

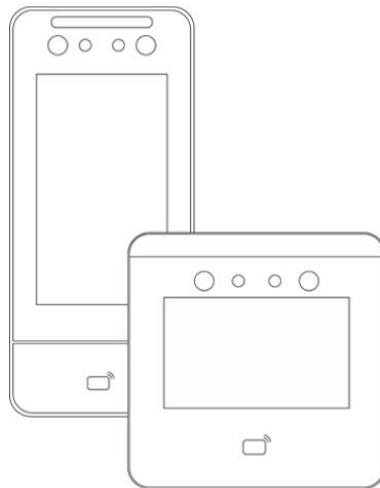


Silicon Wireless Systems Pvt. Ltd.



FACE

ACCURATE IDENTIFICATION



(The image is for reference only)



Quality



Quick



Safety



Accurate



Service

Device usage

1. Entering the menu

Standby screen (Figure 1). Click the bottom-right menu icon to go directly to the menu page (Figure 2). If an administrator is set, administrator authentication is required to enter. 



Figure 1

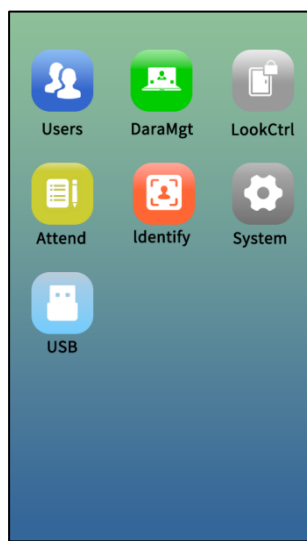


Figure 2 (Standalone)

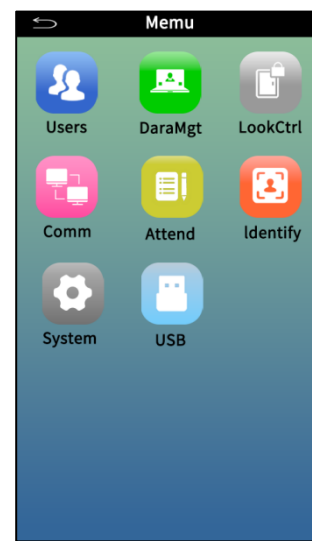


Figure 2

(With Network)

2. User Management

1. Register User

Click **【User Management】** → **【Register User】** to enter (Figure 3),

Number: digits only, up to 8 digits; it is recommended not to modify the default sorting

Name: custom input

Photo: After entering the employee number and name, click the image box to register the user's face. (During registration, please face the camera



Silicon Wireless Systems Pvt. Ltd.

directly and stay still until the prompt indicates successful input; if the capture is unclear, you can click the image box again to re-enter.)

Password: Click the password field to enter the user password, up to a maximum of 6 digits.

Card number: Click the card number area; after swiping the corresponding card, the card number will be filled automatically, or you can enter a phone number as the card number.

Department: Click the department option, select the appropriate department. The default display is empty. For department settings, please go back to the previous menu; refer to 3 for department settings.

Fingerprint: Click the fingerprint area, follow the prompts to register the fingerprint, press the same finger three times.

Palm vein: Click the palm vein area, align the palm with the input box, and register the palm vein.

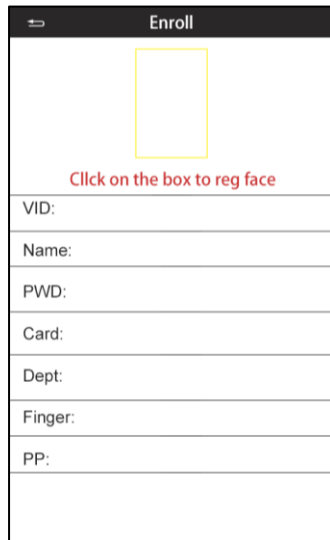
After the setup is complete, click Back to finish user registration.

2. Modify User

Click [User Management] → [Modify User] to enter the user list. Click a user's information to modify the corresponding registration (Figure 4); refer to the operations in user registration for modifications. In the Permissions area you can modify the user's role; selecting Administrator requires administrator verification to enter the login menu.

Validity period: You can set a user's validity period; within the period, access is allowed; outside the period, access is denied.

User search: Modify the user list page, click the top-right of the screen to pop up "" (Fig. 5), click the blank box, input the employee ID or name, and perform a precise search. 

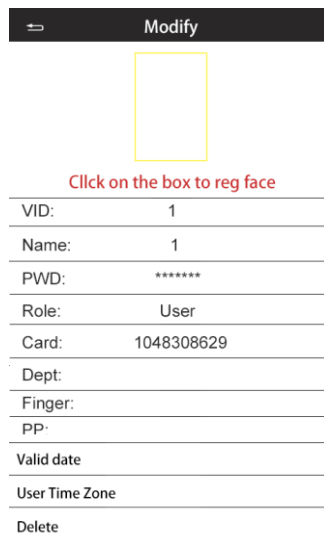


Enroll

Click on the box to reg face

VID:	
Name:	
PWD:	
Card:	
Dept:	
Finger:	
PP:	

Figure 3

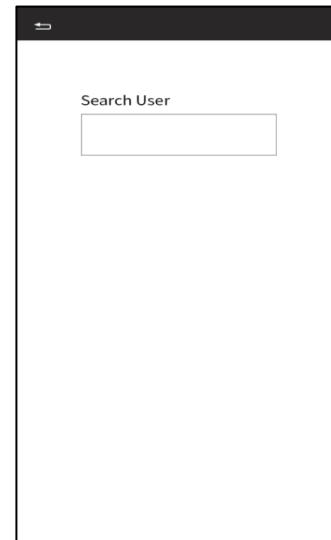


Modify

Click on the box to reg face

VID:	1
Name:	1
PWD:	*****
Role:	User
Card:	1048308629
Dept:	
Finger:	
PP:	
Valid date	
User Time Zone	
Delete	

Figure 4



Search User

Figure 5

3. Department Settings

Department settings are mainly used for attendance reports; up to 16 departments can be configured. Based on the listed department names, click to modify the corresponding department names.

3. Data Management

Click Data Management to view and manage various device data, as shown in the

DataMgt	Reg.Info
Log Info >	Users 0/2000
Reg Info >	Admins: 0/255
Dev Info >	Face: 0/2000
Delete All logs >	Fingers 0/4000
Delete All Users >	Palms 0/500
Delete All Data >	Cards 0/2000
	Passwords 0/2000

4. Access Control Settings

Click [Access Control Settings] to enter the page shown below (Figure 6).

Door opening button: enabled by default; after it is turned off, the door opening button on the device side will not work.

Simultaneous verification count: after setting, multiple users must verify in combination to open the door; up to 10 people can be configured.

Door open delay: after a card swipe to open, the door will re-lock after the delay; the delay is configurable from 0 to 255 seconds.

Wiegand settings: As shown in Figure 7, configure Wiegand input/output signals. Wiegand format options are 26/34, input/output format options are card number/employee ID. Output must be enabled for Wiegand signals to be output correctly.

Door access device status: In/Out

Mask detection: Off by default. When enabled, you must wear a mask to be recognized for opening the door. However, mask recognition is not 100% mandatory; there is still a certain chance to pass when not wearing a mask.

Scheduled door opening: weekly cycle, available from Monday to Sunday. Each day can set three time periods, with options for normally open, normally closed, or closed (online) within the time period.

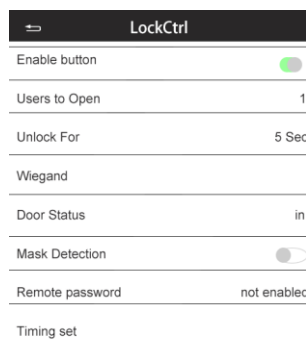


Figure 6

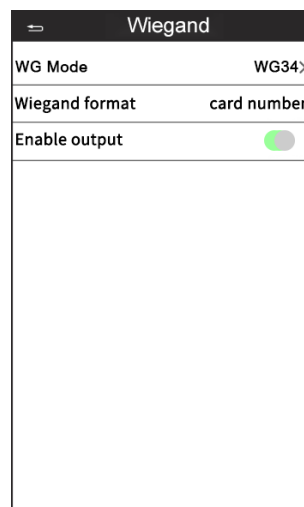


Figure 7

5. Communication settings

Click the menu page [Communication Settings], as shown in Figure 8:

Communication method: LAN / Cloud configuration.

Ethernet: Click "Ethernet" to enter the Ethernet settings screen (Figure 9). Select "Enable" (Ethernet in the ON state). If automatic IP assignment is enabled, the router will automatically allocate an IP address, and you must connect to a router or switch that supports DHCP in order to use it normally; if automatic IP assignment is not enabled, you can freely set the IP address, subnet, and gateway, but they must match the local network to properly connect to the network.

Wireless network: Only models with WIFI capability can be configured. Allow enabling wireless connection, click to select a network, and you can choose to connect to a WiFi network.

Mobile network: Only models with 4G capability can be configured.

Cloud/Cloud configuration: Only cloud models can be configured.

Communication password can only be configured by software; the device only displays it and cannot be modified.

Show IP address: On/Off. If Off, the device screen will not display the IP address.

Network	
Mode	LAN
ETH	192.168.1.18
Wi-Fi	No
Mobile Net.	No
Cloud	
Net PWD	0
Display IP in status bar	☐

Figure 8

ETH	
Enable	☒
DHCP	☐
IP Address	192.168.1.18
Netmask	255.255.255.0
Gateway	192.168.1.1
DNS Server	192.168.1.1

Figure 9

Section 6: Attendance Settings

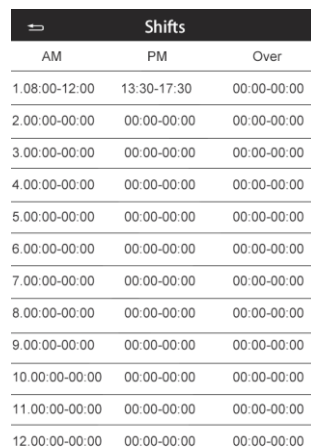
Click the menu page [Attendance Settings] to enter the attendance settings page, as shown in Figure 10,

Scheduling settings: as shown in Figure 11, set the shifts used by employees. Up to 24 shifts can be configured. Shift times are divided into three segments: two segments for normal working hours and one segment for overtime. If normal work uses only one segment, then only one in/out segment needs to be set. The system defaults to Shift 1 for employees. If you need to modify other shifts, you can download the schedule to a USB drive, edit it on a computer, and then upload it back to the device.

Attendance rules: as shown in Figure 12, the permissible time ranges for being late or leaving early.

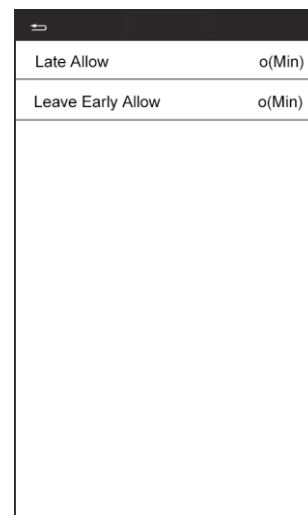


Figure 10



Shifts		
AM	PM	Over
1:08:00-12:00	13:30-17:30	00:00-00:00
2:00:00-00:00	00:00-00:00	00:00-00:00
3:00:00-00:00	00:00-00:00	00:00-00:00
4:00:00-00:00	00:00-00:00	00:00-00:00
5:00:00-00:00	00:00-00:00	00:00-00:00
6:00:00-00:00	00:00-00:00	00:00-00:00
7:00:00-00:00	00:00-00:00	00:00-00:00
8:00:00-00:00	00:00-00:00	00:00-00:00
9:00:00-00:00	00:00-00:00	00:00-00:00
10:00:00-00:00	00:00-00:00	00:00-00:00
11:00:00-00:00	00:00-00:00	00:00-00:00
12:00:00-00:00	00:00-00:00	00:00-00:00

Figure 11



Late Allow	o(Min)
Leave Early Allow	o(Min)

Figure 12

7. Identification Settings

Click the menu **【Identification Settings】** to enter the Identification Settings page, where you can configure various parameters, as in Figure 13,

Confirmation methods: Face/Card/Password/Fingerprint/Palm Vein, Face + Fingerprint, Password + Face/Fingerprint/Palm Vein, Card + Face/Fingerprint/Palm Vein

Repeated confirmation time: default 1 minute; for the same user, only the earliest recognition record is retained within one minute.



Silicon Wireless Systems Pvt. Ltd.

Continuous recognition: On/Off, when enabled, facial recognition, fingerprint, and palm vein can be recognized continuously.

Full record warning: Set this value to emit a warning sound when the record reaches maximum capacity.

Liveness detection: No / Medium / High; If set to No, liveness detection is not enabled, and a photo can pass recognition.

Recognition score: default value 50, adjustable from 30 to 60. Higher score increases security, but recognition becomes more difficult.

Liveness score: default 45, adjustable from 10 to 80. The higher the liveness score, the stricter the check, making recognition harder to pass; please modify carefully.

Recognition distance: default is far; adjustable to far/medium/near.

Enable fingerprint: enabled by default; if turned off, fingerprints cannot be recognized.

Enable QR code / QR code settings: default is off; after enabling, you can use a QR code to scan and open the door.

QR code timeout: duration for which the QR code recognition frame is displayed.

Identify	
Verify Mode	Face/Card/PWD/Finger/pp
Punch Interval	1Min.
Continuous Match	☒
AVL Logs Alert	0
Live Detection	Middle Level
1:N Verification	50
Live detection threshold value	45
Identification Distance	Far
FP Enable	☒
QRCode Enable	☒
QRCode Timeout	20

Figure 13

Section 8: System Settings

In the menu page, click [System Settings] to configure various system parameters, as in Figure 14,

Date and Time: Set and adjust the machine's time; it can also be synchronized via software or automatically synced online.

Display Settings: Screen saver type off/picture; set screen saver time; sleep time; LCD brightness to adjust screen brightness.

Fill light: Off/Auto/Timed/On; Fill light brightness, default 6, adjustable 0~9; Fill light sensitivity default 115, adjustable 80~140.

Sound settings: adjust volume by sliding left and right.

Ring settings: up to 24; preset time and ring count (0~59); when the preset time is reached, a ringing sound is played.

Language settings: Chinese and English can be switched.

Automated testing: infrared camera preview / color camera preview / composite preview / fingerprint camera preview / touch test / LCD test / QR code; for detection only.

Restart the device: reboot the machine.

Factory reset: restores the device to factory settings; users, records, and configured parameters will be erased. Please use with caution.

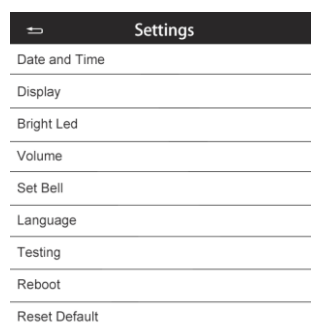


Figure 14

9. USB Drive Function

On the menu page [USB Drive Function], you can upload and download various data from the device, as shown in Figure 15,

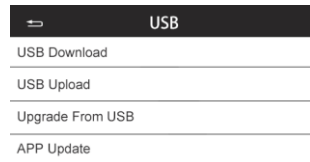


Figure 15

1. USB download

Download report	Download attendance reports. After downloading, the USB drive will contain “X Summary.xls,” which includes five kinds of reports: 1. Summary: It compiles and calculates employees’ monthly attendance information, such as lateness, early departures, and absences. 2. Scheduling information: an employee’s monthly shift schedule, allowing comparison with data in other reports; 3. Anomaly statistics: a per-employee daily anomalies report, such as lateness and early departures; 4. Swipe records: mainly detailed timecard records for each employee; 5. 1, 2, 3 ... : card-type reports, each employee has a
-----------------	--



Silicon Wireless Systems Pvt. Ltd.

	card-type attendance record with detailed punch data.
User download	Download user data to the USB drive for backup to prevent data loss on the machine; it can also be uploaded to another device. After downloading, the USB drive will include the AttendPhoto folder and plu001.dat
Scheduling download	After downloading, you will see “AttendanceSettings.xls,” which contains two types of reports: 1. Attendance settings 2. Scheduling settings The two tables above can be edited and then uploaded to the machine via USB drive for scheduling.
Export user information	After exporting, the USB drive root directory will contain two files: a DCIM folder for storing user pictures, and a user information file, person.xls.

2. USB drive upload

User upload: You can upload user data downloaded from the machine to a new machine, avoiding re-entry. Scheduling upload: You can upload the edited scheduling table downloaded to the machine for scheduling.

User information import: You can import the exported user data into a new machine; you can also use this function to quickly register users in bulk without going to the machine. Use the exported user information as a template, place the pictures in the DCIM folder as required, edit the person.xls table with user information, and import.

3. Firmware upgrade: Used to upgrade firmware.

Steps:

① Copy the firmware that needs upgrading to the root directory of the USB flash drive.



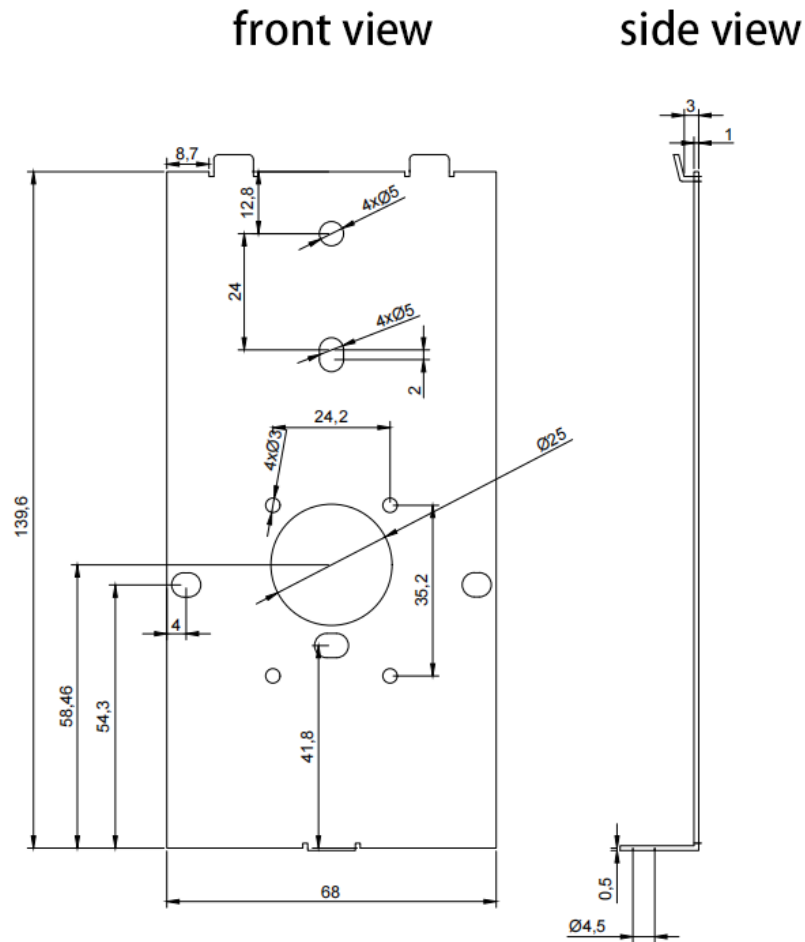
Silicon Wireless Systems Pvt. Ltd.

- ② Insert the USB drive into the device's USB port;
 - ③ Click "Menu" → "USB Function" → "Firmware Upgrade" → "OK";
 - ④ After the upgrade is complete, the device will reboot automatically.
4. App upgrade; use to upgrade apps.

Note: The above device function menus are for illustration only; the actual functions available depend on the device display.

DimensionsFi

4-inch by 5-inch facial recognition wall-mount bracket size (there may be some deviation; please refer to the actual product for details)



Installation

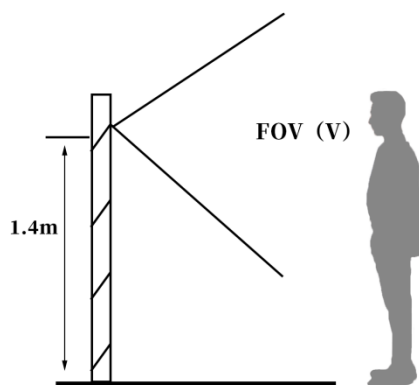
The device should be installed away from backlight, side light, and direct strong light as much as possible

The recommended mounting height h is about 1.4 m (distance from the lens to the ground). At this distance, the identifiable height range at 0.5 m from the device is 1.3 m to 1.7 m; at 1 m distance, the identifiable height range is 1 m to 2 m (there may be some deviation). You may also adjust the installation height according to your actual use

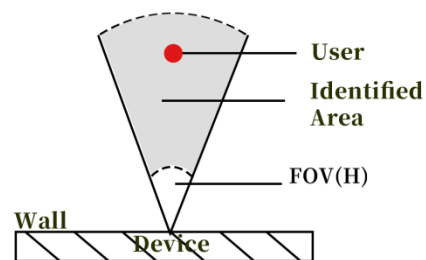
To ensure fast and accurate authentication, 0.4 m from the device is ideal for person identification (range 0.3 – 0.5 m), and registered facial

photos should have at least 100 pixels; the illuminated intensity on the recognized face (Luminosity) should not be lower than 30 Lux. The device has a built-in fill light; when the device is in a relatively dim environment, the face illumination at 0.5 m from the device is about 100 Lux, and the closer the distance, the higher the facial illumination. If facial exposure is too high, feature points may not be extractable, making recognition more difficult

Camera vertical wide-angle



Camera horizontal wide-angle



Installation Steps

Wall-mounted installation steps:

1) According to the bracket specifications, drill three screw holes at an appropriate position on the wall. If the wall is a hard base wall, use the expansion screws in the accessory pack. Then align the three holes on the bracket with the holes on the wall, and fasten the bracket to the wall using the screws from the accessory pack. Before fixing the bracket, route the wiring from the bracket's outlet or bring it out from the equipment edge. See the figure below.

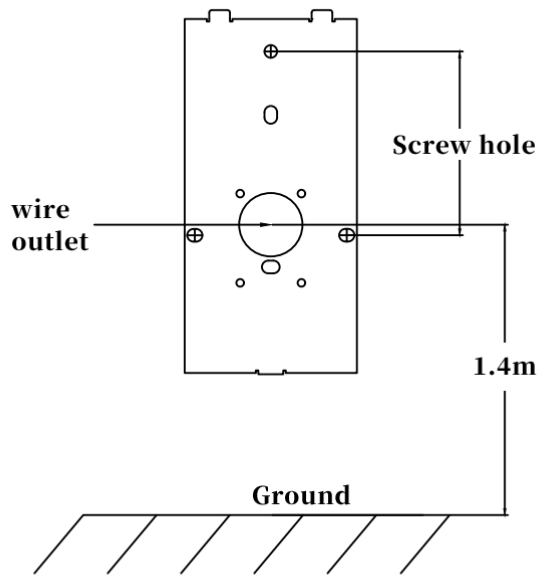


Figure 1

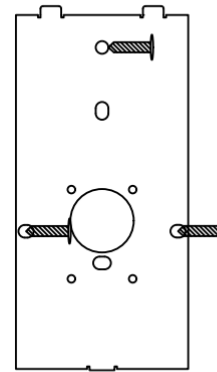
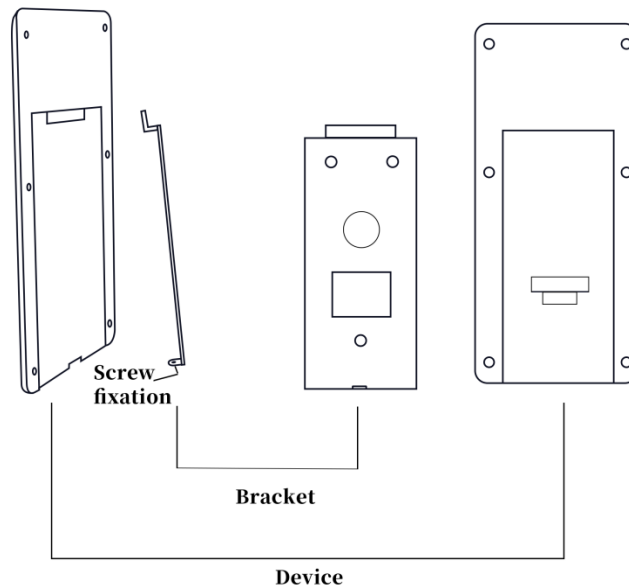


Figure 2

2) Insert the tail lead into the terminal strip, then align the bracket with the groove on the facial recognition device and snap it in. Align the bottom of the bracket with the screw holes at the bottom of the facial recognition device, and tighten the screws in a clockwise direction to complete the installation.



Installation and usage precautions:

1. Install the device in a place where it is least affected by light sources.
2. Adjust the recognition threshold appropriately according to usage to achieve better recognition performance.
3. The actual wiring should use suitable cables according to the distance to ensure the device is supplied with the correct voltage.

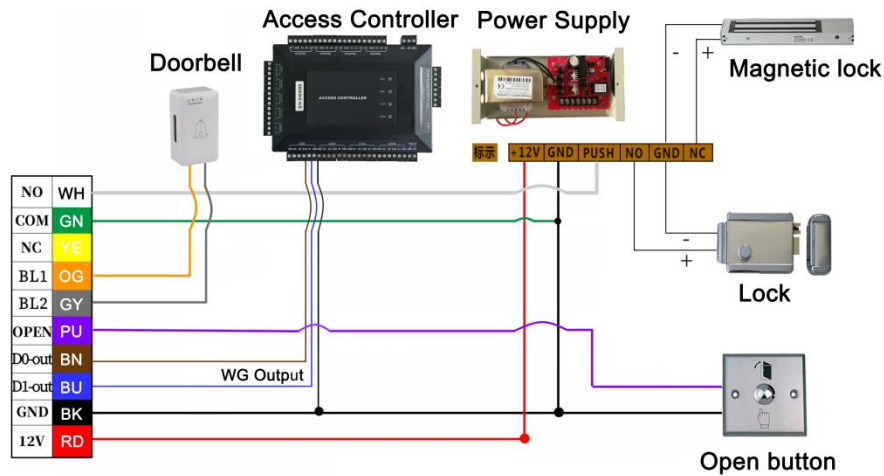
Device wiring

Wiring diagram for the facial recognition access control device:

Define the wiring according to the actual device you have.



Silicon Wireless Systems Pvt. Ltd.



Power supply line: Use two-core wire with a diameter over 1.0 mm to ensure terminal voltage > 11V.

Door opening button line: Use two-core wire with a diameter over 0.5 mm.

Door lock wire: It is recommended to use two-core power cable with a diameter over 1.0 mm. If the length exceeds 50 meters, consider using thicker wire or parallel strands. Maximum length should not exceed 80 meters, generally within 50 meters.

TCP/IP communication: Use national standard network cable; the distance from the controller to the switch or computer should not exceed 80 meters.

Doorbell: Use two-core wire, polarity does not matter. If there is no response after wiring, swap the connections and test whether the output is normal.