

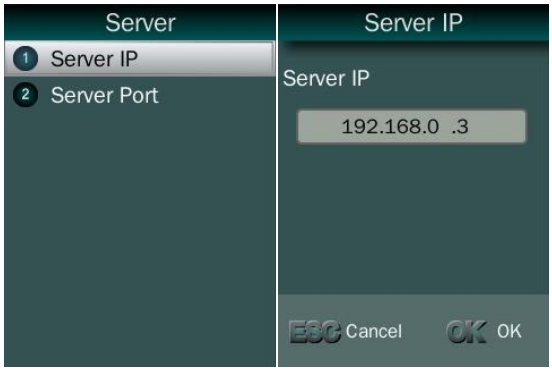
Need software supports as well

Push to Server

- Push to sever Switch: On/OFF

The default is off.

- Record Data Switch: User can select record data/record+security photo data be pushed to the server.



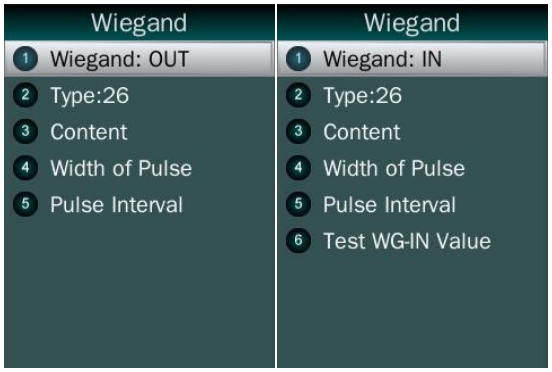
- Server: User needs to set IP address and port of server.

The default IP address is 192.168.0.3.

- Command Port (TCP) is 9920.
- Heart Beat Package Port (UDP) is 9924.
- Heart Beat Package delay is 60 seconds.

The HBP delay range is 10~300 seconds.

- **Wiegand**



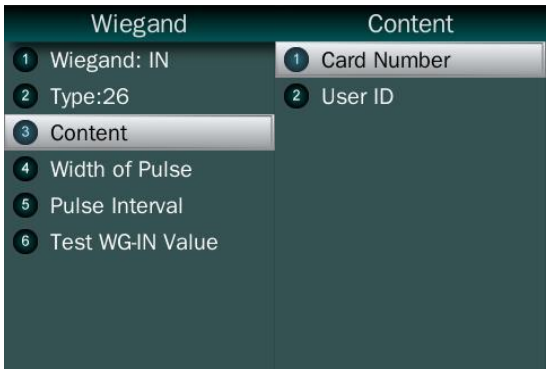
- **Wiegand Mode:** Wiegand OUT and Wiegand IN

The default type is OUT mode.

- **Wiegand Type:** System supports standard Wiegand protocol output on the follow list.

The default type is Wiegand 26.

- **Custom Type:** User can define their own wiegand signal type for a special use.



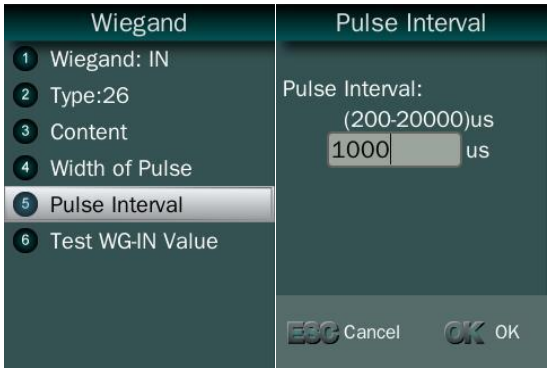
- Content:The user can set Weigand output content with Card ID or User ID.

The default content is User ID.

- **Pulse Width:** Set proper pulse width for wiegand output to match the external wiegand input terminal.

The default Pulse Width is 100 us.

The pulse width range is 20~8000 us.



- Pulse Interval: Set proper pulse interval for wiegand output to match the external wiegand input terminal.

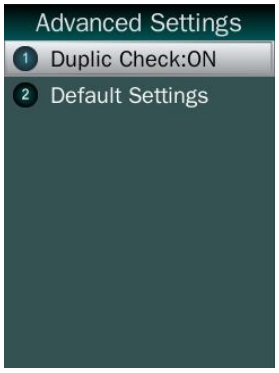
The default Pulse Interval is 1000 us.

The interval range is 200~20000 us.

- WG-IN Monitor: Test wiegand input signal value.

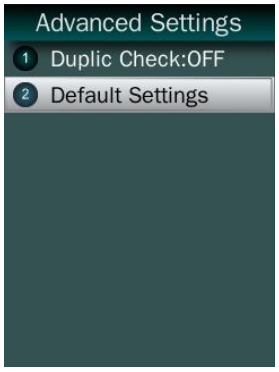
Test WG-IN Value function only appears in Wiegand IN mode.

- **Advanced**



- Duplication Check: System will match new enrolled user with database to check this user already enrolled or not. If system displaying “Similar to ID XX”, admin is suggested to check this user for double enrollment.

The default is OFF.

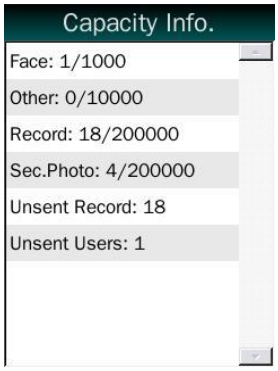


- Default: This operation will delete all data and configurations. And then initialize the device to factory setting.

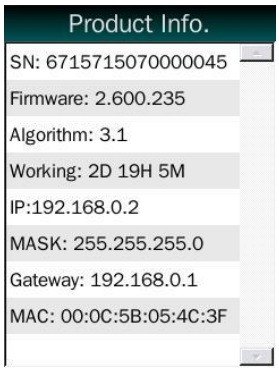
If the administrator **<confirm to default>**, the terminal will be in factory mode!

3.6 System Info.

- **Capacity Info.**



- Face: Current enrolled user numbers and total capacity of user numbers for face related recognition mode.
- Other: Current enrolled user numbers and total capacity of user numbers for card and ID+PIN related recognition mode.
- Record: Current record numbers and total capacity of record numbers.
- Sec. Photo: Current security photo numbers and total capacity of security photos.
- Unsent Records: Unsent record numbers while push to server mode is on.
- Unsent Users: Unsent user numbers while push to server mode is on.



- Product info: SN / Firmware version / Algorithm version / Working Time / IP Address / Mask / Gateway / MAC

4. 7 Auto Test

- Test All: Test all below hardware automatically

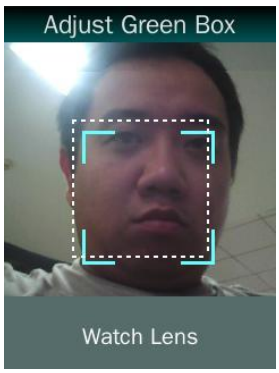
Press **<OK>** if it is working normal

Press **<ESC>** if it is working abnormal.

A list of status will be displayed after all testing.

- Check LCD: Display Red, Green and Blue on the screen

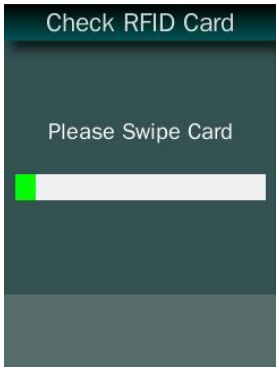
- Check Keyboard: Follow the screen message to check all keys.



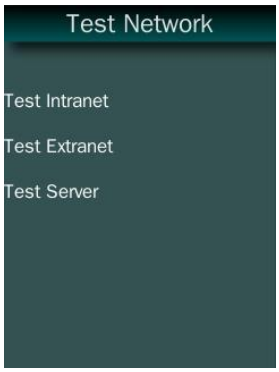
- Check Detection.

- Check Speaker.

- Check Camera.



- Check RFID Cards.



- Check Network.

- Check USB Disk.

5. Appendix

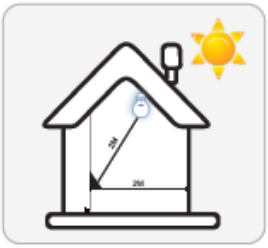
Appendix1. Product Specification

- **User capacity**
  - 1,000 users for face related verification method;
  - 10,000 users for other verification methods including card, card and photo, ID and Pin
- **Record capacity**
  - Data Capacity: 200,000
  - Security Photo: 200,000
- **Verification methods**
  - Face
  - Card and Face
  - Card or Face
  - Card
- **Languages:**
  - English
  - Simplified Chinese
- **Recognition algorithm**
  - V3.1
- **Display**: 3.5 inch TFT
- **Keypad**: 4 * 4 touch keypad
- **RFID card**: Proximity card
- **Communication**
  - TCP/IP
  - USB port
- **Power:** 12V DC, 1.0A (Max. 12V DC, 3A)
- **Environment Light**: 0-5000Lux
- **Working Temperature**: 0°C-40°C
- **Working Humidity**: 20% - 80%

Appendix2. Caution

- **Installation Environment**

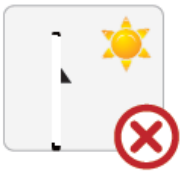
  Terminal should install inside of the room, and make sure the installation place far with the window/door/light more than 2 meters.



Outside of the room

Sunlight directly shines on the terminal through the window.

Sunlight slanted shines on the terminal through the window.



- **Restoration and restart**

  When the system halted and cannot quit, you can remove the adapter to restore and restart the system, or you also can press **<RESET>** to restart the terminal.

- **Restore to default setting**

  Restore all parameters to the default setting.

- **Non-Water proof**

  The terminal is non-waterproof, please keep away from water.

- **Prevent from Falling**

  The parts in this terminal are friable; please prevent the terminal from dropping, smashing, bending and high pressure.

- **Cleaning**

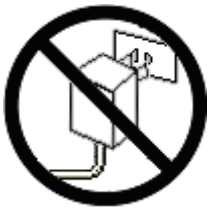
  Please use soft cloth or the other similar material to clean the screen and faceplate, please avoid cleaning with water and cleanser.

- **Low Temperature Environment**

  The working temperature for screen and the main parts in this terminal are the normal

indoor temperature. The performance of this terminal will get worse, if the working temperature extend this temperature range.

Please prevent the screen from oil or any sharp objects.



Please use the equipped adapter for the terminal, the other unknown adapters will burn out

Warning

Any Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.
Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generate, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
—Reorient or relocate the receiving antenna.
—Increase the separation between the equipment and receiver.
—Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
—Consult the dealer or an experienced radio/TV technician for help.
This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment.