Face & Fingerprint Time Attendance & Access Control

Hardware User Manual

Rev: 1.2

Content

Chapter 1 Notice for Using

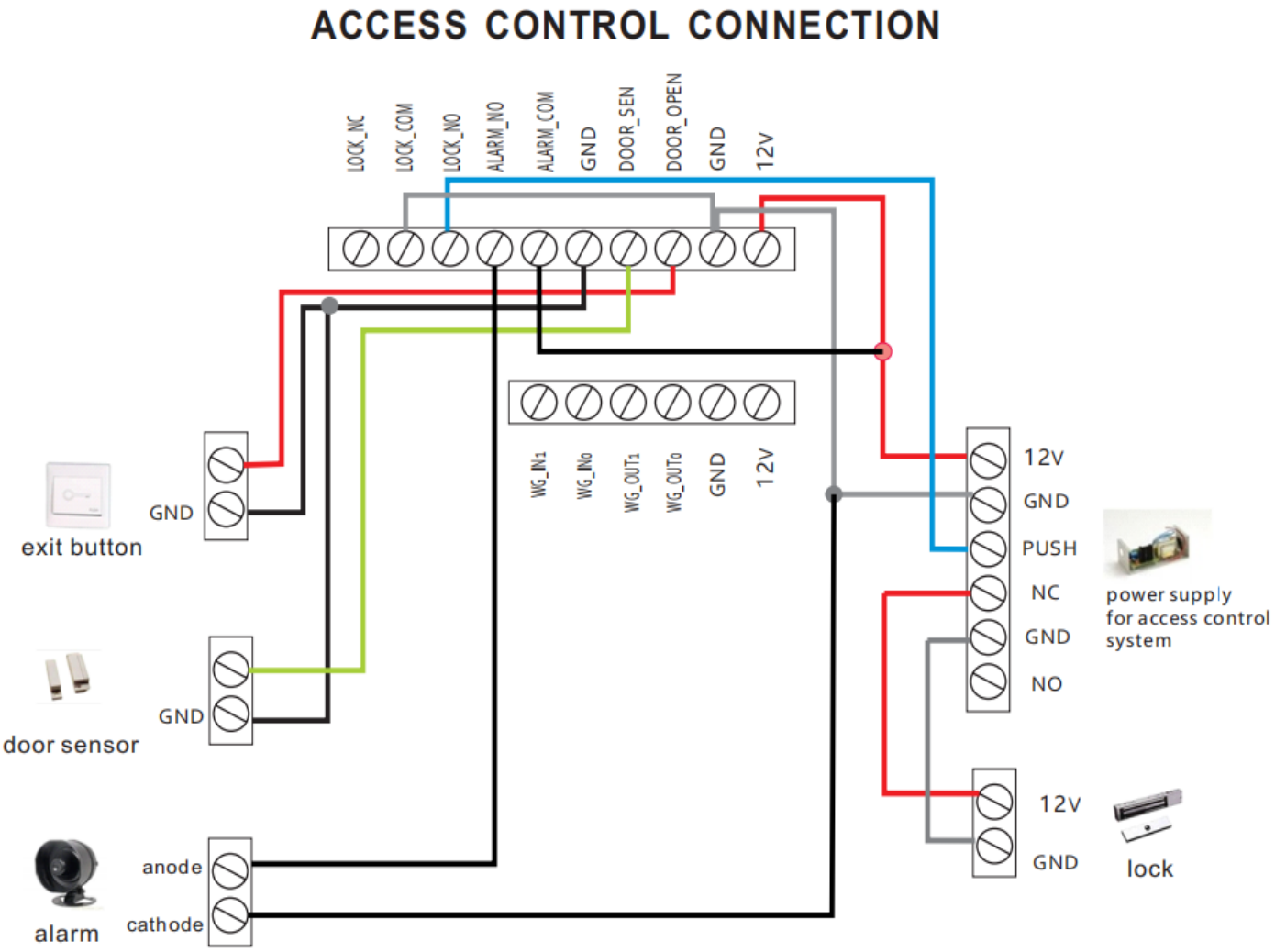
1.1 Operating Environment

- Avoid installing the device at places where irradiated by strong light directly. The strong light affects the collecting of fingerprints that would lead to the failure of the fingerprint authentication.
- The operating temperature of the device is 0℃ ~ 45℃. Avoid using the device outdoors for a long time. The normal working of the Access Control Device will be affected by the long term outdoor usage. It is suggested that using sunshade or cooling equipment in summer and heating installation in winter to protect the device if it is necessary to use outdoor.

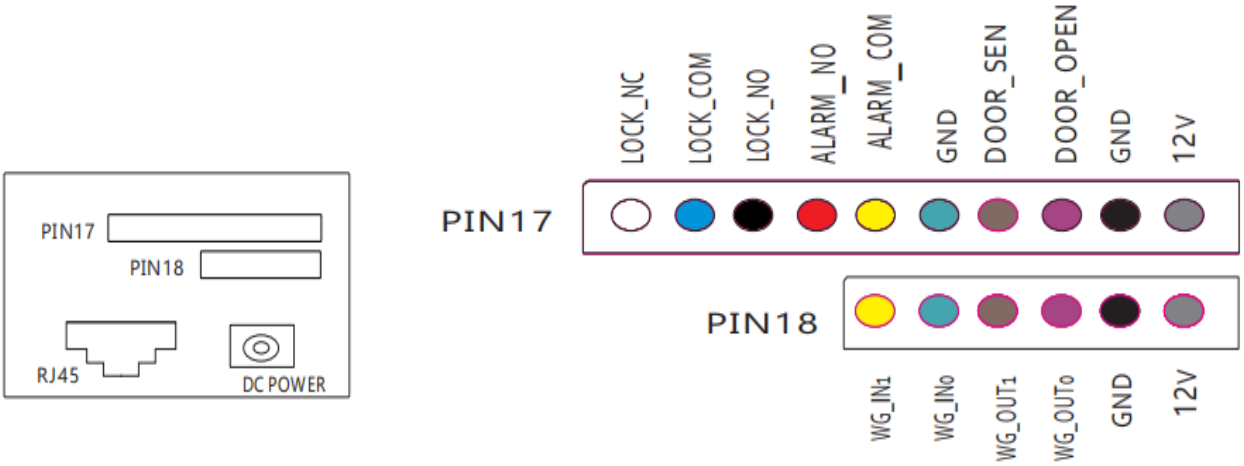
1.2 Notes for Installation

- Please use DC 12V adapter coming with the device.
- Please make sure your power supply is on “OFF” status. Else it may damage the device or the core part of the device if you turn on the power during installation.
- When installing in electrostatic environment or dry weather, please connect to the GND cable first to avoid the device damage from excessive static electricity.
- For all the connection cable, the core should not be exposed more than 5MM. It’s better to use the insulating tape on the connection area, and use different color to differentiate the cables.
- Please connect the power cable after connecting all other cables. Once the device cannot work normally, please cut off the power and check all the connection. Note: all wiring operation with live may lead to device damage. Warranty does not apply under this damage.
- If the device is far from the power supply, please do not connect the device to the power supply with an Ethernet cable. Because the long transmission distance might cause the voltage attenuation.
- It’s recommended to install the device on height of 1.4M - 1.5M.
- Please make sure someone is outside the door during testing the door opening function to avoid any accident that you cannot open the door.
- Please strictly follow this “installation manual. Otherwise, any device damage because of the incorrect wiring is not under the warranty.\

1.3 Connector Diagram



CONNECTION PORTS



Interface	Port	Interface	Port
12V+	DC input	12V+	DC input
GND	Ground	GND	Ground
DOOR_OPEN	Exit button	WG_OUT0	Weigand W0 output
DOOR_SEN	Door sensor input	WG_OUT1	Weigand W1 output
GND	Ground	WG_IN0	Weigand W0 input
ALARM_COM	Alarm input	WG_IN1	Weigand W1 input
ALARM_NO	Alarm output		
LOCK_NO	Normal Open output		
LOCK_COM	Lock power input		
LOCK_NC	Normal close output		

Chapter 2 User Management

Press **[MENU]** to enter the device menu (If manager has been registered, you need to be verified manager before enter the menu) → select **[User]** → press **[OK]** key (or press key **[1]**) to enter the menu.

2.1 Enroll User

Press **[MENU]** key → select **[User]** → select **[Enroll]** → input Enroll ID → input Name and Role → then you can enroll face and fingerprint / password (input password and press **[OK]** key)/ card (present the card) → press **[ECS]** key.

Notice:

For user registration, each one has a unique **ID**, and the **ID** in device has to be the same as that in software.

There are four verification methods: face, fingerprint, RFID card and password.

- **Face registrations:** select registration way as **[face]**, look at the camera to get registered, it takes about 5s and you will hear beep sound after registration successful.
- **Fingerprint registrations:** select registration way as **[fingerprint]**, press fingerprint for 3 times, and you will hear beep sound after registration successful.
- **Card registrations:** select registration way as **[card]**, press **[ok]**, put the card close to device (card sensor), you will hear beep sound after registration successful.
- **Password registrations:** select registration way as **[password]**, press **[ok]**, input password and confirm password, you will hear beep sound after registration successful.

Note:

Manager: can operate all the functions of the device.

When query registered Enroll ID, you just need to input the latest non-zero number(s). For example, the ID is 0000000050, you could just input “50”.

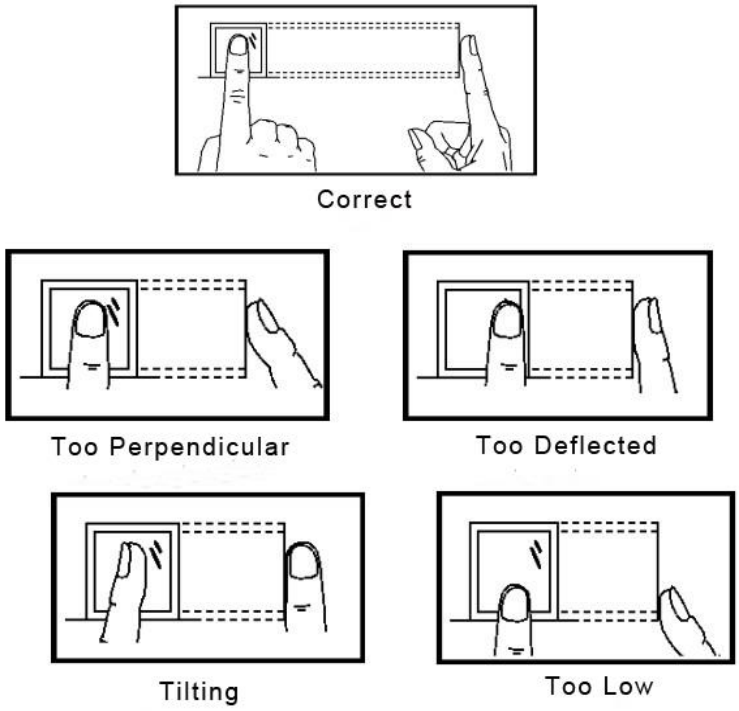
2.2 Delete/ Edit Enroll

Tips: The device has the max capacity for the fingerprint enrollment. When it comes to the max, there is a warning from the device. When the employee left the company, please delete his/her enroll info.

Press **[MENU]** key → **[User]** → **[Del]** / **[Edit]** → press **[OK]** key → input the Enroll ID that you need to delete or edit.

2.3 User Authentication

- **Face:** Keep face within the frame on the screen until device prompts “Success”.
- **Fingerprint:** Verify fingerprint in 1: N mode. Press finger on the sensor correctly. When verify successfully, device prompts “Thank you” and displays “Success” on the screen. If fails, it prompts and displays “Press again”.

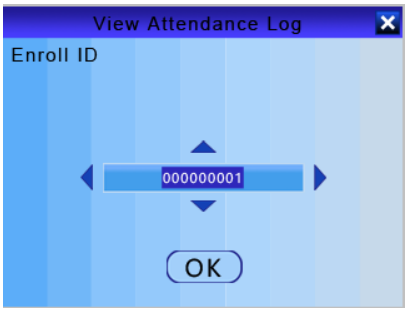


- **Password:** Input the Enroll ID on the main interface → press **[OK]** key → input the password. When verify successfully, device prompts “Thank you” and displays “Success” on the screen. If fail, it prompts and displays “Incorrect password”.
- **Card:** Put the card on the sensing area. When verify successfully, device prompts “Thank you” and displays “Success” on the screen. If fails, it prompts and displays “Invalid card”.

Chapter 3 Data Management

3.1 View Log

Press **[MENU]** key → select **[Log Mgt.]** → press **[OK]** key (or press key **[2]**) → select "View Attendance Log" or "View Admin Log" → input Enroll ID (When the Enrol ID=0, it shows all the users' attendance logs/ all the admins operation logs.)



Description of the Attendance Log

Item	Description	Item	Description
V-FA	Face Verification	**V-F**	Fingerprint Verification
V-P	Password Verification	**V-C**	Card Verification
OI	Over time IN	**OO**	Over time OUT
N	Attend	**O**	OUT
CI	Clock In	**I**	BACK
CO	Clock Out	**U1/2**	Definition 1/2

3.2 Log Settings

Press **[MENU]** key → select **[LogSet]**, you can set re-verification time and delete the logs and user data.

Note:

Item	Description
Re-Verify(Min.）	Time interval for the same Enroll ID to clock in. Default is 3min and the max is 480min. For example, if you set it to 3min, the attendance log only records the first attendance within 3min.
Delete Attendance Log	Delete all attendance logs on the device. Please backup the data by USB flash drive or software before empty it.
Delete Admin Log	Delete all admin operation logs.
Delete Enroll Data	Delete all enroll info on the device, including fingerprints, passwords and so on.

3.3 Log Information

Press **[MENU]** key → select **[LogInfo]** → press **[OK]**, you can view the log information.

- **User**: user amount that already enrolled in the device and user capacity.
- **Admin**: admin amount that already enrolled in the device and admin capacity.
- **Face**: face amount that already enrolled in the device and face capacity
- **Fingerprint**: fingerprint amount that already enrolled in the device and fingerprint capacity
- **Password:** fingerprint amount that already enrolled in the device and password capacity.
- **Card:** card amount that already enrolled in the device and card capacity.
- **Attendance Record:** attendance record amount and attendance log capacity.
- **Admin Record:** admin operation record amount and admin log capacity.

3.4 Auto Status

Press **[MENU]** key → **[Log Data]** → **[Auto Status]** → select the group you need to set →

scroll **[▲]** or **[▼]** key or input number to set the time → press **[OK]** key → scroll **[▲]** or **[▼]** key to select the status → press **[ECS]** key and you could set the next one → all the groups are set → press **[ECS]** key → press **[OK]** key → the time segments saved.

Time Segment is the status (Duty On, Duty Off, In, Over Time In, etc.) shows on the homepage. This status will be along with the attendance records on the software.

Noted:

1. You could set 24 time segments in this device.
2. The status includes User Def1, User Def2, In, Out, Over Time On, Over Time Off, Duty On and Duty off.

Chapter 4 USB Flash Drive

4.1 Download

Insert the USB flash drive → press **[MENU]** key → scroll **[▼]** key or press key **[3]** to select **[USB Drive]** → select **[Download]** → press **[OK]** key, you can download logs and user data.

1. Download Historic Attendance Log

Download all the attendance records stored in the device. There is a folder named "LogData" on the USB flash drive when finished downloading. And there is a file named "HisGLog_0001_20190101.csv", of which is named according to the date you download.

2. Download Historic Admin Log

Download all the admin menu operation logs stored in the device. There is a folder named "LogData" on the USB flash drive when finished downloading. And there is a file named "HisSLog_0001_20190101.csv", of which is named according to the date you download.

3. Download All Enroll Data

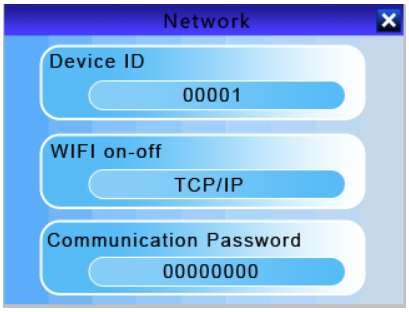
Download all the enrolled information in the device, including all the fingerprints, passwords, card numbers, etc. There is a folder named "UserData" on the USB flash drive when finish downloading. And there is a file named "AllEnrollData.fps.

4.2 Upload

Insert the USB flash drive → press **[MENU]** key → scroll **[▼]** key or press key **[3]** to select **[U-Disk]** → select **[Upload]** → press **[OK]** key, you can upload user data.

Chapter 5 Communication

Press **[MENU]** key → press **[▼]** key or press key **[4]** to select **[Comm.]**.



1. Device ID

Item	Description
1~65536	Set the identification number of the device.
Default	1

Note: Device ID is the unique mark for different devices. When you need to connect more than one device to the software, the Device ID is the unique mark to differentiate the data and records from different devices.

2. WIFI on-off

Item	Description
WIFI on-off	You could set the communication to TCP/IP or WIFI.
Default	TCP/IP

Note: Switch to WIFI → select the WIFI → press **[OK]** key → press **[ESC]** key → device restarts automatically → **[MENU]** → **[4]** key → select “WIFI Name” and input the password → press **[OK]** key.

3. Communication Password

Item	Description
0~99999999	Set TCP/IP communication access password.

Default	0

4. DHCP

When turn on the DHCP, the device will obtain an IP address automatically and you cannot set the IP Address manually.

Item	Description
DHCP	Set if enable the device obtains IP address automatically.
Default	On

5. Local port

Item	Description
1~65534	Set TCP/IP communication port.
Default	5500

Note: When connect the device to the software, you need to input this port No., otherwise, you cannot connect successfully.

6. IP Address

Note: It shows the IP address after the device connected to the network via WIFI or TCP/IP.

7. Subnet Mask

Item	Description
255.255.255.0	Set the subnet mask for TCP/IP communication.
Default	255.255.255.0

8. Gateway

Item	Description
192.168.1.1	Set the gateway for TCP/IP communication.
Default	192.168.1.1

Note: The subnet mask and default gateway must be consistent with those on your local LAN.

9. DNS

Item	Description
DNS Server	Set network address resolution of the device for TCP/IP communication when accessing the external network.
Default	000.000.000.000

10. Real Time Push

Item	Description
Push Function	Set if the device is enabled real-time push.
Default	On

11. Server

Item	Description
Server IP	Set the background address of the device to be accessed during real-time push.
Default	S0.weixinac.com

12. Server Port

Item	Description
Server Port No.	Set the port no. of the device's background address to be accessed during real-time push.
Default	5055

13. P2P Service

Item	Description
P2P Comm. Service	Set if the device enables P2P communication

	service.
Default	On

14. P2P Server

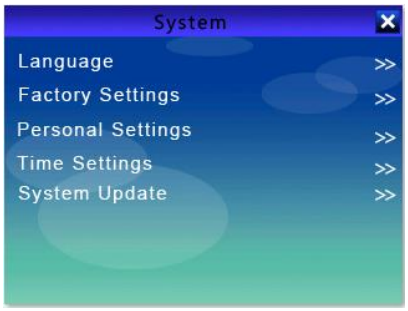
Item	Description
P2P Server IP	Set the address to access P2P server.
Default	Sl.weixinac.com

15. P2P Port

Item	Description
P2P Port No.	Set the port no. of the device's background address to be accessed during P2P communication.
Default	5505

Chapter 6 System Management

Press **[MENU]** key → press **[▼]** key to select **[System]** or press key **[5]**.



1. **Language:** scroll **[▲]** or **[▼]** key to select the language.

2. **Factory Settings:** initializing the device, it will empty all enrollment, records and restore all settings.

3. **Personal Settings**

Item	Description
Volume	Set the volume level of the device from 0 to 6. Default is 3.
Screen Saver Timer	Set time period for the device to enter screen protect state. You could turn it off (default) and set it to 1min, 5mins, 10mins or 30mins.

4. **Time Settings:** set system time and alarm.

5. **System Update**: upgrade firmware of the device via USB flash drive. Before upgrade, please backup all enroll info and attendance records of the device. This action may cause the device clear up all the info on the device.

Attention:

There is risk for upgrade the firmware. Non-professionals are not suggested to operate. Do not unplug the USB flash drive and enter or exit the menu, and make sure power support is consistent while upgrading. Otherwise, it will damage the device and cause failure to boot.

Chapter 7 Access Control

Press **[MENU]** key → scroll **[▼]** key to select **[Access]** or press key **[6]**.

1. Unlock Delay

Item	Description
1~240	You could set the open the value from 1 to 240 seconds. The door locks after this time. When you set it to 0, the door locks immediately when you verify successfully.
Default	5 seconds

2. Check Door Status

Item	Description
On	Check the status of door sensor (turn it on for unlock delay or force open alert).
Off	Don't check the status of door sensor.
Default	Off

3. Lock Control

Item	Description
Lock Control Status	There are three status: Auto, NO and NC.
Default	Auto

4. Tamper Alarm

Item	Description
On	Enable tamper alarm. When turn it on, it displays "Tamper Alarm" on the top left corner of the screen and prompts "DIDIDI" when you don't install the device on the wall.

Off	Disable tamper alarm.
Default	On

5. External Bell

Item	Description
On	Turn it on, the external bell connected to the device will alarm when the internal bell alarms.
Off	Turn it on, only the internal bell will alarm.
Default	Off

6. Wiegand

Item	Description
26	The device outputs data through Wiegand signal interface according Wiegand 26 format protocol.
35	The device outputs data through Wiegand signal interface according Wiegand 34 format protocol.
66	The device outputs data through Wiegand signal interface according Wiegand 66 format protocol.
Default	26

Chapter 8 Device Information

Press **[MENU]** key → press **[▼]** key to select **[About]** and select or press key **[7]**, you can view the device information.

Item	Description
MFRS.	Manufacturer
S/N	Serial number
Date	Date of manufacture
Mac	Media Access Control Address
P2P	P2P No.
Soft	Firmware version
Face count	Face Capacity
FP count	Fingerprint capacity
Glog count	Transaction

Remove Administrator

1. Remove by Software

   It's suggested to enroll at least two admins in the device. When an admin is unable to operate the device, another admin can be verified.

   When the only one admin cannot enter the main menu, please connect the device to the software and cancel the privilege on the software.

   Steps:

   ① Connect the device and PC to the same LAN. (Please choose TCP/IP communication.)

   ② Open desktop software → select [Device Management] and add the device.

   ③ When the device connected to the software successfully, click "Cancel Privilege".

   If the bottom left shows "Operation Complete", the admin is removed.

   ④ If you need you enroll a new admin, please refer to the enrollment details above.

2. Remove by Hardware

   You could remove the admin privilege by pressing a key on the mainboard.

   Steps:

   Turn off the device → disassemble the device →power on → press the button 'DEL_ADMIN' on the mainboard → press 'OK' button.