User Manual

5-inch Visible Light Terminal

Date: November 2023

Doc Version: 1.2

English

About the Manual

This manual introduces the operations of **5-inch Visible Light Terminal**.

All figures displayed are for illustration purposes only. Figures in this manual may not be exactly consistent with the actual products.

Features and parameters with ★ are not available in all devices.

Table of Contents

Data Security Statement

As a smart product supplier, we may also need to know and collect some of your personal information in order to better assist you in using our goods and services, and will treat your privacy carefully by developing a Privacy Policy.

Please read and understand completely all the privacy protection policy regulations and key points that appear on the device before using our products.

As a product user, you must comply with applicable laws and regulations related to personal data protection when collecting, storing, and using personal data, including but not limited to taking protective measures for personal data, such as performing reasonable rights management for devices, strengthening the physical security of device application scenarios, and so on.

Safety Measures

The below instructions intend to ensure that the user can use the product correctly to avoid danger or property loss. The following precautions are to keep users safe and prevent any damage. Please read carefully before installation.

⚠ Noncompliance with instructions could lead to product damage or physical injury (may even cause death).

1. **Read, follow, and retain instructions** - All safety and operational instructions must be properly read and followed before bringing the device into service.
2. **Do not ignore warnings** - Adhere to all warnings on the unit and in the operating instructions.
3. **Accessories** - Use only manufacturer-recommended or product-sold accessories. Please do not use any other components other than manufacturer suggested materials.
4. **Precautions for the installation** – Do not place this device on an unstable stand or frame. It may fall and cause serious injury to persons and damage to the device.
5. **Service** - Do not try to service this unit yourself. Opening or removing covers may expose you to hazardous voltages or other hazards.
6. **Damage requiring service** - Disconnect the system from the Mains AC or DC power source and refer service personnel under the following conditions:
   - When cord or connection control is affected.
   - When the liquid spilled, or an item dropped into the system.
   - If exposed to water or due to inclement weather (rain, snow, and more).
   - If the system is not operating normally, under operating instructions.

   Just change controls defined in operating instructions. Improper adjustment of the controls may

result in damage and involve a qualified technician to return the device to normal operation.

And do not connect multiple devices to one power adapter as adapter overload can cause overheat or fire hazard.

7. **Replacement parts** - When replacement parts are needed, service technicians must only use replacement parts provided by the supplier. Unauthorized substitutes can result in a burn, shock, or other hazards.
8. **Safety check** - On completion of service or repair work on the unit, ask the service technician to perform safety checks to ensure proper operation of the device.
9. **Power sources** - Operate the system only from the label's power source form. If the sort of power supply to use is unclear, call your dealer.
10. **Lightning** - Can install external lightning conductors to protect against electrical storms. It stops power-ups from destroying the system.

    Recommended installing the devices in areas with limited access.

Electrical Safety

- Before connecting an external cable to the device, complete grounding properly, and set up surge protection; otherwise, static electricity will damage the mainboard.
- Make sure that the power has been disconnected before you wire, install, or dismantle the device.
- Ensure that the signal connected to the device is a weak-current (switch) signal; otherwise, components of the device will get damaged.
- Ensure that the standard voltage applicable in your country or region is applied. If you are not sure about the endorsed standard voltage, please consult your local electric power company. Power mismatch may cause a short circuit or device damage.
- In the case of power supply damage, return the device to the professional technical personnel or your dealer for handling.
- To avoid interference, keep the device far from high electromagnetic radiation devices, such as generators (including electric generators), radios, televisions, (especially CRT) monitors, or speakers.

Operation Safety

- If smoke, odour, or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service centre.
- Transportation and other unpredictable causes may damage the device hardware. Check whether the device has any intense damage before installation.
- If the device has major defects that you cannot solve, contact your dealer as soon as possible.

- Dust, moisture, and abrupt temperature changes can affect the device's service life. You are advised not to keep the device under such conditions.
- Do not keep the device in a place that vibrates. Handle the device with care. Do not place heavy objects on top of the device.
- Do not apply rosin, alcohol, benzene, pesticides, and other volatile substances that may damage the device enclosure. Clean the device accessories with a piece of soft cloth or a small amount of cleaning agent.
- If you have any technical questions regarding usage, contact certified or experienced technical personnel.

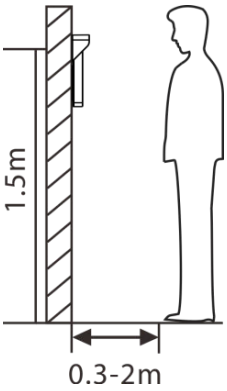
Note:

- Make sure whether the positive polarity and negative polarity of the DC 12V power supply is connected correctly. A reverse connection may damage the device. It is not advisable to connect the AC 24V power supply to the DC 12V input port.
- Make sure to connect the wires following the positive polarity and negative polarity shown on the device's nameplate.
- The warranty service does not cover accidental damage, damage caused by mis-operation, and damage due to independent installation or repair of the product by the user.

1 Instructions to use

1.1 Standing Position, Facial Expression and Standing Posture

Recommended Distance



The distance between the device and a user whose height is within 1.55m to 1.85m is recommended to be 0.3 to 2m. Users may slightly move forwards and backwards to improve the quality of facial images captured.

Facial Expression and Standing Posture

Note: During enrollment and verification, please keep natural facial expression and standing posture.

1.2 Palm Registration★

Place your palm in the palm multi-mode collection area, such that the palm is placed parallel to the device.

Make sure to keep space between your fingers.

Note:

1） Place your palm within 30 to 50 cm of the device.

2） Place your palm in the palm collection area, such that the palm is placed parallel to the device.

3） Make sure to keep space between your fingers.

4） Please avoid direct sunlight when using the palm function outdoors. According to laboratory test, the palm recognition effect is best when the light intensity is not more than 10,000 lux.

1.3 Face Registration

Try to keep the face in the center of the screen during registration. Please face the camera and stay still during face registration. The page looks like shown below:

Face registration and authentication methods

Instructions to Register a Face

- When registering a face, maintain a distance of 40cm to 80cm between the device and the face.
- Be careful not to change the facial expression. (smiling, drawn, wink, etc.)
- If you do not follow the instructions on the screen, the face registration may take a longer time or may fail.
- Be careful to not cover the eyes or eyebrows.
- Do not wear hats, masks, sunglasses, or eyeglasses.
- Be careful to not display two faces on the screen. Register only one person at a time.
- It is recommended for a user wearing glasses to register both faces with and without glasses.

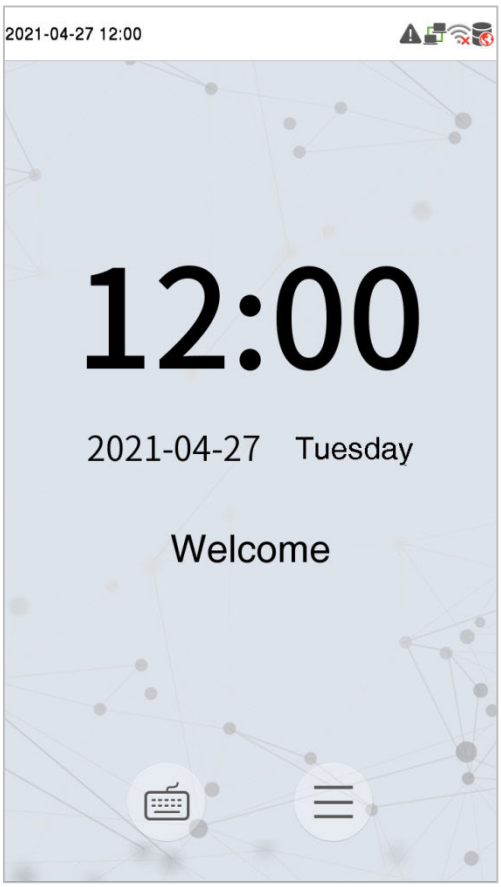
Instructions to Authenticate a Face

- Ensure that the face appears inside the detection area displayed on the device screen.

- If eyeglasses have been changed, authentication may fail. If the face without glasses has been registered, authenticate the face without glasses. If only the face with glasses has been registered, authenticate the face with the previously worn glasses again.
- If a part of the face is covered with a hat, a mask, an eye patch, or sunglasses authentication may fail. Do not cover the face, allow the device to recognize both the eyebrows and the face.

1.4 Standby Interface

After connecting the power supply, the interface appears as shown below:

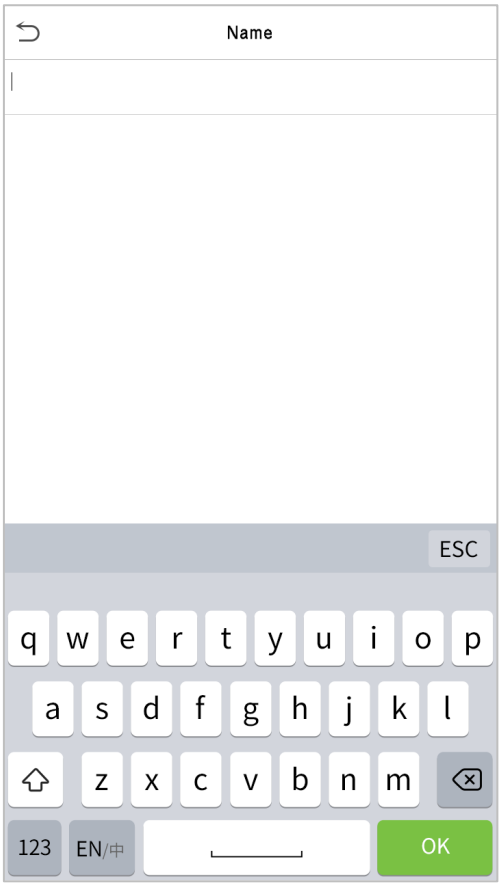


Note:

1) Click  to open the interface to enter the User ID.

2) When there is no super administrator registered in the device, click  to enter the menu. After setting the super administrator, it requires the super administrator's verification before entering the menu operation. For the security of the device, it is recommended to register a super administrator the first time you use the device.

1.5 Virtual Keyboard



Note: The device supports the input of Chinese and English characters, numbers, and symbols. Click [**En**] to switch to the English keyboard. Press [**123**] to switch to the numeric and special character keyboard, and click [**ABC**] to return to the alphabetic keyboard. Click the input box, and the virtual keyboard appears. Click [**ESC**] to exit the keyboard screen.

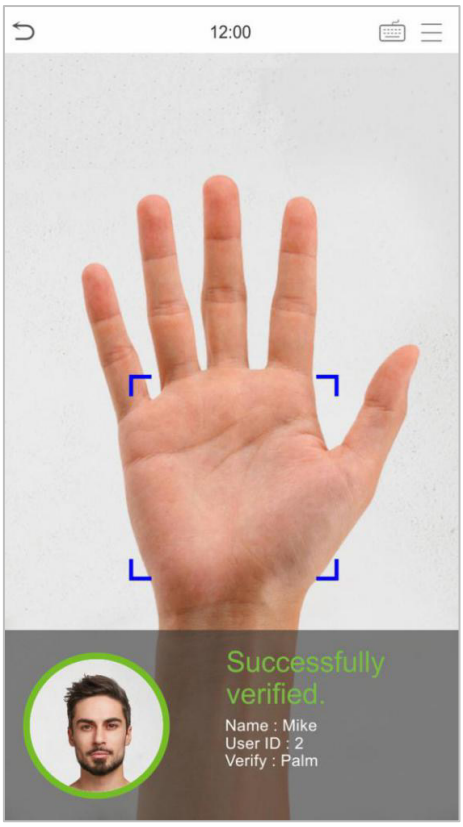
1.6 Verification Mode

1.6.1 Palm Verification★

1:N Palm Verification Mode

This verification mode compares the palm image collected by the palm module with all the palm data template in the device.

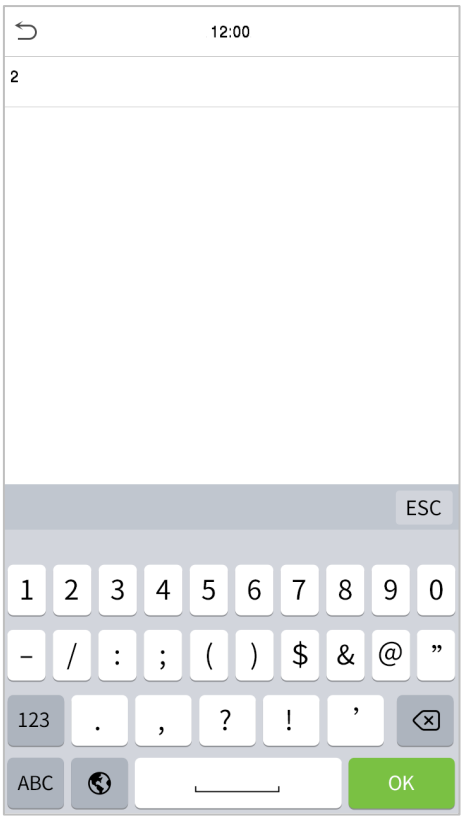
The device will automatically distinguish between the palm and face verification mode. Place the palm in the area that can be collected by the palm module, so that the device will automatically switch to palm verification mode.



1:1 Palm Verification Mode

Click the  button on the main screen to open the 1:1 palm verification mode.

1. Input the user ID and press [**OK**].



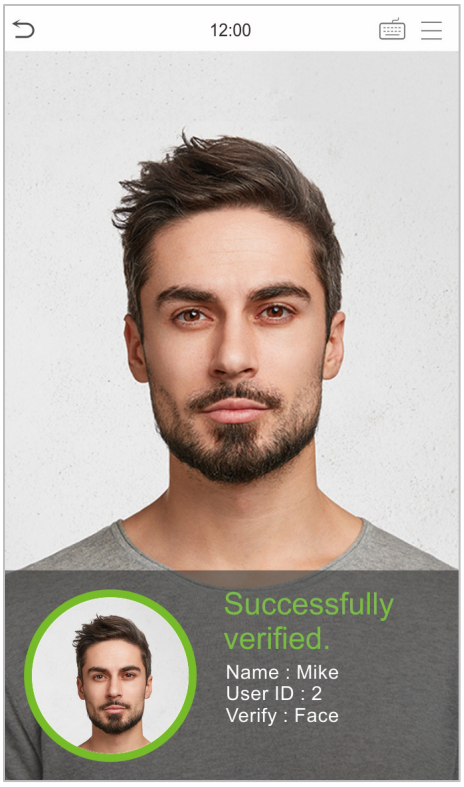
If the user has registered the card, face and password in addition to palm, and the verification method is set to Password/Face/Palm/Card, the following screen will appear. Select the palm icon to enter palm verification mode.

1.6.2 Facial Verification

1:N Facial Verification

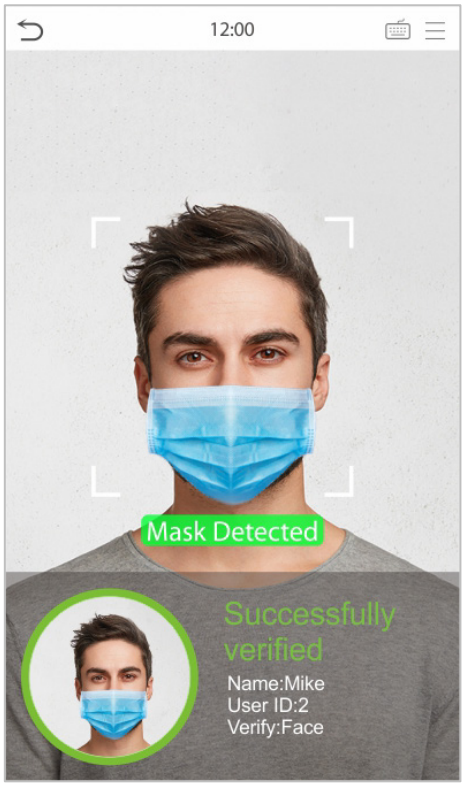
1. Conventional verification

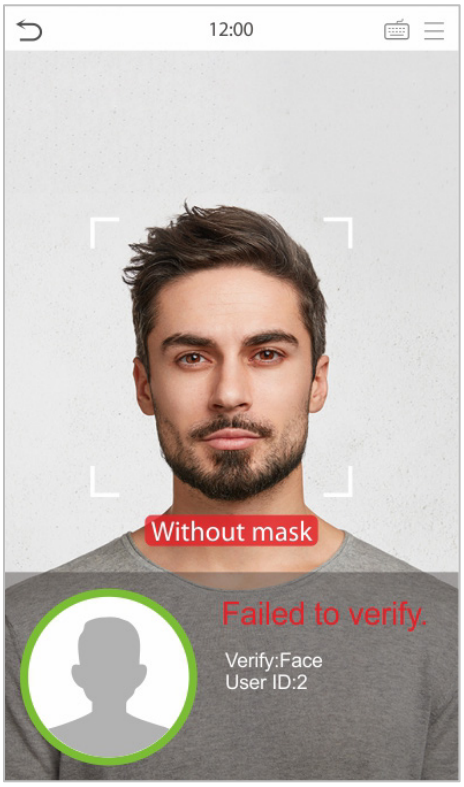
In this verification mode, the device compares the collected facial images with all face data registered in the device. The following is the pop-up prompt of a successful comparison result.



2. Enable mask detection

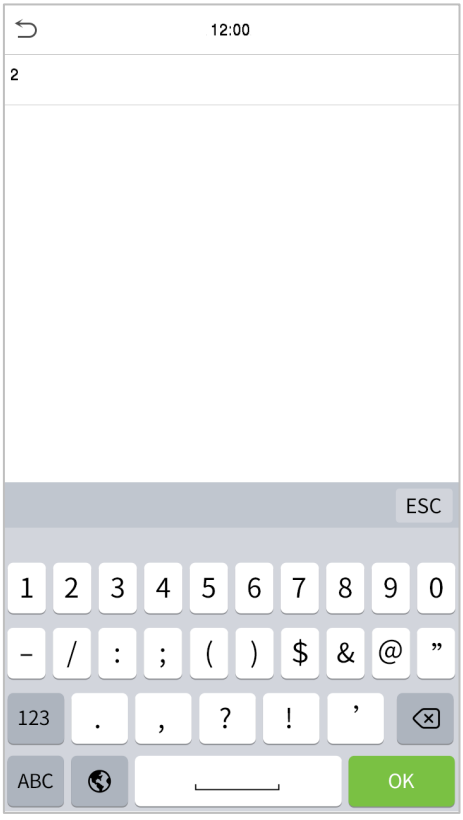
When the user enables the **Enable mask detection** function, the device identifies whether the user is wearing a mask while verification or not. The following are the popups of the comparison result prompt interface.





1:1 Facial Verification

In this verification mode, the device compares the face captured by the camera with the facial template related to the entered user ID. Press on the main interface and enter the 1:1 facial verification mode and enter the user ID and click [**OK**].



If the user has registered password, card and palm★ in addition to the face, and the verification method is set to Password/Face/Palm★/Card verification, the following screen will appear. Select the  icon to enter the face verification mode.

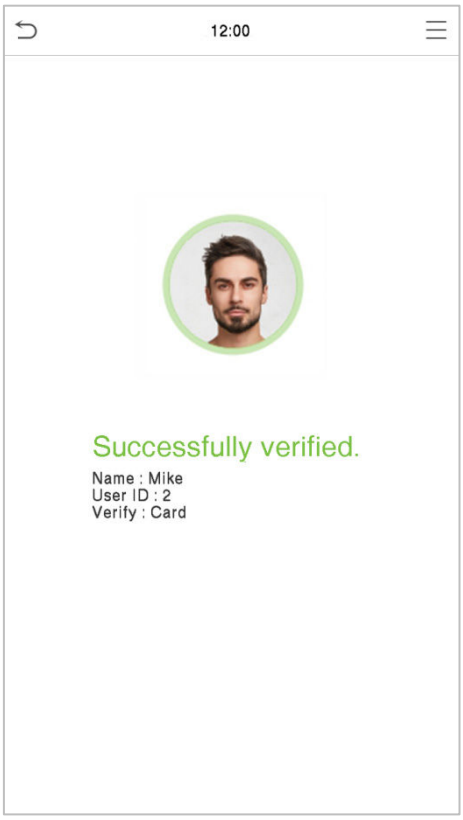
After successful verification, the prompt box displays "**Successfully verified**", as shown below:

If the verification is failed, it prompts "**Please adjust your position!** ".

1.6.3 Card Verification

1:N Card Verification

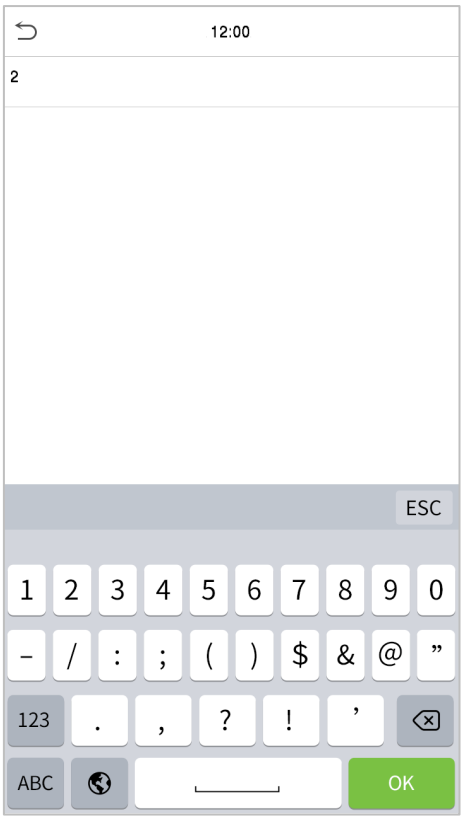
This verification mode compares the card number in the Card induction area with all the card number data registered in the device; the following is the card verification screen.



1:1 Card Verification

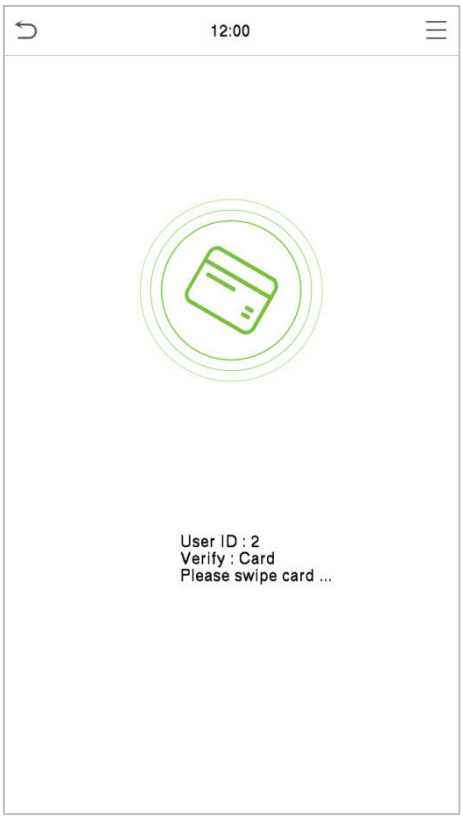
Click the  button on the main screen to open the 1:1 Card verification mode.

1. Input the user ID and press [**OK**].

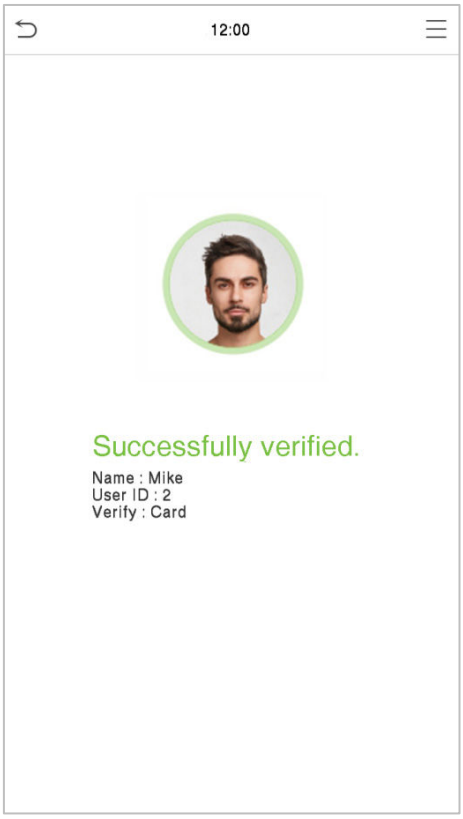


If an employee registers palm★, face and password in addition to card, and the verification method is set to Password/Face/Palm★/Card, the following screen will appear. Select the icon to enter the card verification mode.

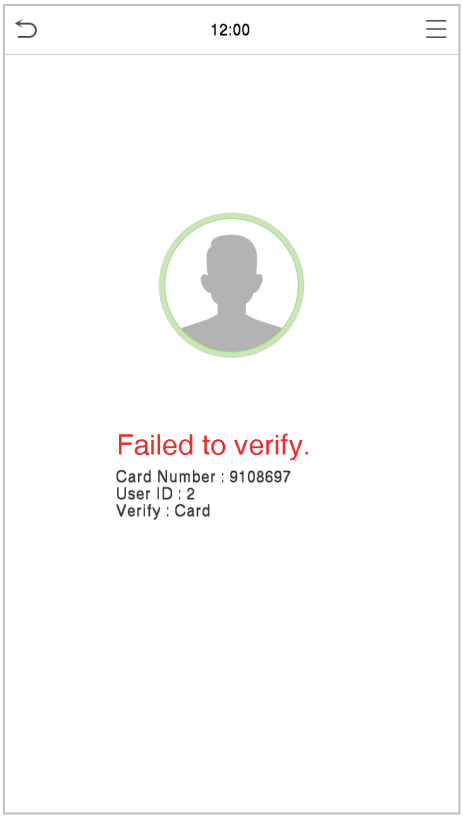
2. Swipe the card above the card area (the card must be registered first).



Successful Verification:



Failed Verification:

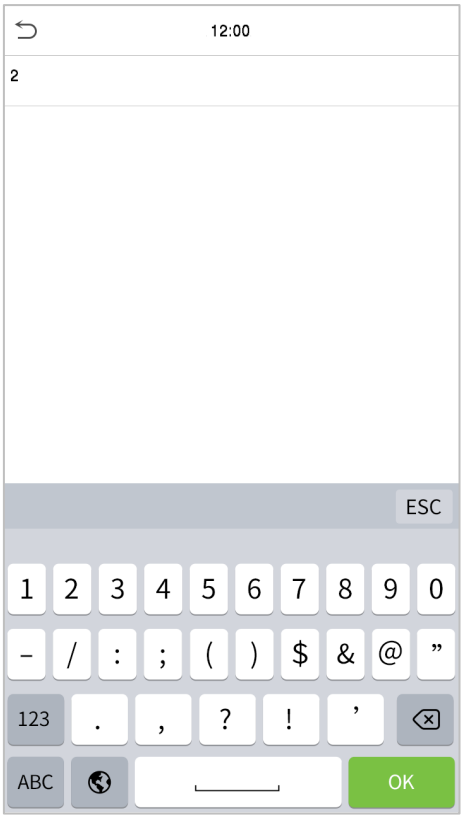


1.6.4 Password Verification

The Password Verification mode compares the entered password with the registered User ID and Password.

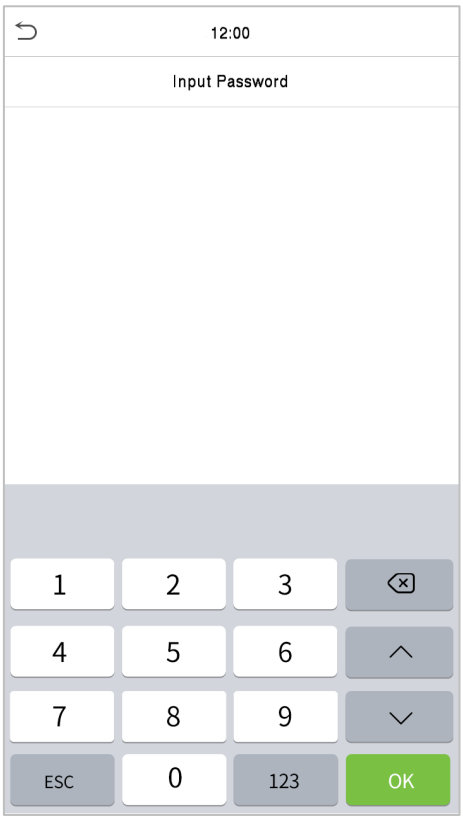
Click the  button on the main screen to open the 1:1 password verification mode.

1. Input the user ID and press [**OK**].

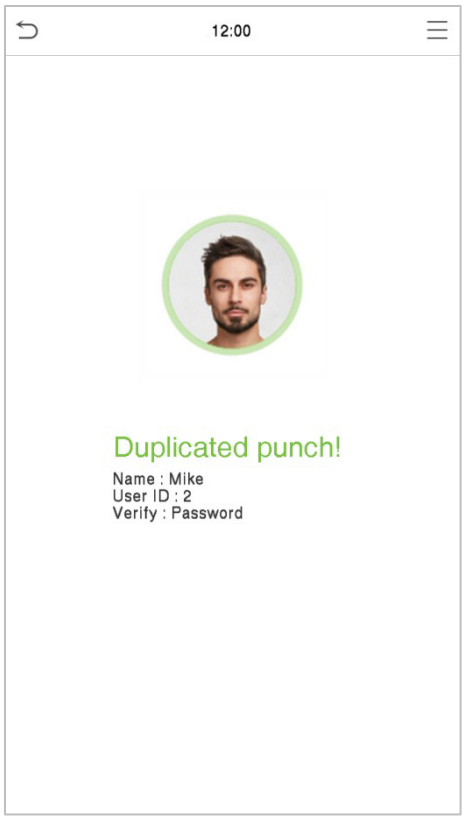


If an employee registers palm★, card and face in addition to password, and the verification method is set to Password/Face/Palm★/Card, the following screen will appear. Select the  icon to enter the password verification mode.

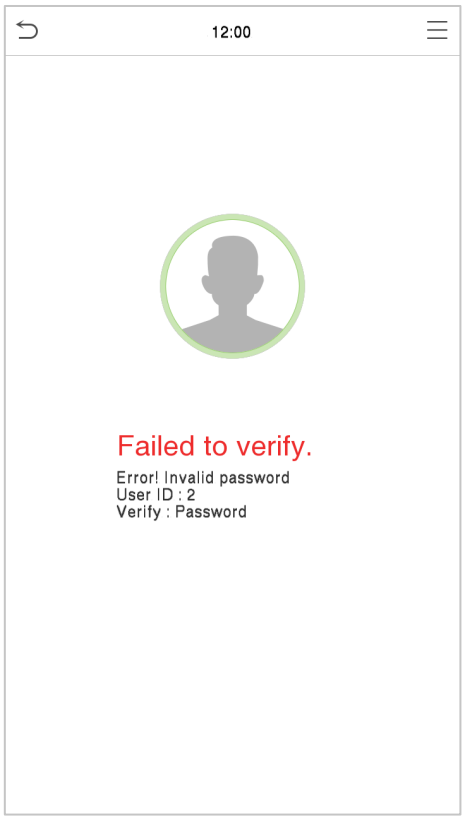
2. Input the password and press [**OK**].



Successful Verification:

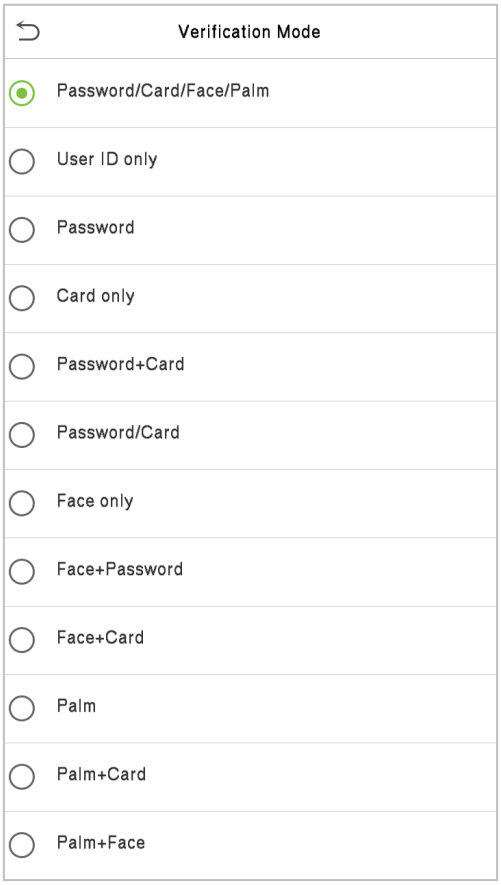


Failed Verification:



1.6.5 Combined Verification

To increase the security, this device offers the option of using multiple forms of verification methods. A total of 12 different verification combinations can be used, as shown below:



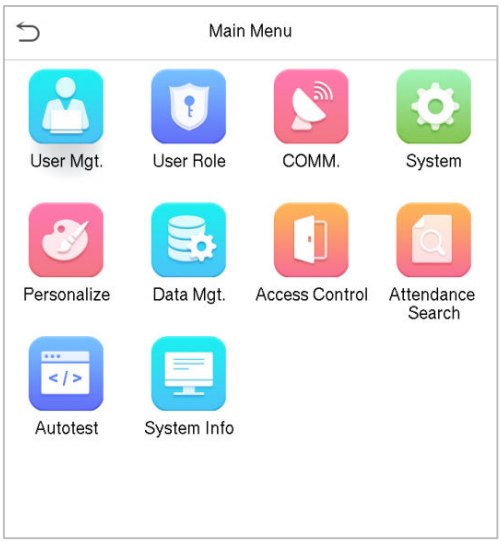
Note:

1) "/" means "or", and "+" means "and".

2) You must register the required verification information before using the combination verification mode, otherwise, the verification may fail. For example, if a user uses Face Registration but the verification mode is Face + Password, this user will never pass verification.

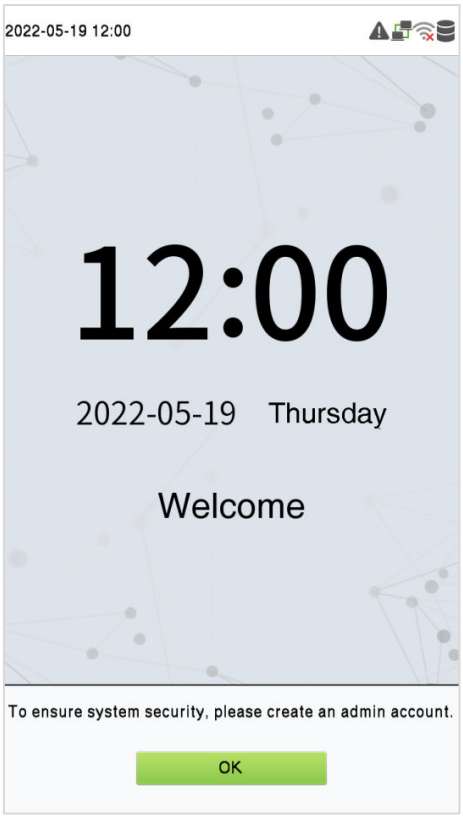
2 Main Menu

Press on the initial interface to enter the main menu, as shown below:



Menu	Description
User Mgt.	To add, edit, view, and delete the basic information about a user.
User Role	To set the permission scope of the custom role, that is, the rights to operate the system.
COMM.	To set the relevant parameters of the network, Serial comm, PC connection, Wireless network, Cloud server, and Wiegand, Network diagnosis.
System	To set the parameters related to the system, including date & time, attendance, facial templates, palm templates★, resetting to factory settings, security settings, device type setting and detection management.
Personalize	This includes user Interface, voice, bell settings.
Data Mgt.	To delete all the relevant data in the device.
Access Control	To set the parameters of the lock and the relevant access control device including options like Time Rule Setting, Holiday Settings, Combine verification, Anti-Passback Setup and Duress Option Settings.
Attendance Search	To query the specified Event Logs, check Attendance Photos and Blocklist attendance photos.
Autotest	To automatically test whether each module functions properly, including the screen, audio, camera, and real-time clock.
System Info	To view the data capacity, device and firmware information and privacy policy of the device.

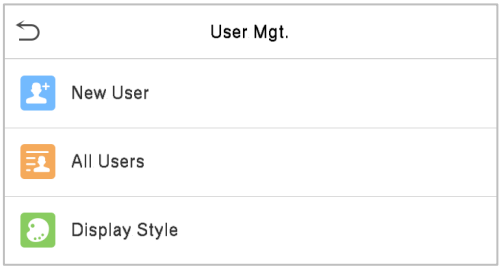
Note: When users use the product for the first time, they should operate it after setting administrator privileges. Tap **User Mgt.** to add an administrator or edit user permissions as a super administrator. If the product does not have an administrator setting, the system will show an administrator setting command prompt every time you enter the device menu.



3 User Management

3.1 Add Users

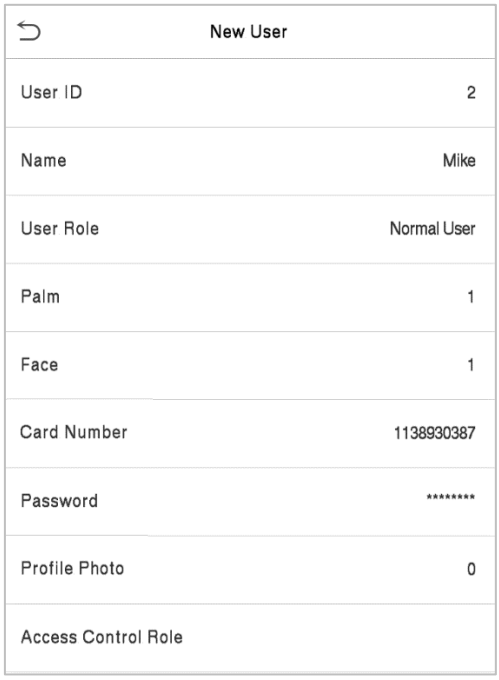
Click **User Mgt.** on the main menu.



Click **New User.**

Register a User ID and Name

Enter the User ID and Name.



Note:

1) A username may contain 17 characters.
2) The user ID may contain 1 to 9 digits by default.
3) During the initial registration, you can modify your ID, which cannot be modified after registration.
4) If a message "Duplicated ID" pops up, you must choose another ID.

Setting the User Role

There are two types of user accounts: **Normal user** and **Super admin**. If there is already a registered administrator, the normal users have no rights to manage the system and may only access authentication verifications. The Administrator owns all the management privileges. If a custom role is set, you can also select **user-defined role** permissions for the user.

Click **User Role** to select Normal User or Super Admin.

Note: If the selected user role is the Super Admin, the user must pass the identity authentication to access the main menu.

Register Palm★

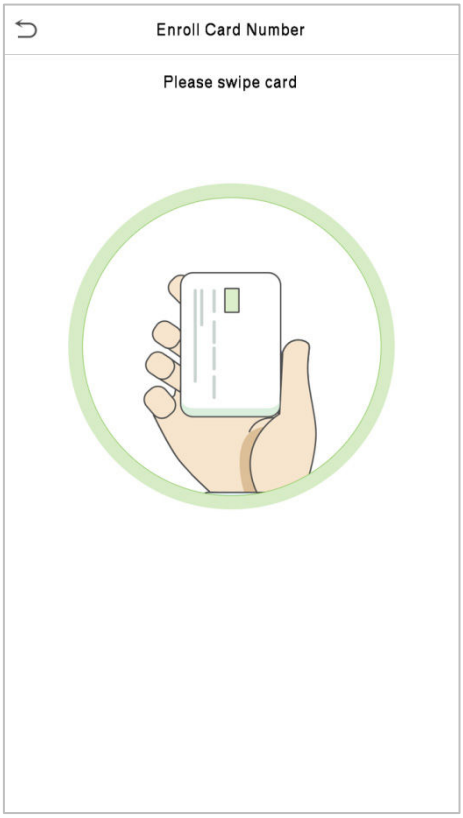
Click **Palm** to open the palm registration page. Select the palm to be enrolled.

Register Face

Click **Face** to enter the face registration page. Please face the camera and stay still during face registration. The registration interface is as follows:

Register Card

Press your **card** above the card area. The card number registration will be successful.



Register Password

Click **Password** to open the password registration page. Enter a password and re-enter it. Click **OK**. If the two entered passwords are different, the prompt "Password not match" will appear.

Note: The password may contain one to eight digits by default.

Register Profile Photo

When a user registered with a photo passes the authentication, the registered photo will be displayed.

Click **Profile Photo**; click the camera icon to take a photo. The system will return to the New User interface after taking a photo.

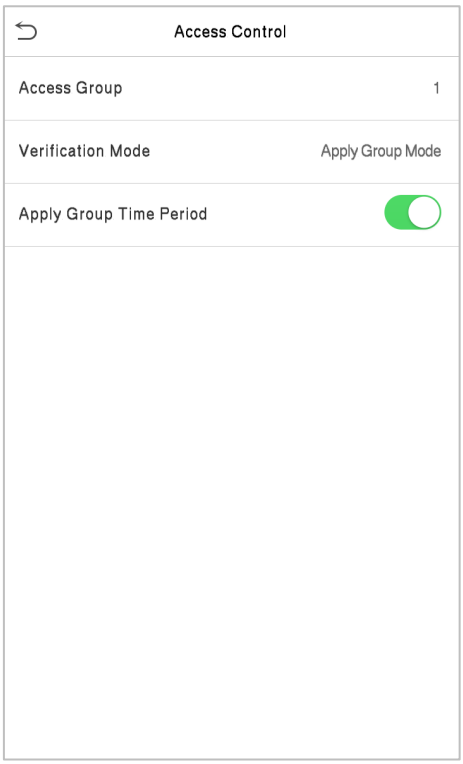
Note: While registering a face, the system will automatically capture a picture as the profile photo. If you do not want to register a profile photo, the system will automatically set the picture captured as the default photo.

Access Control Role

User access control sets the door unlocking rights of each person, including the group, the verification mode and select whether to apply group time period.

Click **Access Control Role** > **Access Group**, assign the registered users to different groups for better management. New users belong to Group 1 by default and can be reassigned to other groups. The device supports up to 99 access control groups.

Click **Verification Mode**, select the Verification Mode to use.

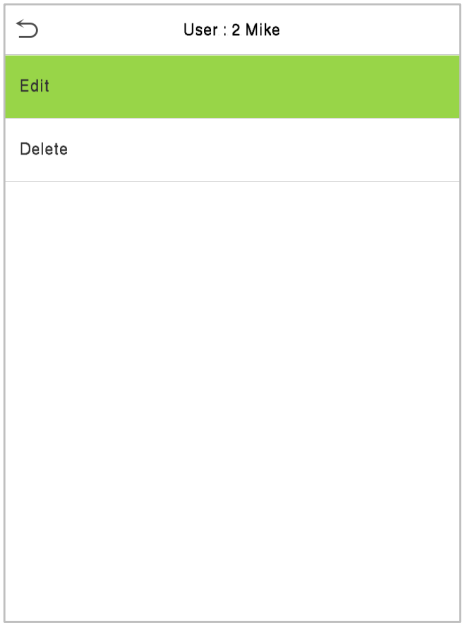


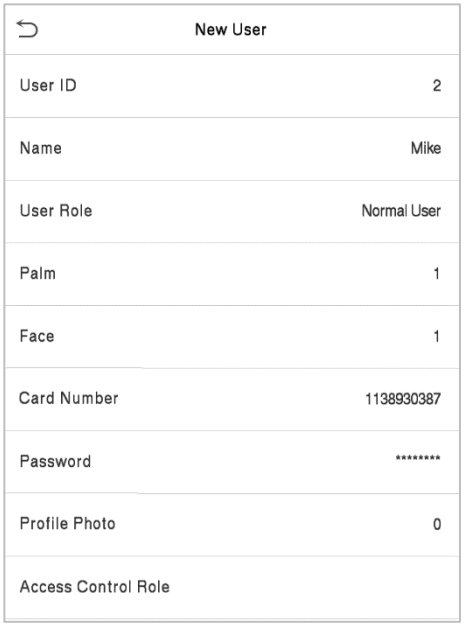
3.2 Search for Users

Click the search bar on the user list and enter the retrieval keyword (The keyword may be an ID, surname or full name).The system will search for the users related to the information.

3.3 Edit Users

Select a user from the list and click **Edit** to enter the edit user interface.



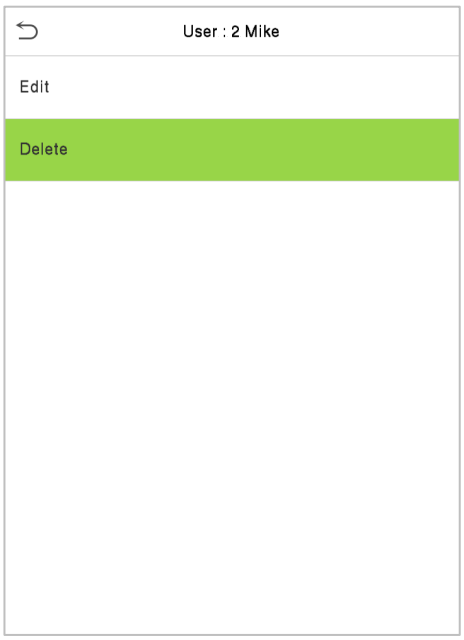


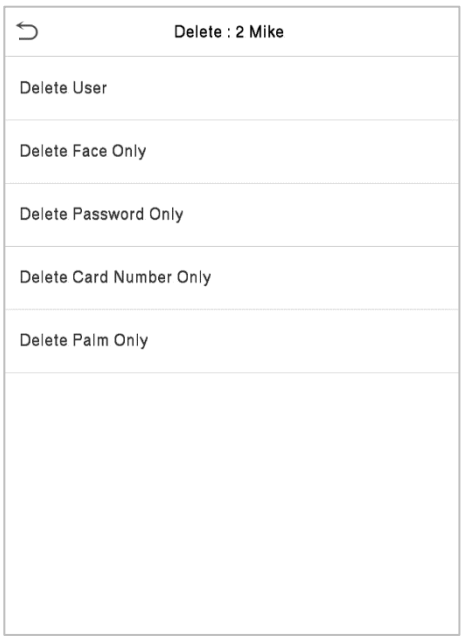
Note: The operation of editing a user is the same as that of adding a user, except that the user ID cannot be modified when editing a user. For further details, refers "3.1 Add users".

3.4 Delete Users

Select a user from the list and click **Delete** to enter the delete user interface. Select the user information to be deleted and click **OK**.

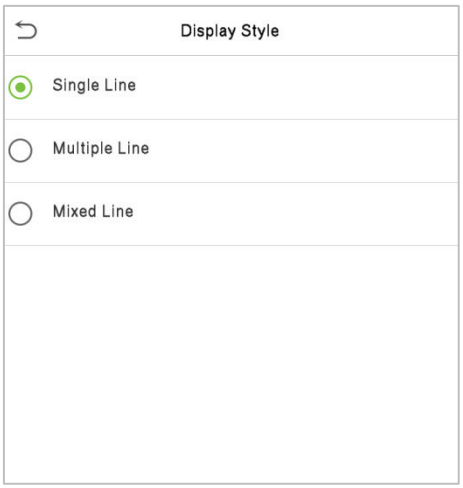
Note: If you select **Delete User**, all information of the user will be deleted.





3.5 Display Style

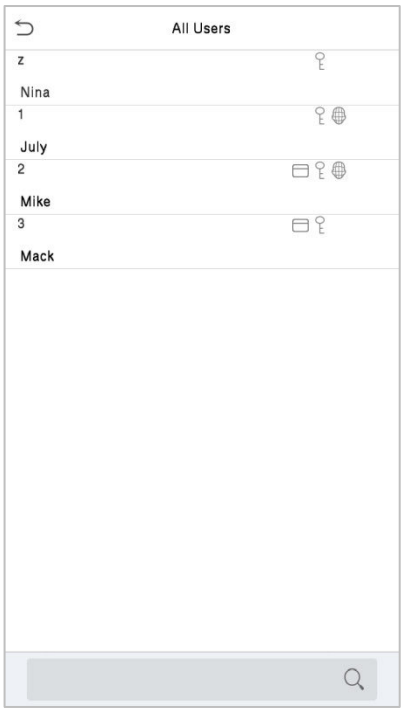
On the **Main Menu**, click **User Mgt.,** and then click **Display Style** to enter Display Style setting interface.



All the Display Styles are shown as below:

Single Line

Multiple Line



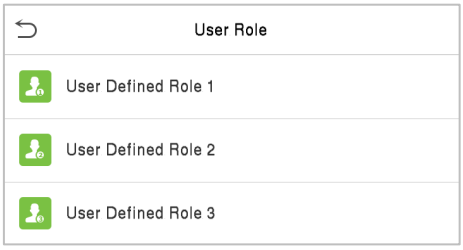
Mixed Line

4 User Role

If you need to assign some specific permissions to certain users, you may edit the "User Defined Role" under the **User Role** menu.

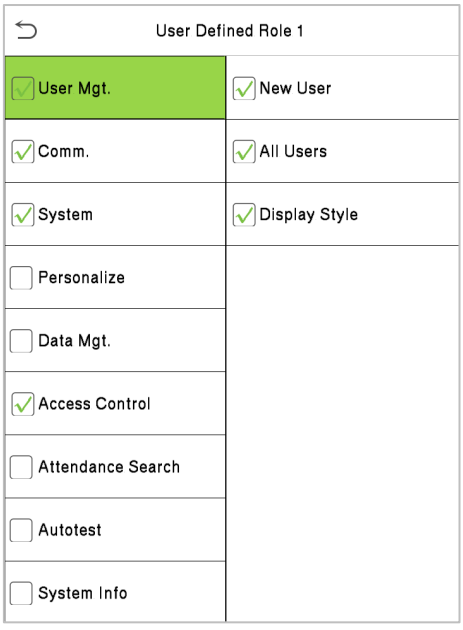
You may set the permission scope of the custom role (up to 3 roles), that is, the permission scope of the operation menu.

Click **User Role** on the main menu interface.

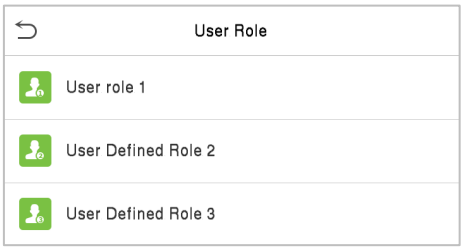


1. Click any user role to set a defined role. Toggle the **Enable Defined Role** button to enable this defined role. Click **Name** and enter the name of the role.

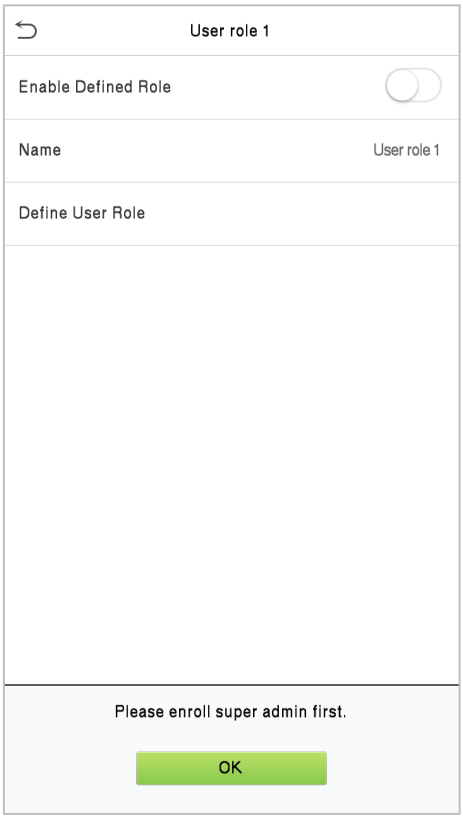
2. Click **Define User Role** to assign privileges to the role. Once the privilege assignment is completed, click **Return**.



Note: During the privilege assignment, the main menu is on the left and its sub-menus are on the right. You only need to select the features in sub-menus. If the device has a role enabled, you may assign the roles you set to users by clicking **User Mgt. > New User> User Role**.



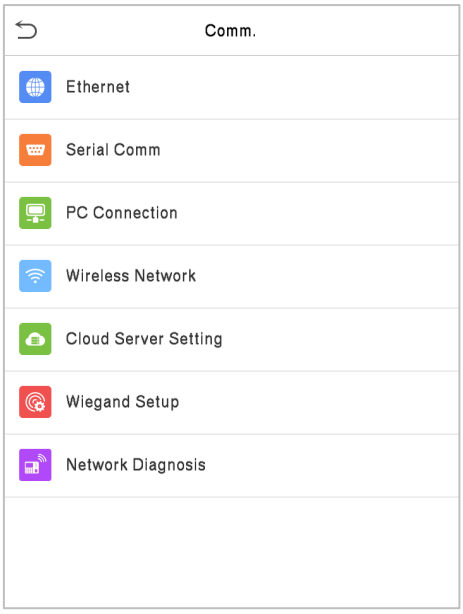
If no super administrator is registered, the device will prompt "Please enroll super admin first!" after clicking the enable bar, as shown below.



5 Communication Settings

Communication Settings are used to set the parameters of the Network, Serial Comm, PC connection, Wireless Network, Cloud server, and Wiegand, Network Diagnosis.

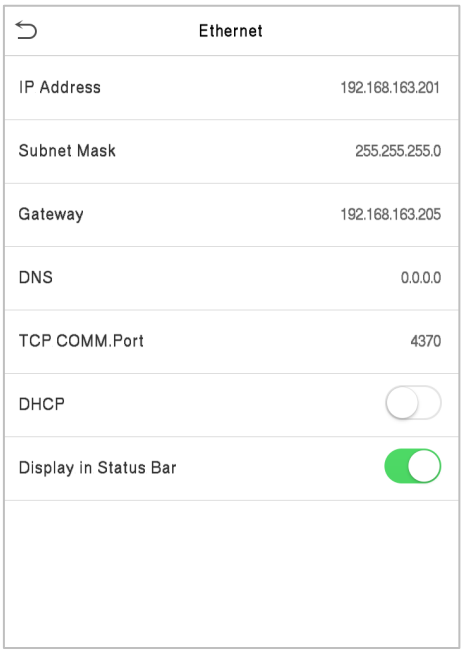
Click **COMM.** on the main menu.



5.1 Network Settings

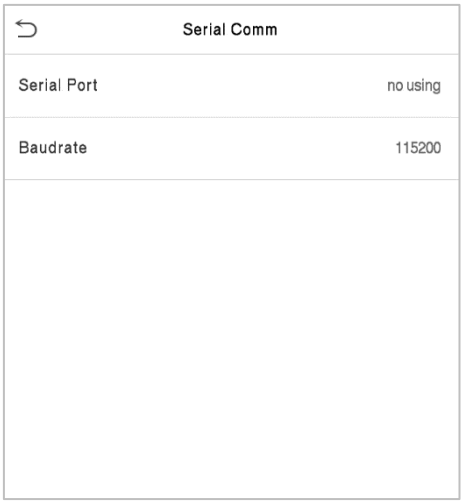
When the device needs to communicate with a PC over the Ethernet, you need to configure network settings and ensure that the device and the PC are connecting to the same network segment.

Click **Ethernet** on the Comm. Settings interface.



Menu	Description
IP Address	The factory default value is 192.168.1.201. Please set the IP Address as per the requirements.
Subnet Mask	The factory default value is 255.255.255.0. Please set the value as per the requirements.
Gateway	The factory default address is 0.0.0.0. Please set the value as per the requirements.
DNS	The factory default address is 0.0.0.0. Please set the value as per the requirements.
TCP COMM. Port	The factory default value is 4370. Please set the value as per the requirements.
DHCP	Dynamic Host Configuration Protocol, which is to dynamically allocate IP addresses for clients via server.
Display in Status Bar	To set whether to display the network icon on the status bar.

5.2 Serial Comm



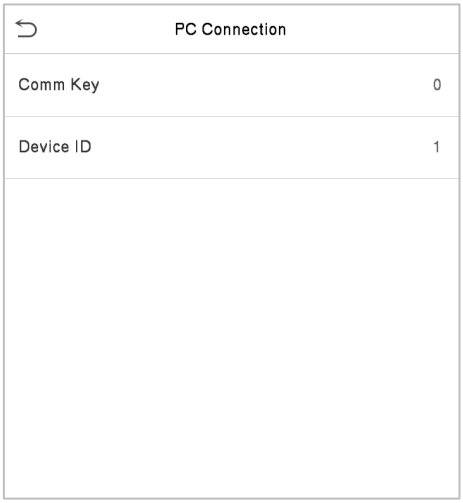
Menu	Description
Serial Port	Including no using, RS232(PC) and RS485(PC), select RS232(PC) to communicate with the device through an RS232 serial port. Select RS485(PC) to communicate with the device through an RS485 serial port.
Baudrate	The rate of the communication with PC; there are 5 options of baud rate: 115200 (default), 57600, 38400, 19200 and 9600. The higher is the baud rate, the faster is the communication speed, but also the less reliable. In general, a higher baud rate can be used when the communication distance is short; when the communication distance is long, choosing a lower baud rate would be more reliable.

5.3 PC Connection

To improve the security of data, please set a **Comm Key** for communication between the device and the PC.

If a Comm Key is set, this connection password must be entered before the device can be connected to the PC software.

Click **PC Connection** on the Comm. Settings interface.

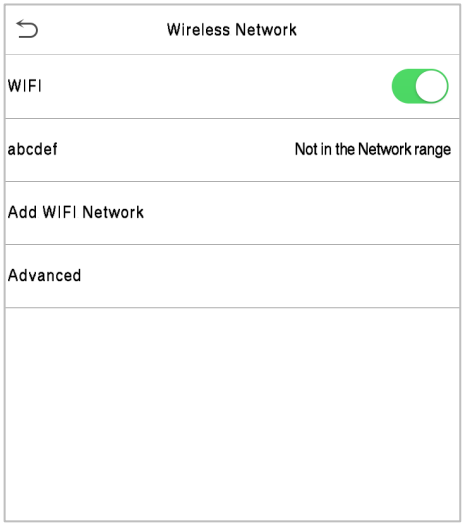


Menu	Description
Comm Key	Comm Key: The default password is 0, which can be changed. The Comm Key may contain 1 to 6 digits.
Device ID	The identity number of the device, which ranges between 1 and 254. If the communication method is RS232/RS485, you need to input this device ID in the software communication interface.

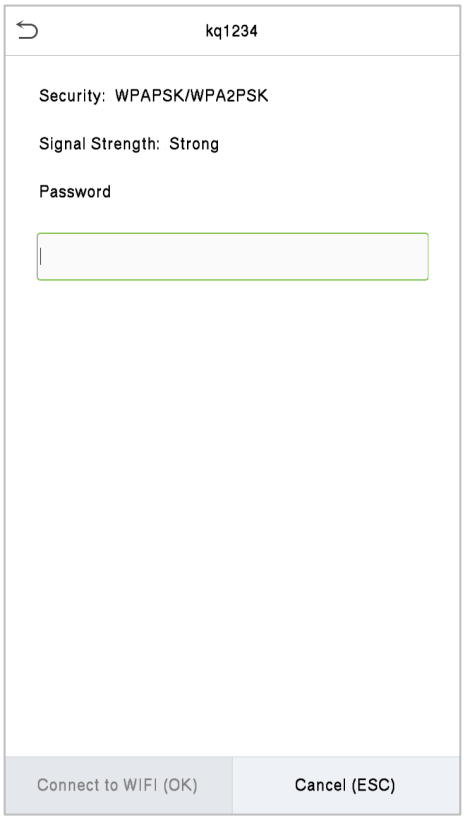
5.4 Wireless Network

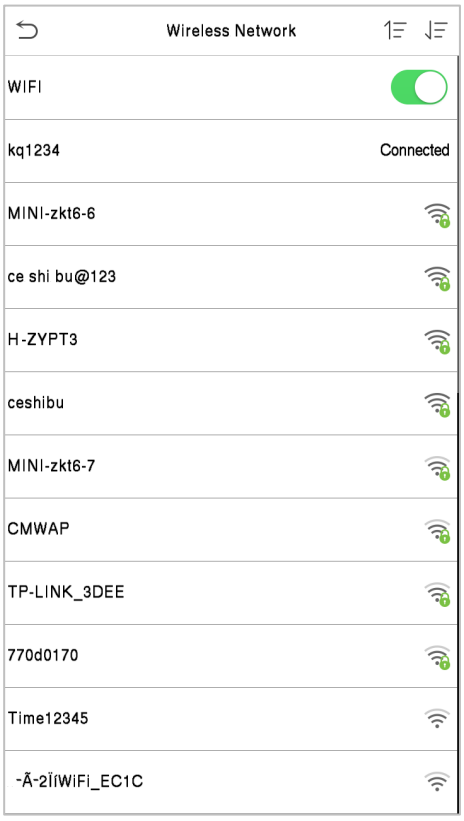
Wi-Fi is short for Wireless Fidelity. The device provides a Wi-Fi module, which can be built in the device mould or externally connected, to enable data transmission via Wi-Fi and establish a wireless network environment.

Wi-Fi is enabled in the system by default. If the Wi-Fi network does not need to be used, you can click the button to disable Wi-Fi.



When Wi-Fi is enabled, click the searched network. Click the password entry text box to enter the password, and click **Connect to Wi-Fi (OK)**.



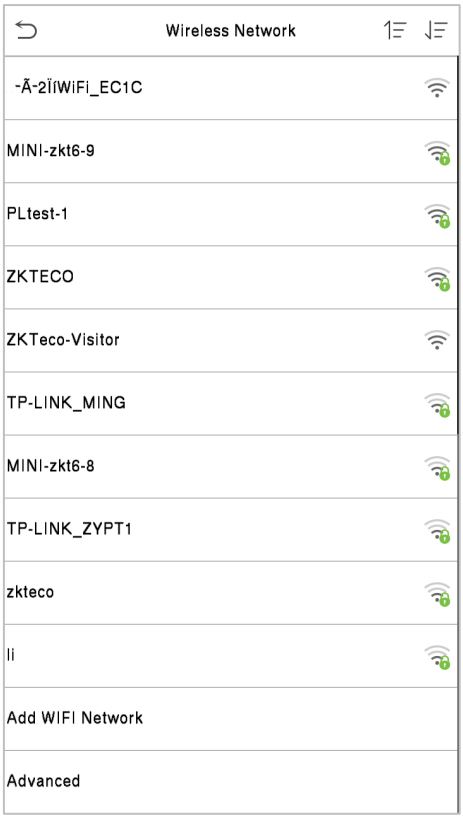


The connection succeeds, with status displayed on the icon bar.

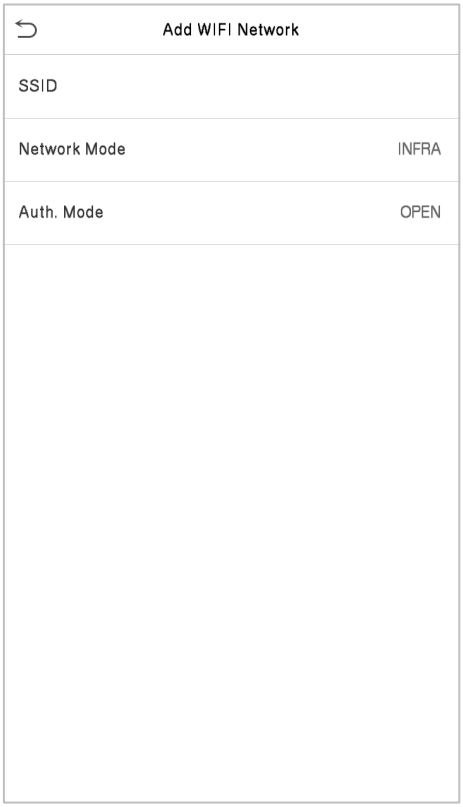
Adding Wi-Fi Network

If the desired Wi-Fi network is not in the list, you can add the Wi-Fi network manually.

Click **Page Down** and **Add Wi-Fi Network**.



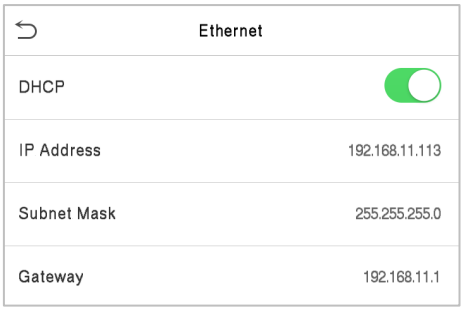
Enter the parameters of Wi-Fi network. (The added network must exist.)



After adding, find the added Wi-Fi network in list and connect to the network in the above way.

Advanced Options

This is used to set Wi-Fi network parameters.

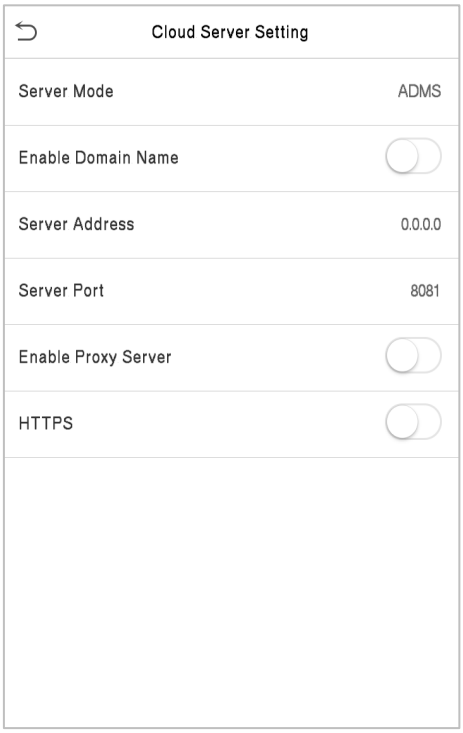


Menu	Descriptions
DHCP	Short for Dynamic Host Configuration Protocol, which involves allocating dynamic IP addresses to network clients.
IP Address	IP address of the Wi-Fi network.
Subnet Mask	Subnet mask of the Wi-Fi network.
Gateway	Gateway address of the Wi-Fi network.

5.5 Cloud Server Setting

This represents the settings used for connecting the ADMS server.

Click **Cloud Server Setting** on the Comm. Settings interface.

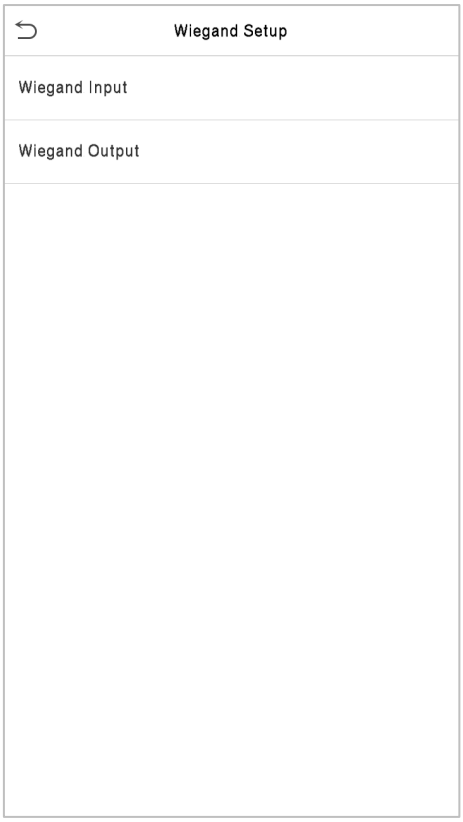


Menu		Description
Enable Domain Name	**Server Address**	When this function is enabled, the domain name mode "http://... "will be used, such as http://www.XYZ.com, while "XYZ" denotes the domain name when this mode is turned ON.
Disable Domain Name	**Server Address**	IP address of the ADMS server.
	Server Port	Port used by the ADMS server.
Enable Proxy Server		When you choose to enable the proxy, you need to set the IP address and port number of the proxy server.
HTTPS		To increase the security of browser access, users can enable the HTTPS protocol to create a secure and encrypted network transmission and assure the security of sent data through identity authentication and encrypted communication. This function is enabled by default. This function can be enabled or disabled through the menu interface, and when changing the HTTPS status, the device will pop up a security prompt, and restart after confirmation.

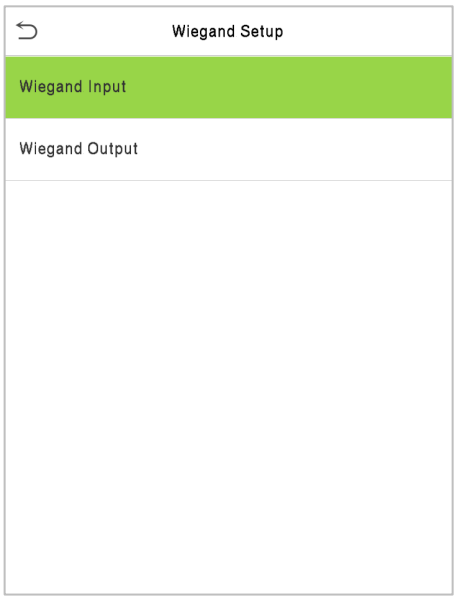
5.6 Wiegand Setup

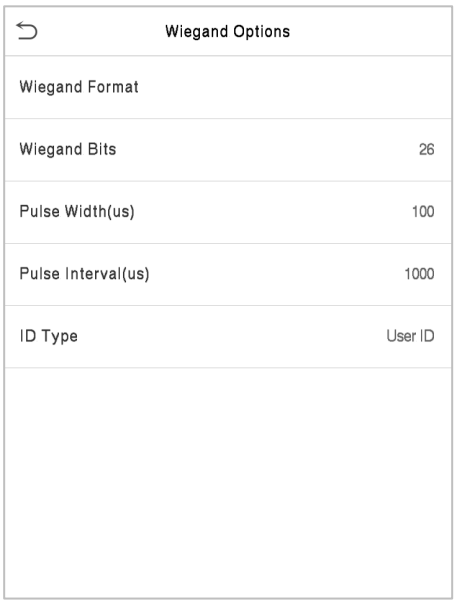
The menu is used to set the Wiegand Input & Output parameters.

Click **Wiegand Setup** on the Comm. Settings interface.



Wiegand Input





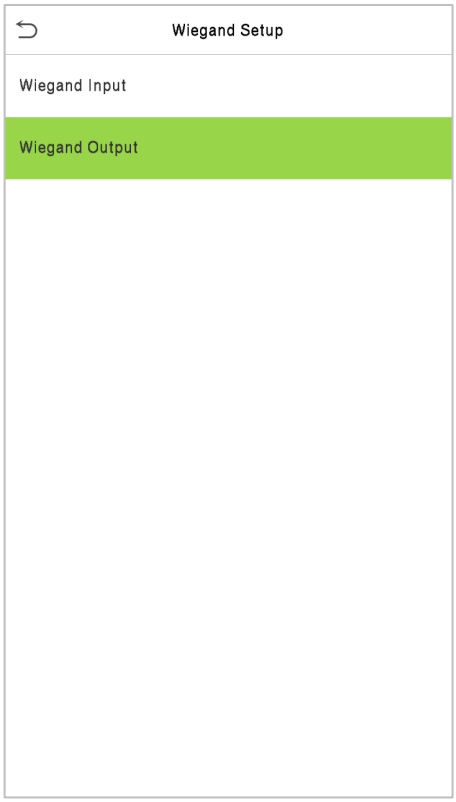
Menu	Descriptions
Wiegand Format	Values range from 26 bits, 34 bits, 36 bits, 37 bits, and 50 bits.
Wiegand Bits	Number of bits of Wiegand data.
Pulse Width(us)	The value of the pulse width sent by Wiegand is 100 microseconds by default, which can be adjusted within the range of 20 to 100 microseconds.
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 the User ID and Card number.

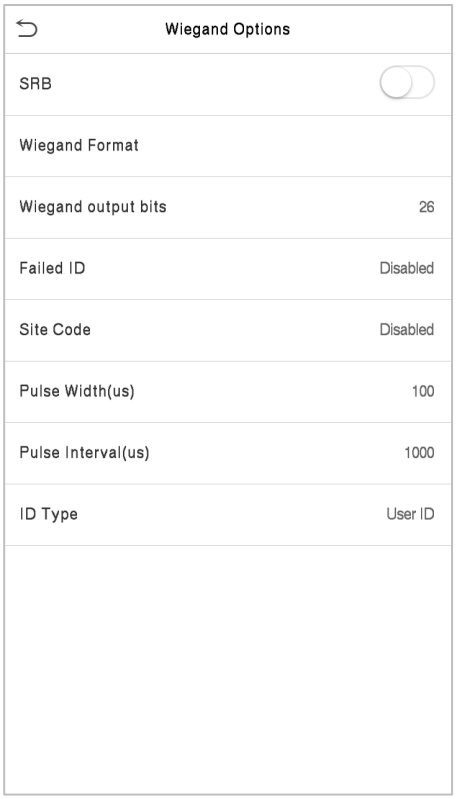
Definitions of various common Wiegand formats:

Wiegand Format	Description
Wiegand26	ECCCCCCCCCCCCCCCCCCCCCCCCO It consists of 26 bits of binary code. The 1st bit is the even parity bit of the 2nd to 13th bits, while the 26th bit is the odd parity bit of the 14th to 25th bits. The 2nd to 25th bits is the card numbers.
Wiegand26a	ESSSSSSSSCCCCCCCCCCCCCCCCO It consists of 26 bits of binary code. The 1st bit is the even parity bit of the 2nd to 13th bits, while the 26th bit is the odd parity bit of the 14th to 25th bits. The 2nd to 9th bits is the site codes, while the 10th to 25th bits are the card numbers.
Wiegand34	ECCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO It consists of 34 bits of binary code. The 1st bit is the even parity bit of the 2nd to 17th bits, while the 34th bit is the odd parity bit of the 18th to 33rd bits. The 2nd to 25th bits is the card numbers.

Wiegand34a	ESSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCO It consists of 34 bits of binary code. The 1st bit is the even parity bit of the 2nd to 17th bits, while the 34th bit is the odd parity bit of the 18th to 33rd bits. The 2nd to 9th bits is the site codes, while the 10th to 25th bits are the card numbers.
Wiegand36	OFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCMME It consists of 36 bits of binary code. The 1st bit is the odd parity bit of the 2nd to 18th bits, while the 36th bit is the even parity bit of the 19th to 35th bits. The 2nd to 17th bits is the device codes. The 18th to 33rd bits is the card numbers, and the 34th to 35th bits are the manufacturer codes.
Wiegand36a	EFFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCO It consists of 36 bits of binary code. The 1st bit is the even parity bit of the 2nd to 18th bits, while the 36th bit is the odd parity bit of the 19th to 35th bits. The 2nd to 19th bits is the device codes, and the 20th to 35th bits are the card numbers.
Wiegand37	OMMMMSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCE It consists of 37 bits of binary code. The 1st bit is the odd parity bit of the 2nd to 18th bits, while the 37th bit is the even parity bit of the 19th to 36th bits. The 2nd to 4th bits is the manufacturer codes. The 5th to 16th bits is the site codes, and the 21st to 36th bits are the card numbers.
Wiegand37a	EMMMFFFFFFFFFSSSSSSCCCCCCCCCCCCCCCCO It consists of 37 bits of binary code. The 1st bit is the even parity bit of the 2nd to 18th bits, while the 37th bit is the odd parity bit of the 19th to 36th bits. The 2nd to 4th bits is the manufacturer codes. The 5th to 14th bits is the device codes, and15th to 20th bits are the site codes, and the 21st to 36th bits are the card numbers.
Wiegand50	ESSSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO It consists of 50 bits of binary code. The 1st bit is the even parity bit of the 2nd to 25th bits, while the 50th bit is the odd parity bit of the 26th to 49th bits. The 2nd to 17th bits is the site codes, and the 18th to 49th bits are the card numbers.
"C" denotes the card number; **"E"** denotes the even parity bit; **"O"** denotes the odd parity bit; **"F"** denotes the facility code; **"M"** denotes the manufacturer code; **"P"** denotes the parity bit; and **"S"** denotes the site code.	

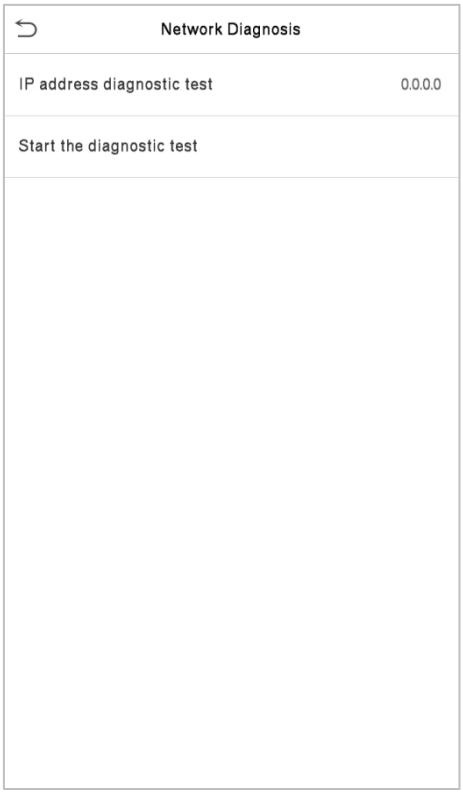
Wiegand Output





Menu	Descriptions
SRB	When SRB is enabled, the lock is controlled by the SRB to prevent the lock from being opened due to device removal.
Wiegand Format	Values range from 26 bits, 34 bits, 36 bits, 37 bits, and 50 bits.
Wiegand output bits	After choosing the Wiegand format, you can select one of the corresponding output digits in the Wiegand format
Failed ID	If the verification is failed, the system will send the failed ID to the device and replace the card number or personnel ID with the new ones.
Site Code	It is similar to the Device ID. The difference is that a site code can be set manually, and is repeatable in a different device. The valid value ranges from 0 to 256 by default.
Pulse Width(us)	The pulse width represents the changes in the quantity of electric charge with high-frequency capacitance regularly within a specified time.
Pulse Interval(us)	The time interval between pulses.
ID Type	Select between the User ID and Card number.

5.7 Network Diagnosis

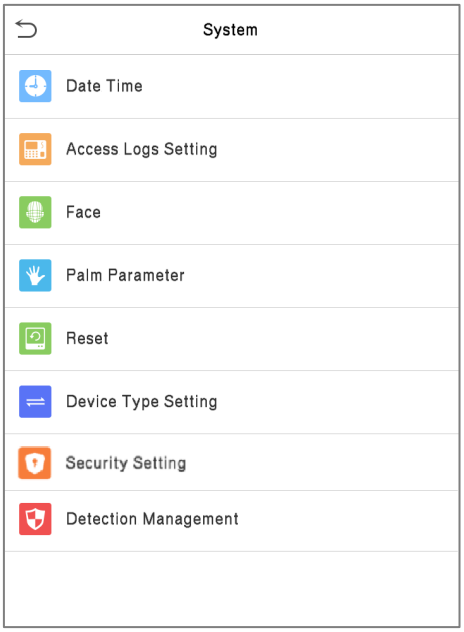


Menu	Description
IP address diagnostic test	The factory default address is 0.0.0.0. Please set the value as per the requirements.
Start the diagnostic test	Click start to automatically diagnose the network.

6 System Settings

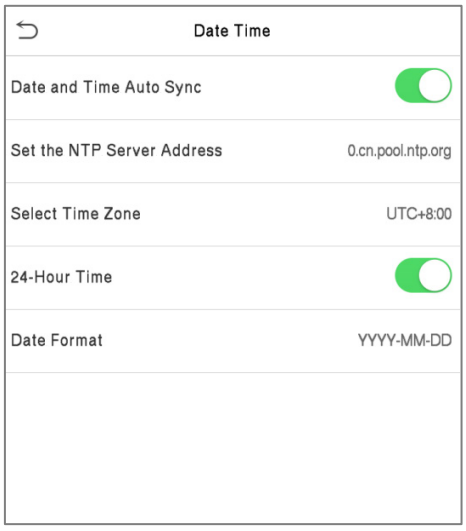
The System Settings is used to set the related system parameters to optimize the performance of the device.

Click **System** on the main menu interface.

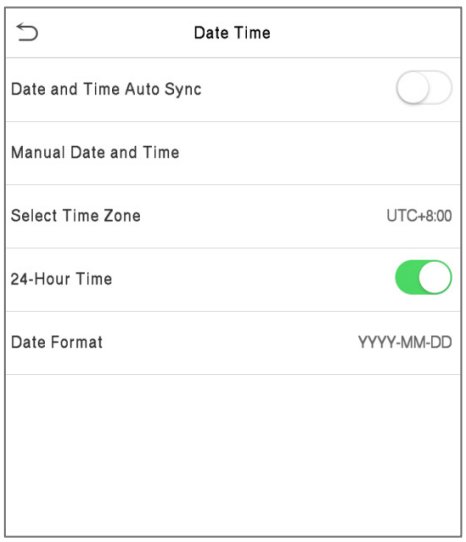


6.1 Date and Time

Click **Date Time** on the System interface.



1. The product supports the NTP synchronization time system by default. This function takes effect after **Date and Time Auto Sync** is enabled and the corresponding NTP server address link is set.
2. If users need to set date and time manually, disable **Date and Time Auto Sync** first, and then tap **Manual Time Setting** to set date and time and tap Confirm to save.



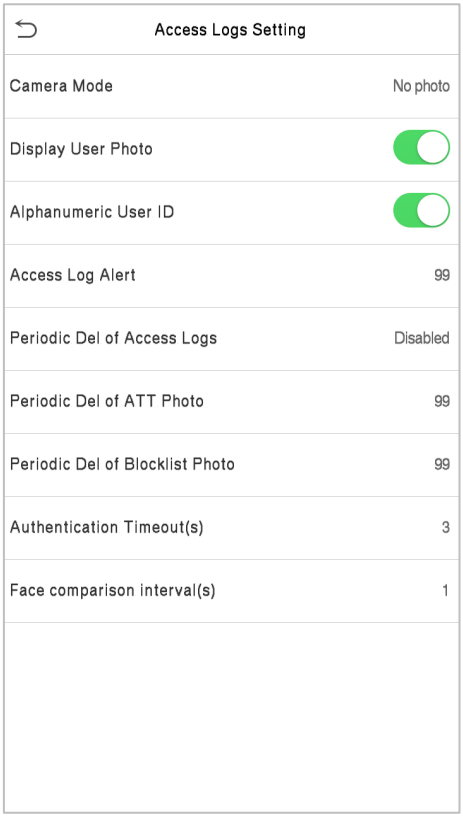
3. Click 24-Hour Time to enable or disable this format and select the date format.

When restoring the factory settings, the time (24-hour) and date format (YYYY-MM-DD) can be restored, but the device date and time cannot be restored.

Note: For example, the user sets the time of the device (18:35 on March 15, 2020) to 18:30 on January 1, 2021. After restoring the factory settings, the time of the device will change to 18:30, January 1, 2021.

6.2 Access Logs Setting

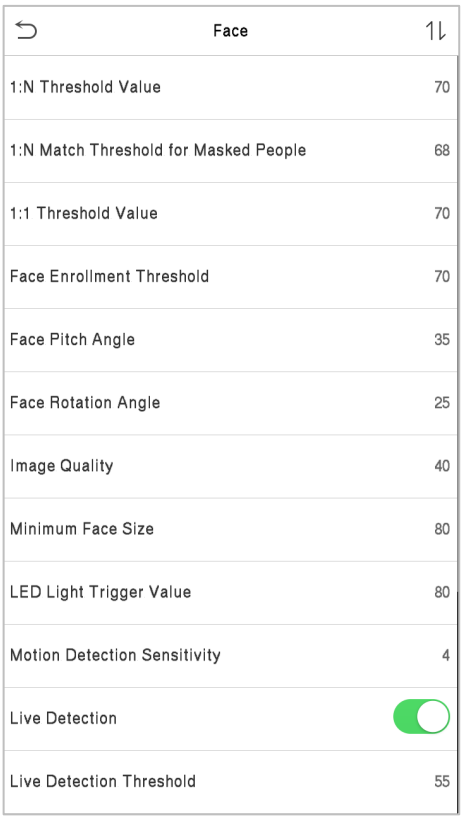
Click **Access Logs Setting** on the System interface.

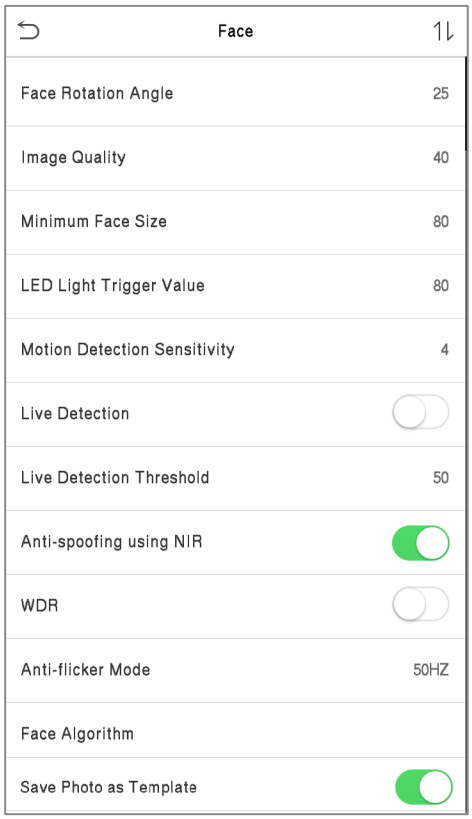


Function Name	Description
Camera Mode	This function is disabled by default. When enabled, a security prompt will pop-up and the sound of shutter in the camera will turn on mandatorily. There are 5 modes: **No Photo:** No photo is taken during user verification. **Take photo, no save:** Photo is taken but not saved during verification. **Take photo and save:** All the photos taken during verification is saved. **Save on successful verification:** Photo is taken and saved for each successful verification. **Save on failed verification:** Photo is taken and saved only for each failed verification.
Display User Photo	This function is disabled by default. When enabled, there will be a security prompt.
Alphanumeric User ID	Whether to support letters in employee ID.
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 its maximum capacity, the device automatically deletes a set of old access logs. Users may disable the function or set a valid value between 1 and 999.
Periodic Del of ATT Photo	When attendance photos reach its maximum capacity, the device automatically deletes a set of old attendance photos. Users may disable the function or set a valid value between 1 and 99.
Periodic Del of Blocklist Photo	When block listed photos reach its maximum capacity, the device automatically deletes a set of old block listed photos. Users may disable the function or set a valid value between 1 and 99.
Authentication Timeout(s)	The amount of time taken to display a successful verification message. Valid value: 1 to 9 seconds.
Face Comparison Interval(s)	After the interval identifying is clicked (selected), for example, if the comparison interval is set to 5 seconds, then the face recognition will verify the face every 5 seconds. Valid value: 0 to 9 seconds. 0 means continuous identifying, 1 to 9 means identifying at intervals.

6.3 Face Parameters

Click **Face** on the System interface.





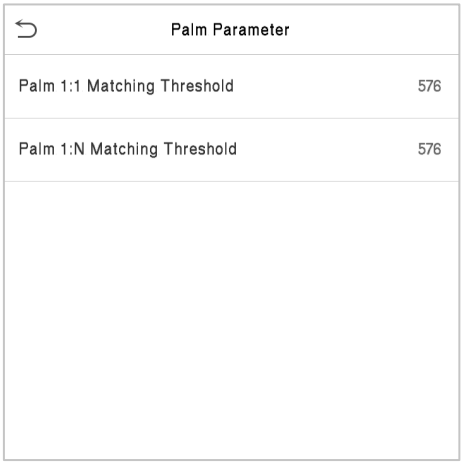
Menu	Description
1:N Threshold Value	Under 1:N verification mode, the verification will only be successful when the similarity between the acquired facial image and all registered facial templates is greater than the set value. The valid value ranges from 0 to 100. The higher the thresholds, the lower the misjudgement rate and the higher the rejection rate, and vice versa. It is recommended to set the default value of 47.
1:N Match Threshold for Masked People	Under 1:N verification mode, the device will perform similarity matching between the face currently wearing the mask and the registered face template in the device. When the similarity is greater than this value, it means the matching is successful, otherwise it means the matching fails. The valid value ranges from 0 to 100. The higher the thresholds, the lower the misjudgement rate and the higher the rejection rate, and vice versa. It is recommended to set the default value of 68.

1:1 Threshold Value	Under 1:1 verification mode, the verification will only be successful when the similarity between the acquired facial image and the facial templates enrolled in the device is greater than the set value. The valid value ranges from 0 to 100. The higher the thresholds, the lower the misjudgement rate and the higher the rejection rate, and vice versa. It is recommended to set the default value of 63.
Face Enrollment Threshold	During face enrollment, 1:N comparison is used to determine whether the user has already registered before. When the similarity between the acquired facial image and all registered facial templates is greater than this threshold, it indicates that the face has already been registered.
Face Pitch Angle	It is the pitch angle tolerance of a face for facial template registration and comparison. If a face's pitch angle exceeds this set value, it will be filtered by the algorithm, i.e. ignored by the terminal thus no registration and comparison interface will be triggered.
Face Rotation Angle	It is the rotation angle tolerance of a face for facial template registration and comparison. If a face's rotation angle exceeds this set value, it will be filtered by the algorithm, i.e. ignored by the terminal thus no registration and comparison interface will be triggered.
Image Quality	Image quality for facial registration and comparison. The higher the value, the clearer the image will be.
Minimum Face Size	Required for facial registration and comparison. If an object's size is smaller than this set value, the object will be filtered and not recognized as a face. This value can be understood as the face comparison distance. The farther the person is, the smaller the face is, and the smaller face pixel will be obtained by the algorithm. Therefore, adjusting this parameter can adjust the farthest comparison distance of faces. When the value is 0, the face comparison distance is not limited.
LED Light Triggered Threshold	This value controls the turning on and off of the LED light. The larger the value, the LED light will turn on or off more frequently.
Motion Detection Sensitivity	It sets the value for the amount of change in a camera's field of view known as potential motion detection that wakes up the terminal from standby to the comparison interface. The larger the value, the more sensitive the system would be, i.e., if a larger value is set, the comparison interface activates with much ease, and the motion detection is frequently triggered.

Live Detection	It detects the spoof attempt using visible light images to determine if the provided biometric source sample is of a real person (a live human being) or a false representation.
Live Detection Threshold	It facilitates judging whether the captured visible image is a real person (a live human being). The larger the value, the better the anti-spoofing performance using visible light.
Anti-spoofing using NIR	It uses near-infrared spectra imaging to identify and prevent fake photos and videos attack.
Binocular Live Detection Threshold	It is convenient to judge whether the near-infrared spectral imaging is fake photo and video. The larger the value, the better the anti-spoofing performance of near-infrared spectral imaging.
WDR	Wide Dynamic Range (WDR), which balances light and extends image visibility for surveillance videos under high contrast lighting scenes and improves object identification under bright and dark environments.
Anti-flicker Mode	Used when WDR is turned off. This helps reduce flicker when the device's screen flashes at the same frequency as the light.
Face Algorithm	Used to update or view the Major Version and Minor Version of the face algorithm, and to pause the update of the facial template .
Save Photo as Template	This function is enabled by default, and the menu interface supports enabling or disabling this function, and there is a security prompt when switching. When this function is disabled, it will indicate that there is a risk reminder: "**Face re-registration is required after an algorithm upgrade.**"
Notes	Improper adjustment of the exposure and quality parameters may severely affect the performance of the device. Please adjust the exposure parameter only under the guidance of the after-sales service personnel of our company.

6.4 Palm Parameters★

Click **Palm** on the System interface.

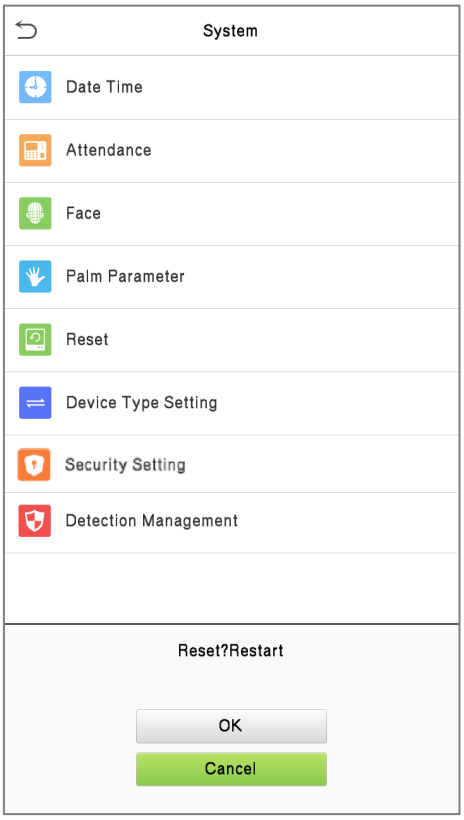


Menu	Description
Palm 1:1 Matching Threshold	Under 1:1 Verification Method, only when the similarity between the verifying palm and the user's registered palm is greater than this value, the verification succeeds.
Palm 1:N Matching Threshold	Under 1:N Verification Method, only when the similarity between the verifying palm and all registered palm is greater than this value, the verification succeeds.

6.5 Factory Reset

This option restores the device, such as communication settings and system settings, to factory settings (does not clear registered user data).

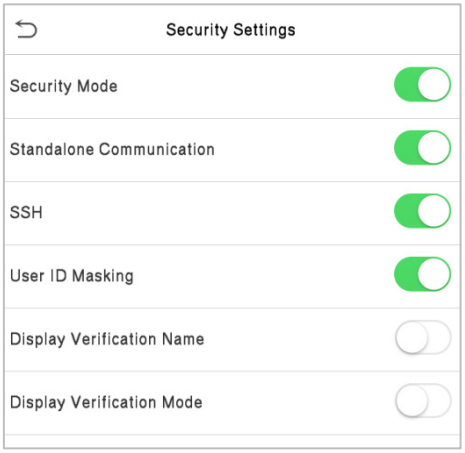
Click **Reset** on the System interface.



Click **OK** to reset.

6.6 Security Settings

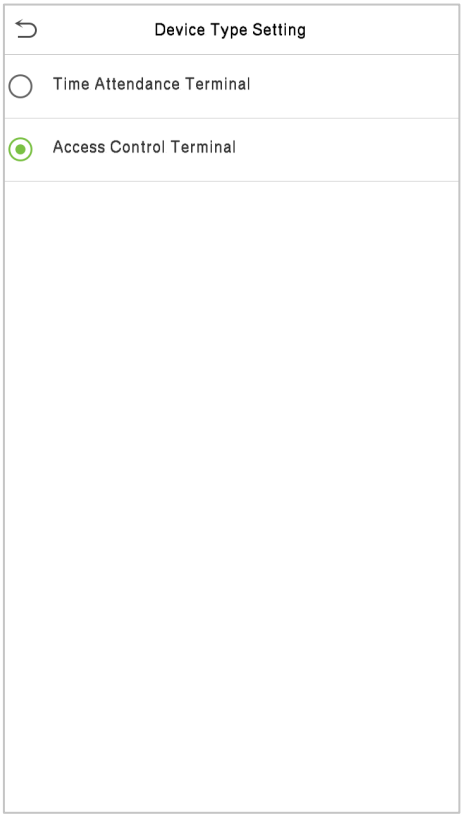
Tap **Security Settings** on the **System** interface.



Function Name	Description
Security Mode	When enabled, user information verification has a high level of security. This function can be enabled or disabled via the menu interface. When switching on and off, there are security prompts. All data will be deleted and the device will be restarted after confirmation. **Note:** After turning on the security mode, the product will forcibly enable the function of returning to the standby interface when the menu times out by default (default 60s). It does not support disabling in security mode, but it does support disabling in non-security mode. To configure, go to **Personalize** > **User Interface** > **Menu Screen Timeout(s)**.
Standalone Communication	By default, this function is disabled. This function can be enabled or disabled via the menu interface. When it is switched on, a security prompt appears, and the device will restart after you confirm.
SSH	The device does not support the Telnet feature, hence SSH is typically used for remote debugging. By default, SSH is enabled. The menu interface allows you to enable and disable SSH. When enabled, there will be a security prompt, but the device will not need to be restarted after confirmation.
User ID Masking	After enabled, the User ID will be partially displayed after the personnel verification result (only the User ID with more than 2 digits supports the masking display), and it is enabled by default.
Display Verification Name	After enabled, the user's name will be displayed after the personnel verification result. The verification result will not show the name after disabling it.
Display Verification Mode	After enabled, the personnel verification result will show the user's verification mode. The verification result will not show the verification mode after you disable it.

6.7 Device Type Setting

Click **Device Type Setting** on the **System** interface to configure the Device Type Setting settings.

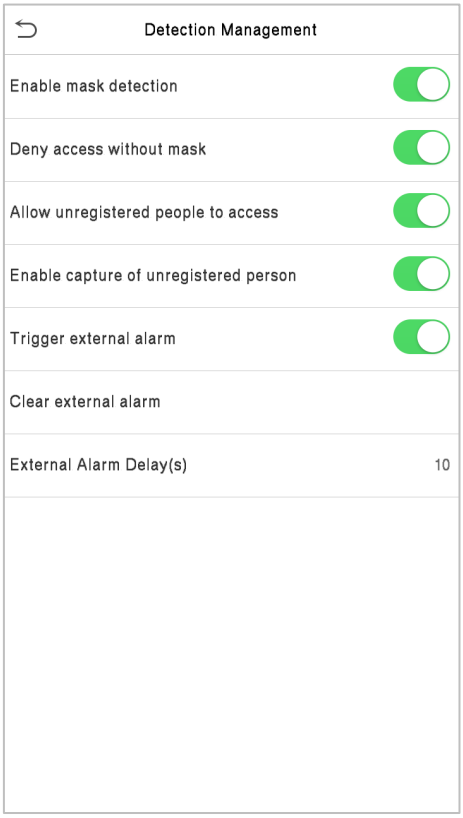


Function Name	Description
Time Attendance Terminal	Set the device as a time attendance terminal.
Access Control Terminal	Set the device as an access control terminal.

Note: After changing the device type, the device will delete all data and restart, and some functions will be adjusted accordingly.

6.8 Detection Management

Click **Detection Management** on the System interface.

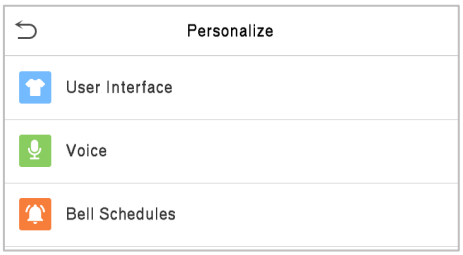


Function Name	Description
Enable Mask Detection	It enables or disables the mask detection function. When enabled, the device identifies whether the user is wearing a mask or not during verification.
Deny Access without Mask	It enables or disables the access of a person without mask. When enabled, the device denies access of a person, if not wearing a mask.
Allow Unregistered People to Access	It enables or disables the access of unregistered person. When enabled, the device allows the person to enter without registration.
Enable Capture of Unregistered Person	To enable or disable capturing the unregistered person. When enabled, the device will automatically capture the photo of the unregistered person, enabling this feature requires to enable **Allow unregistered people to access**.
Trigger External Alarm	When enabled, if the user is not wearing a mask, the system will trigger an alarm.
Clear External Alarm	It clears the triggered alarm records of the device.
External Alarm Delay(s)	It is the delay(s) time for triggering an external alarm. It can be set in seconds. Users may disable the function or set a value between1 to 255.

7 Personalize Settings

You may customize the interface settings, audio, and bell.

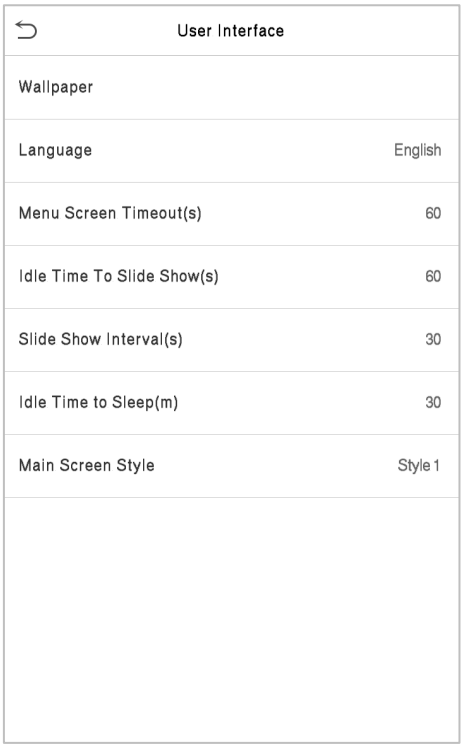
Click **Personalize** on the main menu interface.



7.1 Interface Settings

You can customize the display style of the main interface.

Click **User Interface** on the Personalize interface.

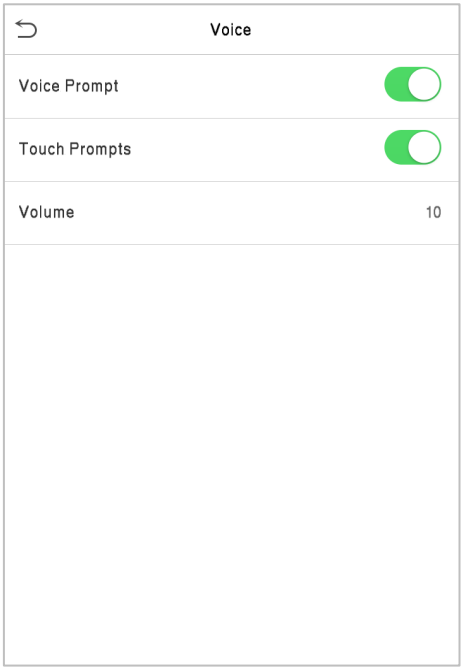


Menu	Description
Wallpaper	To select the main screen wallpaper according to your personal preference.
Language	To select the language of the device.
Menu Screen Timeout (s)	When there is no operation, and the time exceeds the set value, the device will automatically go back to the initial interface. You can disable the function or set the value between 60 and 99999 seconds.

Idle Time To Slide Show (s)	When there is no operation, and the time exceeds the set value, a slide show will be played. It can be disabled, or you may set the value between 3 and 999 seconds.
Slide Show Interval (s)	This refers to the time interval switching different slide show pictures. The function can be disabled, or you may set the interval between 3 and 999 seconds.
Idle Time To Sleep (m)	If you have activated the sleep mode, when there is no operation, the device will enter the standby mode. You can disable this function or set a value within 1-999 minutes.
Main Screen Style	To select the main screen style according to your personal preference.

7.2 Voice Settings

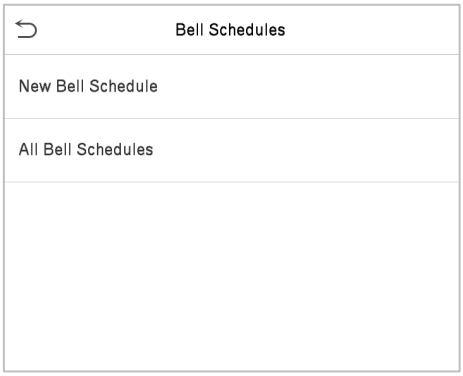
Click **Voice** on the Personalize interface.



Menu	Description
Voice Prompt	Select whether to enable voice prompts during operation.
Touch Prompt	Select whether to enable keypad sounds.
Volume	Adjust the volume of the device; valid value: 0 to 100.

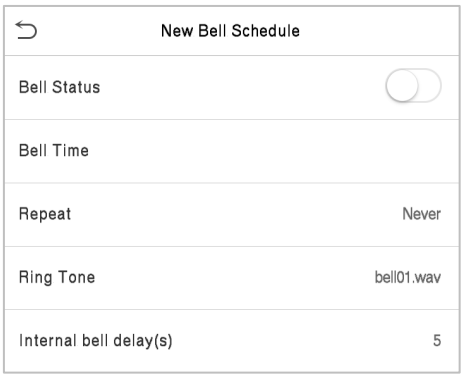
7.3 Bell Schedules

Click **Bell Schedules** on the Personalize interface.



Add a Bell

1. Click **New Bell Schedule** to enter the adding interface:



Menu	Description
Bell Status	Set whether to enable the bell status.
Bell Time	At this time of day, the device automatically rings the bell.
Repeat	Set the repetition cycle of the bell.
Ring Tone	Select a ring tone.
Internal bell delay(s)	Set the duration of the internal bell. Valid values range from 1 to 999 seconds.

2. Back to the Bell Schedules interface; click **All Bell Schedules** to view the newly added bell.

Edit a Bell

On the All Bell Schedules interface, click the bell to be edited.

Click **Edit**, the editing method is the same as the operations of adding a bell.

Delete a Bell

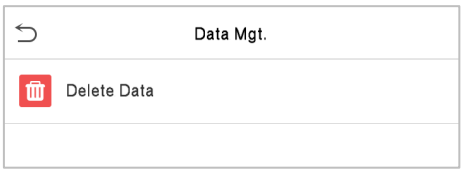
On the All Bell Schedules interface, click the bell to be deleted.

Click **Delete** and select [**Yes**] to delete the bell.

8 Data Management

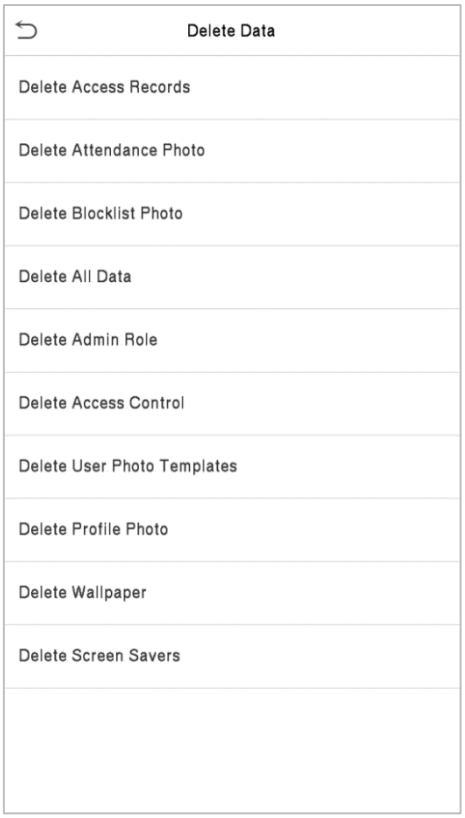
The Data Management is used to delete the relevant data in the device.

Click **Data Mgt.** on the main menu interface.



8.1 Delete Data

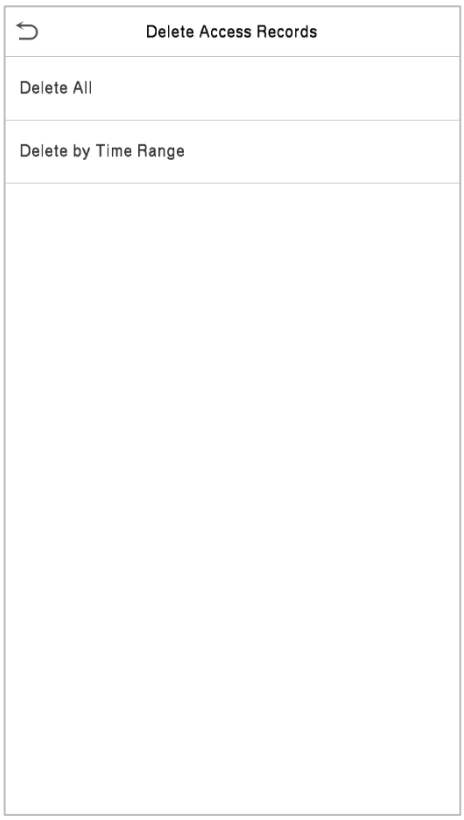
Click **Delete Data** on the Data Mgt. interface.



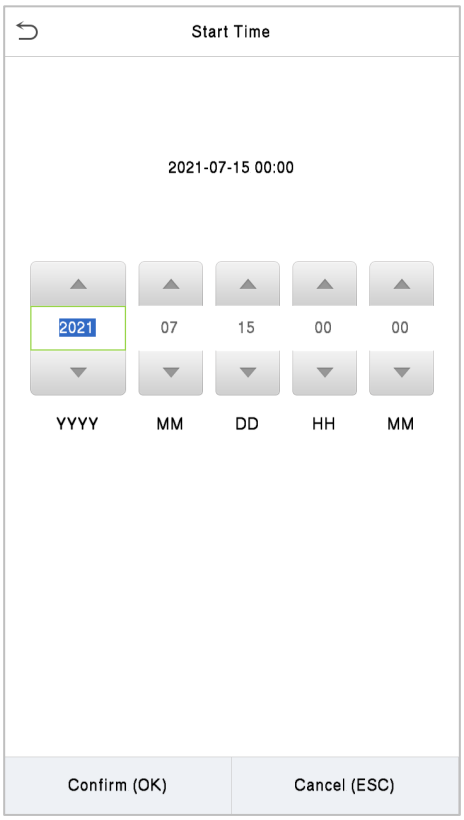
Function Name	Description
Delete Access Records	To delete attendance data/access records conditionally.
Delete Attendance Photo	To delete attendance photos of designated personnel.
Delete Blocklist Photo	To delete the photos taken during failed verifications.
Delete All Data	To delete information and attendance logs/access records of all registered users.
Delete Admin Role	To remove all administrator privileges.

Delete Access Control	To delete all access data.
Delete User Photo Templates	To delete user photo templates in the device. When deleting template photos, there is a risk reminder: "**Face re-registration is required after an algorithm upgrade.**"
Delete Profile Photo	To delete all user photos on the device.
Delete Wallpaper	To delete all wallpapers in the device.
Delete Screen Savers	To delete the screen savers in the device.

The user may select Delete All or Delete by Time Range when deleting the access records, attendance photos or block listed photos. Selecting Delete by Time Range, you need to set a specific time range to delete all data within a specific period.



Select Delete by Time Range

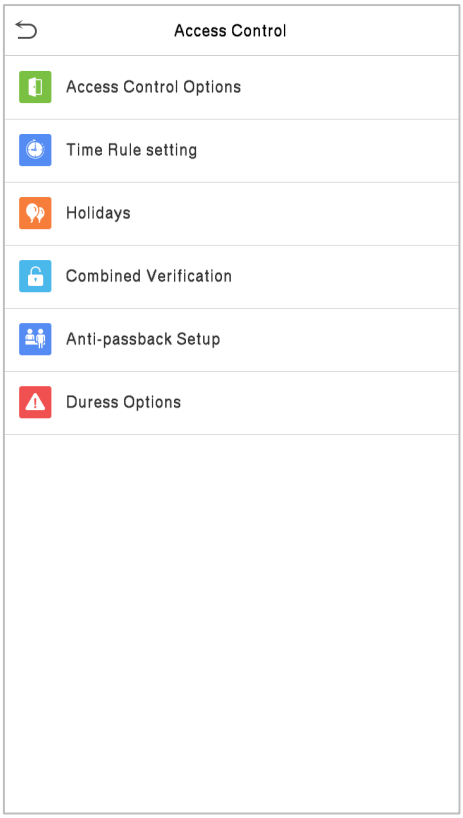


Set the time range and click OK

9 Access Control

Access Control is used to set the schedule of a door opening, locks control and other parameter settings related to access control.

Click **Access Control** on the main menu interface.



To gain access, the registered user must meet the following conditions:

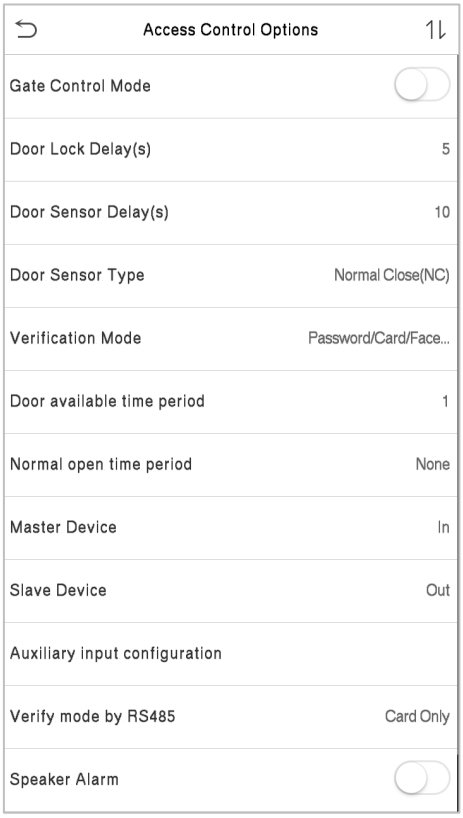
1. The current door unlock time should be within any valid time zone of the user time period.
2. The user's group must be in the door unlock combination (when there are other groups in the same access combo, verification of members of those groups are also required to unlock the door).

In default settings, new users are allocated into the first group with the default group time zone and access combo as "1" and set in an unlocking state.

9.1 Access Control Options

This option is used to set the parameters of the control lock of the device and the related parameters.

Click **Access Control Options** on the Access Control interface.



Function Name	Description
Gate Control Mode	It toggles between **ON** or **OFF** switch to get into gate control mode or not. When set to **ON**, the interface removes the Door lock relay, Door sensor relay, and Door sensor type options.
Door Lock Delay (s)	The length of time that the device controls the electric lock to be in unlock state. Valid value: 1 to 10 seconds; 0 seconds represents disabling the function.
Door Sensor Delay (s)	If the door is not locked and is left open for a certain duration (Door Sensor Delay), an alarm will be triggered. The valid value of Door Sensor Delay ranges from 1 to 255 seconds.
Door Sensor Type	There are three Sensor types: **None, Normal Open,** and **Normal Closed**. **None:** It means the door sensor is not in use. **Normally Open:** It means the door is always left open when electric power is on. **Normally Closed:** It means the door is always left closed when electric power is on.
Verification Mode	The supported verification mode includes password/face, User ID only, password, face only, and face + password.

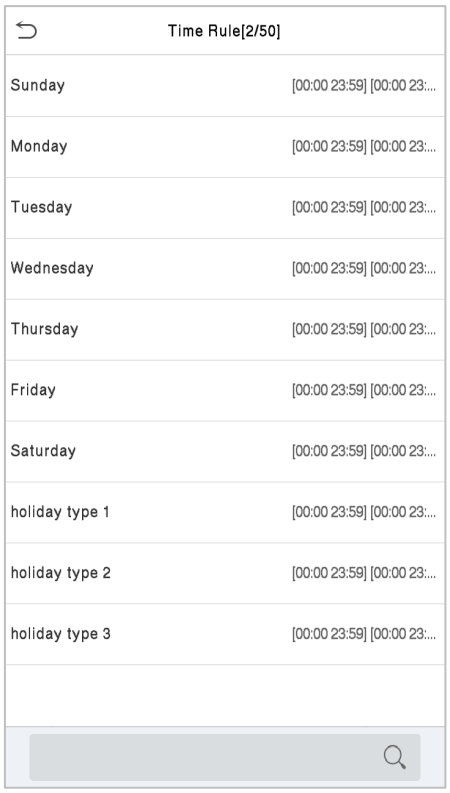
Door Available Time Period	It sets the timing for the door so that the door is accessible only during that period.
Normal Open time Period	It is the scheduled time-period for "Normal Open" mode so that the door is always open during this period.
Master Device	While configuring the master and slave devices, you may set the state of the master as **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	While configuring the master and slave devices, you may 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.
Auxiliary Input Configuration	Sets the door unlock time period and auxiliary output type of the auxiliary terminal device. Auxiliary output types include None, Trigger door open, Trigger Alarm, Trigger door open and Alarm.
Verify Mode by RS485	The verification mode is used when the device is used either as a host or slave. The supported verification mode includes Card only, and Card + Password.
Speaker Alarm	It transmits a sound alarm or disassembly alarm from the local. When the door is closed or the verification is successful, the system cancels the alarm from the local.
Reset Access Setting	The access control reset parameters include door lock delay, door sensor delay, door sensor type, verification mode, door available time period, normal open time period, master device, and alarm. However, erased access control data in Data Mgt. is excluded.

9.2 Time Rule Setting

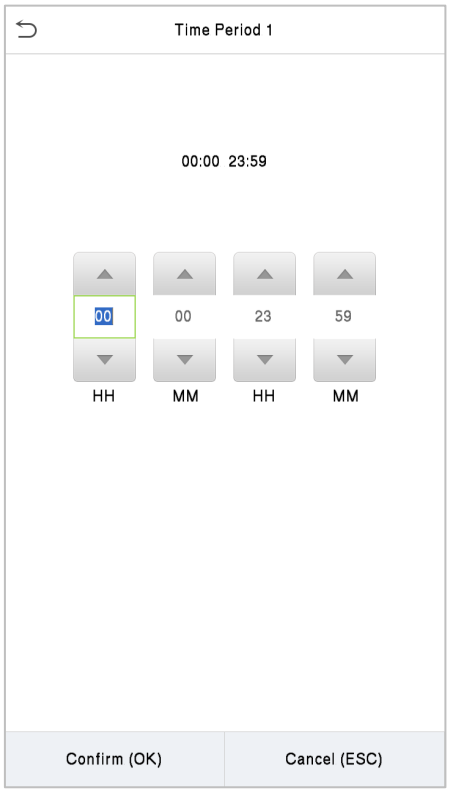
Click **Time Rule Setting** on the Access Control interface to configure the time settings.

- The entire system can define up to 50 Time Periods.
- Each time-period represents **10** Time Zones, i.e., **1** week and **3** holidays, and each time zone is a standard 24 hour period per day and the user can only verify within the valid time-period.
- One can set a maximum of 3 time periods for every time zone. The relationship among these time-periods is "**OR**". Thus, when the verification time falls in any one of these time-periods, the verification is valid.
- The Time Zone format of each time-period is **HH MM-HH MM**, which is accurate to minutes according to the 24-hour clock.

Click the grey box to search the required Time Zone and specify the required Time Zone number (maximum up to 50 zones).



On the selected Time Zone number interface, click on the required day (that is Monday, Tuesday, etc.) to set the time.



Specify the start and the end time, and then click **OK**.

Note:

1) The door is inaccessible for the whole day when the End Time occurs before the Start Time (such as **23:57~23:56**).

2) It is the time interval for valid access when the End Time occurs after the Start Time (such as **08:00~23:59**).

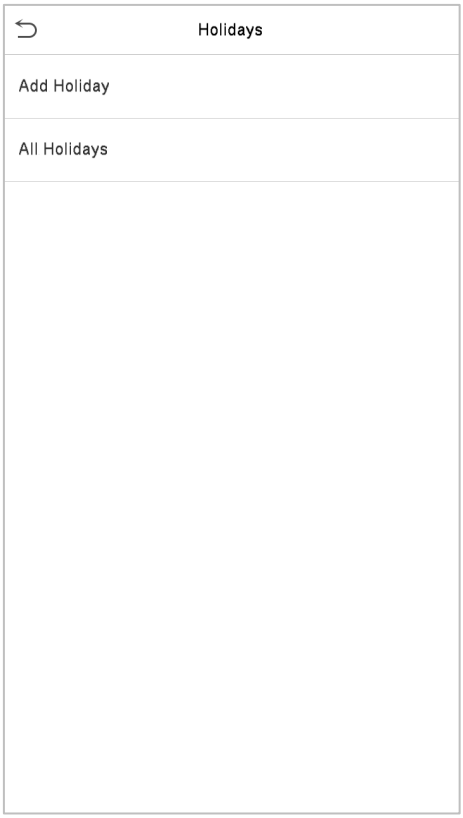
3) The door is accessible for the whole day when the End Time occurs after the Start Time (such that Start Time is **00:00** and End Time is **23:59**).

4) The default Time Zone 1 indicates that the door is open all day long.

9.3 Holiday Settings

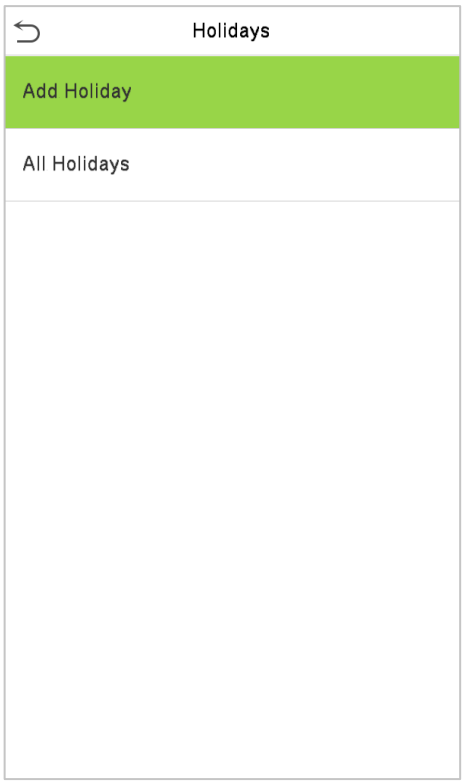
Whenever there is a holiday, you may need a special access time; but changing everyone's access time one by one is extremely cumbersome, so you can set a holiday access time which applies to all the employees, and the user will be able to open the door during the holidays.

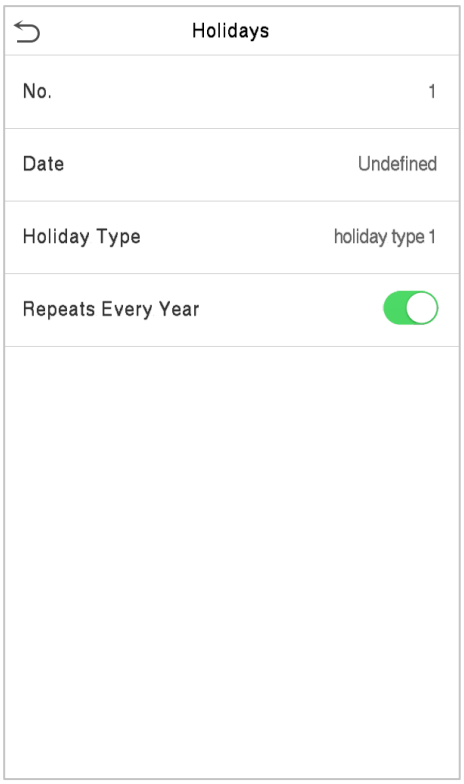
Click **Holidays** on the Access Control interface.



Add a New Holiday

Click **Add Holiday** on the Holidays interface and set the holiday parameters.





Edit a Holiday

On the Holidays interface, select a holiday item to be modified. Click **Edit** to modify holiday parameters.

Delete a Holiday

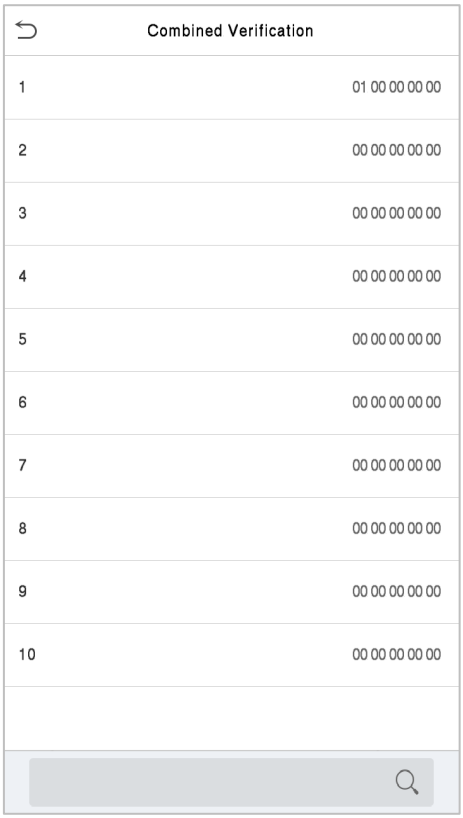
On the Holidays interface, select a holiday item to be deleted and click **Delete**. Click **OK** to confirm the deletion. After deletion, this holiday is no longer displayed on All Holidays interface.

9.4 Combined Verification Settings

Access groups are arranged into different door-unlocking combinations to achieve multiple verifications and strengthen security.

In a door-unlocking combination, the range of the combined number N is $0 \leq N \leq 5$, and the number of members N may all belong to one access group or may belong to five different access groups.

Click **Combined Verification** on the Access Control interface.



Click the door-unlocking combination to be set. Click the up and down arrows to input the combination number, then press OK.

Examples:

The door-unlocking combination 1 is set as (01 03 05 06 08), indicating that the unlocking combination 1 consists of 5 people, and the 5 individuals are from 5 groups, namely, access control group 1 (AC group 1), AC group 3, AC group 5, AC group 6, and AC group 8, respectively.

The door-unlocking combination 2 is set as (02 02 04 04 07), indicating that the unlocking combination 2 consists of 5 people; the first two are from AC group 2, the next two are from AC group 4, and the last person is from AC group 7.

The door-unlocking combination 3 is set as (09 09 09 09 09), indicating that there are 5 people in this combination; all of which are from AC group 9.

The door-unlocking combination 4 is set as (03 05 08 00 00), indicating that the unlocking combination 4 consists of three people. The first person is from AC group 3, the second person is from AC group 5, and the third person is from AC group 8.

Delete a Door-unlocking Combination

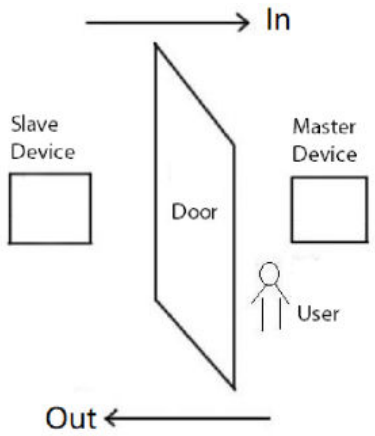
Set all the group numbers as 0 if you want to delete door-unlocking combinations.

9.5 Anti-Passback Setup

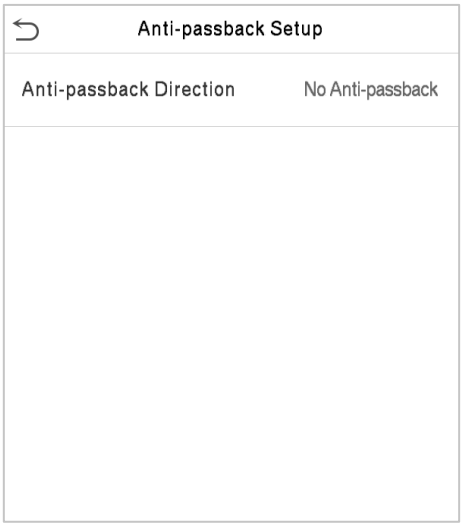
A user may be followed by some person(s) to enter the door without verification, resulting in a security breach. So, to avoid such situations, the Anti-Passback option was developed. Once it is enabled, the check-in and check-out record must occur alternatively to open the door to represent a consistent pattern.

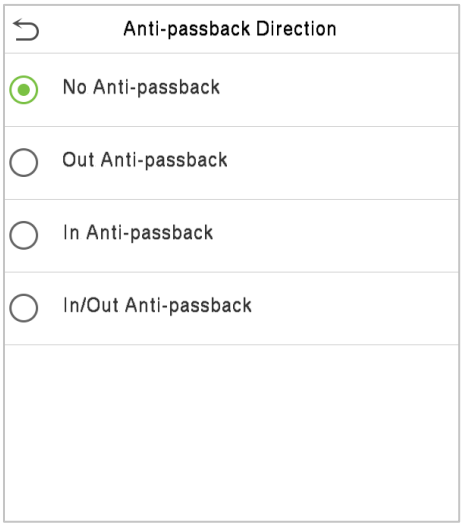
This function requires two devices to work together:

One device is installed on the indoor side of the door (master device), and the other one is installed on the outdoor side of the door (the slave device). The two devices communicate via the Wiegand signal. The Wiegand format and Output type (User ID / Card Number) adopted by the master device and slave device must be consistent.



Click **Anti-Passback Setup** on the **Access Control** interface.



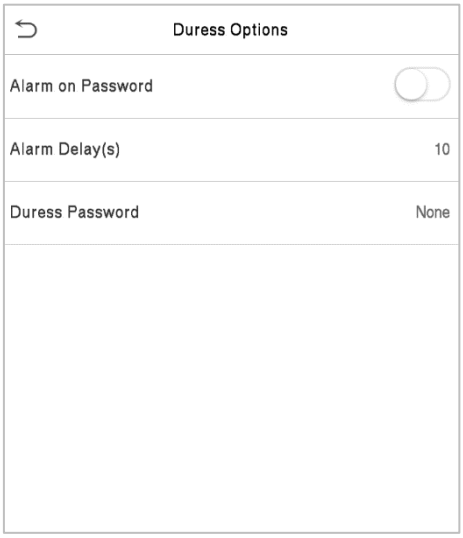


Function Name	Description
Anti-Passback Direction	**No Anti-Passback:** The Anti-Passback function is disabled, which means successful verification through either the master device or slave device can unlock the door. The attendance state is not saved in this option. **Out Anti-Passback:** The user can check-out only if the last record is a check-in record otherwise an alarm is raised. However, the user can check-in freely. **In Anti-Passback:** The user can check-in again only if the last record is a check-out record otherwise an alarm is raised. However, the user can check-out freely. **In/Out Anti-Passback:** In this case, a user can check-in only if the last record is a check-out or the user can check-out only if the last record is a check-in otherwise the alarm is triggered.

9.6 Duress Options Settings

If a user activated the duress verification function with specific authentication method(s), when he/she is under coercion during authentication with such method, the device will unlock the door as usual, but at the same time a signal will be sent to trigger the alarm.

Click **Duress Options** on the Access Control interface.

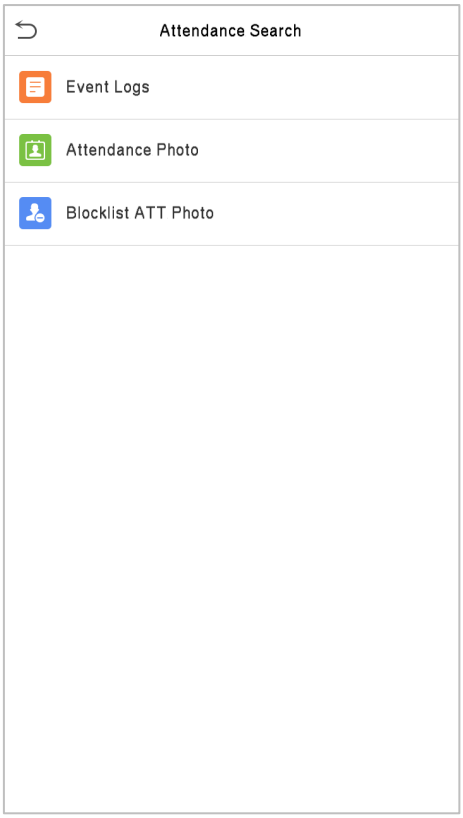


Function Name	Description
Alarm on Password	When a user uses the password verification method, an alarm signal is generated only when the password verification is successful otherwise there is no alarm signal.
Alarm Delay (s)	The alarm signal does not transmit until the alarm delay time elapses. The value ranges from 1 to 999 seconds.
Duress Password	Set the 6-digit duress password. When the user enters this duress password for verification, an alarm signal is generated.

10 Attendance Search

Once the identity of a user is verified, the access record is saved in the device. This function enables users to check their event logs.

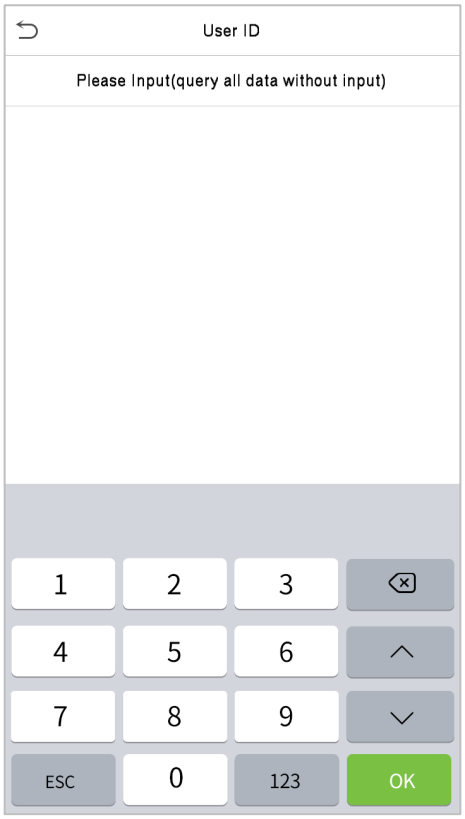
Select **Attendance Search** on the **Main Menu** interface to search for the required event logs.



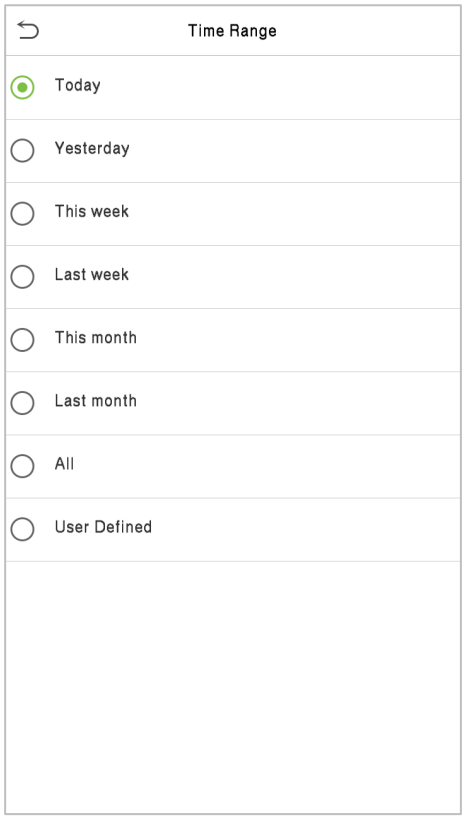
The process of searching for attendance and blocklist photos is similar to that of searching for event logs. The following is an example of searching for event logs.

On the **Attendance Search** interface, click **Event Logs** to search for the required record.

1. Enter the user ID to be searched and click OK. If you want to search for records of all users, click OK without entering any user ID.

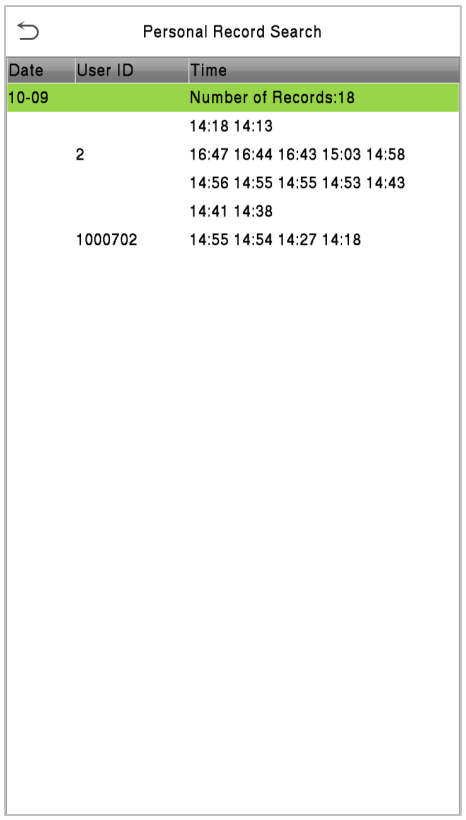


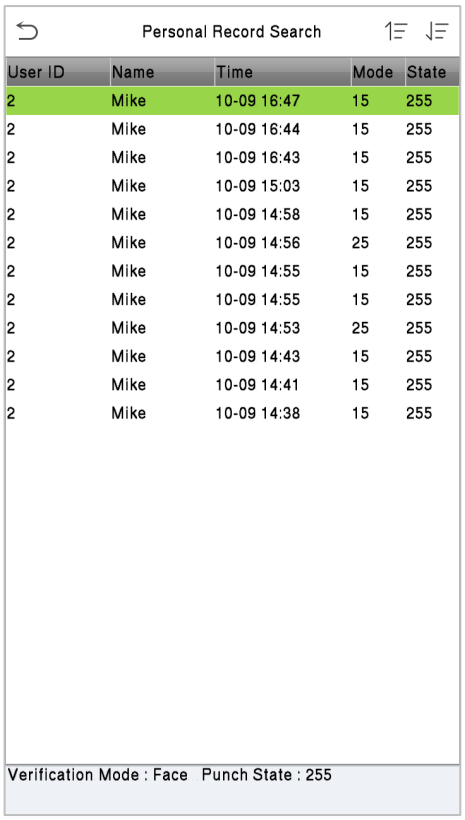
2. Select the time range in which the records you want to search for.



3. The record search succeeds. Click the record in green to view its details.

4. The below figure shows the details of the selected record.

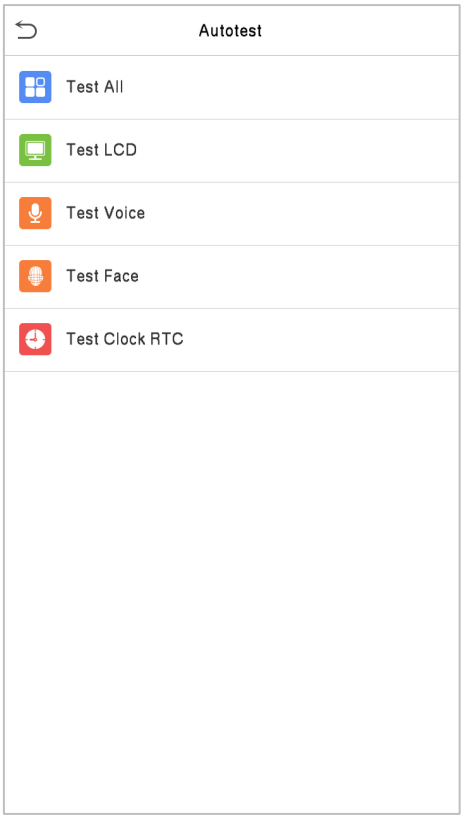




11 Autotest

To automatically test whether all modules in the device function properly, which include the LCD, Audio, Camera and real-time clock (RTC).

Click **Autotest** on the main menu interface.

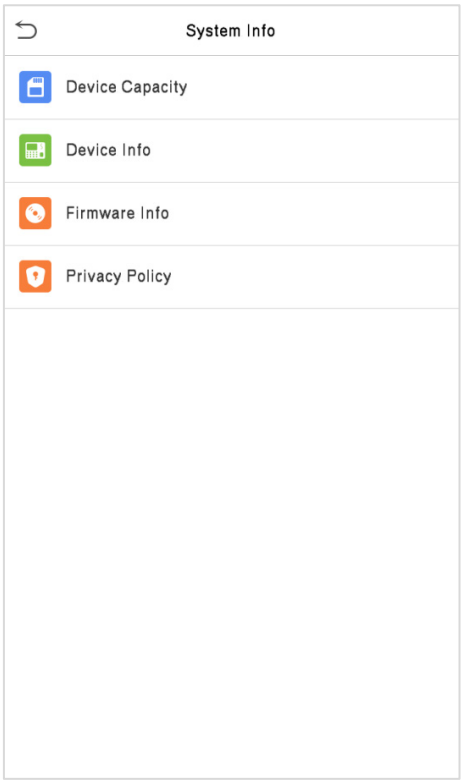


Menu	Description
Test All	To automatically test whether the LCD, audio, camera and RTC are normal.
Test LCD	To automatically test the display effect of LCD screen by displaying full-color, pure white, and pure black to check whether the screen displays the colors normally.
Test Voice	To automatically test whether the audio files stored in the device are complete and the voice quality is good.
Test Face	To test if the camera functions properly by checking the pictures taken to see if they are clear enough.
Test Clock RTC	To test the RTC. The device tests whether the clock works normally and accurately with a stopwatch. Touch the screen to start counting and press it again to stop counting.

12 System Information

With the system information option, you can view the storage status, the version information of the device, and so on.

Click **System Info** on the main menu interface.



Menu	Description
Device Capacity	Displays the current device's user storage, password, palm★, face and card storage, administrators, attendance records, attendance and blocklist photos, and Profile photos.
Device Info	Displays the Device's name, Serial number, MAC Address, Face and Palm algorithm★ version information, platform information, MCU Version, manufacturer and manufacture Date.
Firmware Info	Displays the Firmware version and other version information of the device.
Privacy Policy	The privacy policy control will appear when the gadget turns on for the first time. After clicking "**I have read it**," the customer can use the product regularly. Click **System Info** -> **Privacy Policy** to view the content of the privacy policy. The privacy policy's content does not allow for U disc export. **Note:** The current privacy policy's text is only available in Simplified Chinese/English. However, translation of other multi-language content is underway, with more iterations.

13 Connect to ZKBioAccess IVS Software

13.1 Set the Communication Address

Device Side

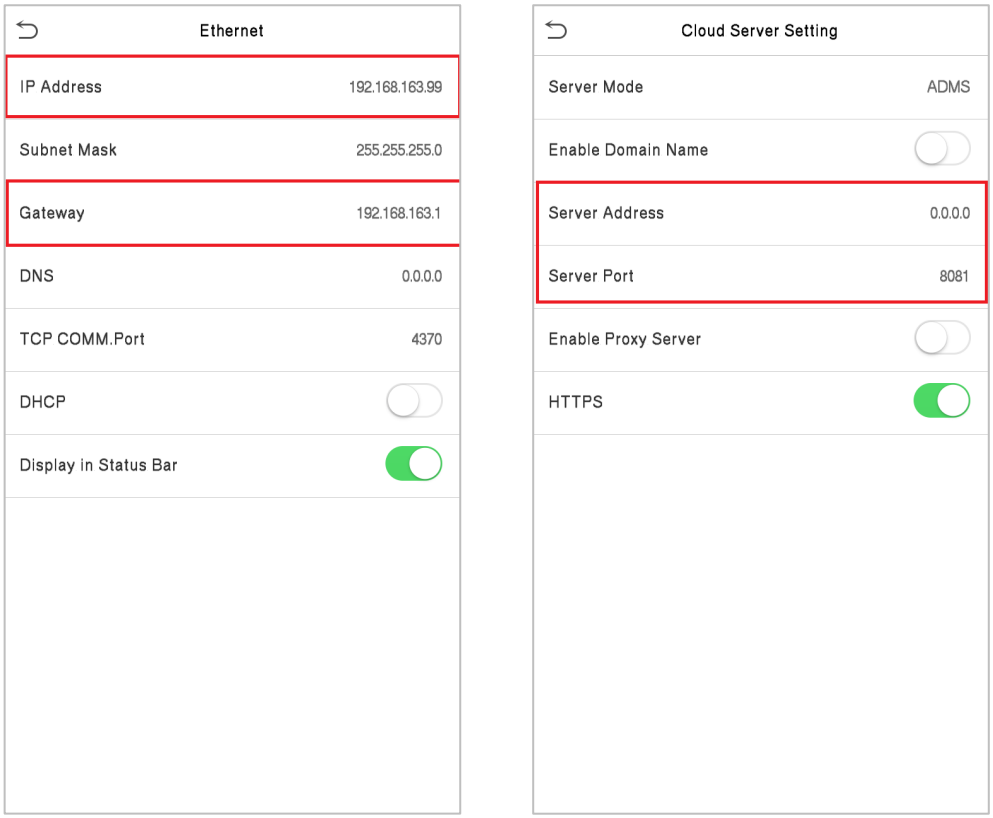
1. Click **COMM.** > **Ethernet** in the main menu to set the IP address and gateway of the device.

(**Note:** The IP address should be able to communicate with the ZKBioAccess IVS server, preferably in the same network segment with the server address)

2. In the main menu, click **COMM.** > **Cloud Server Setting** to set the server address and server port.

   Server address: Set the IP address as of ZKBioAccess IVS server.

   Server port: Set the server port as of ZKBioAccess IVS(The default is 8088).



Software Side

Login to ZKBioAccess IVS software, click **System** > **Communication** > **Communication Monitor** to set the ADMS service port, as shown in the figure below:

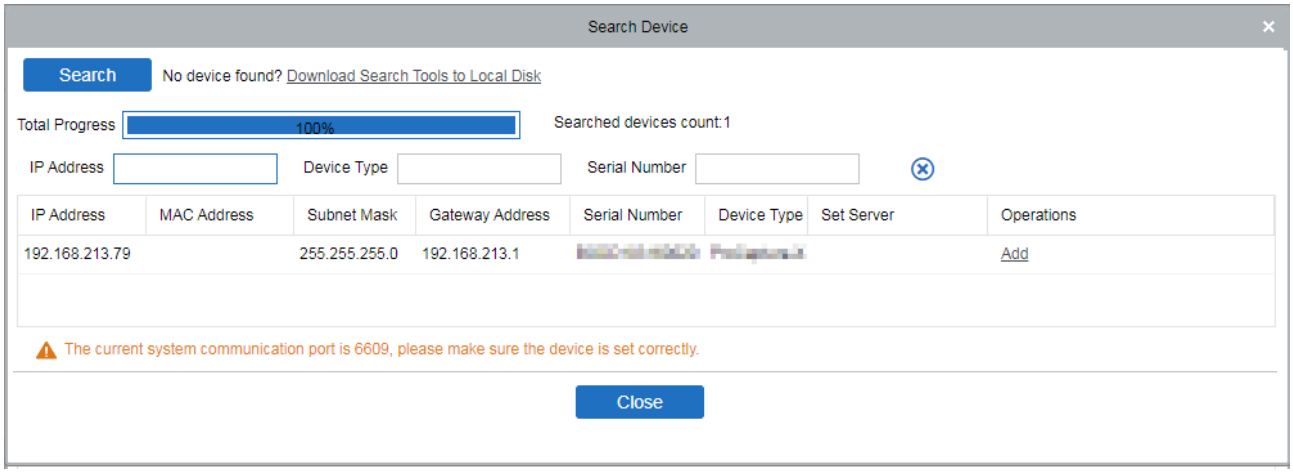
13.2 Add Device on the Software

Add the device by searching. The process is as follows:

1) Click **Access Control** > **Device** > **Search Device**, to open the Search interface in the software.

2) Click **Search**, and it will prompt [**Searching**……].

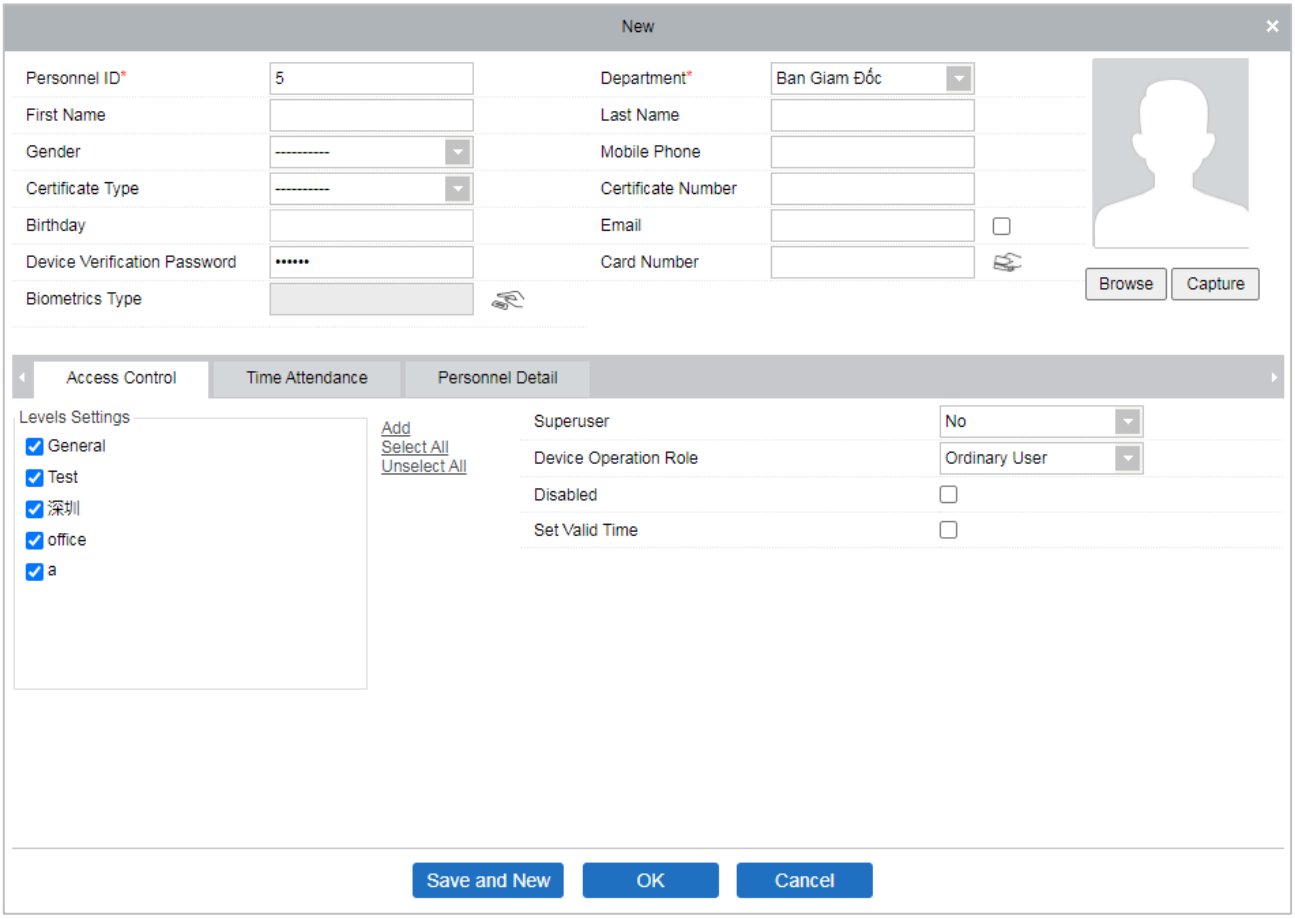
3) After searching, the list and total number of access controllers will be displayed.



4) Click [**Add**] in operation column, a new window will pop-up. Select Icon type, Area, and Add to Level from each dropdown and click [**OK**] to add the device.

13.3 Add Personnel on the Software

1. Click **Personnel** > **Person** > **New**:



2. Fill in all the required fields and click [**OK**] to register a new user.
3. Click **Access > Device > Device Control > Synchronize All Data to Devices** to synchronize all the data to the device including the new users.

For more details, please refer to the *ZKBioAccess IVS User Manual*.

Appendix 1

Requirements for Live Collection and Registration of Visible Light Face Templates

1) It is recommended to perform registration in an indoor environment with an appropriate light source without underexposure or overexposure.
2) Do not point towards outdoor light sources like door or window or other strong light sources.
3) Dark-color apparels which are different from the background color are recommended for registration.
4) Please show your face and forehead, and do not cover your face and eyebrows with your hair.
5) It is recommended to show a plain facial expression. Smile is acceptable, but do not close your eyes, or incline your head to any orientation. Two images are required for persons with eyeglasses, one image with eyeglasses and one other without eyeglasses.
6) Do not wear accessories like scarf or mask that may cover your mouth or chin.
7) Please face right towards the capturing device, and locate your face in the image capturing area as shown in Image 1.
8) Do not include more than one face in the capturing area.
9) 50cm to 80cm is recommended as a capturing distance, adjustable subject to body height.

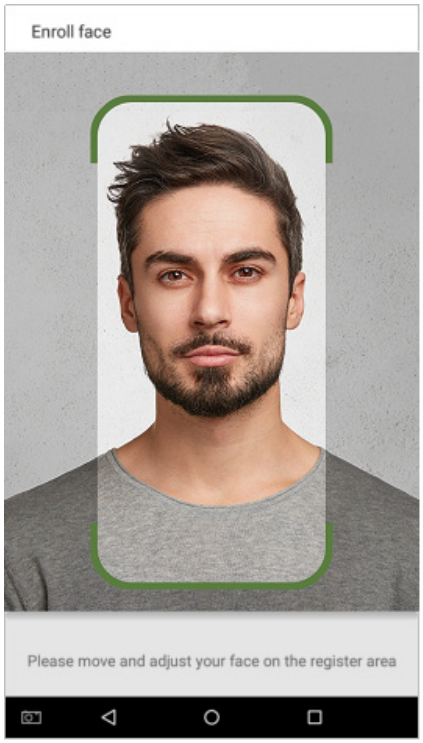


Image1 Face Capture Area

Requirements for Visible Light Digital Face Template Data

The digital photo should be straight-edged, colored, half-portrayed with only one person, and the person should be uncharted and not in uniform. Persons who wear eyeglasses should remain to put on eyeglasses for photo capturing.

Eye Distance

200 pixels or above are recommended with no less than 115 pixels of distance.

Facial Expression

A plain face or smile with eyes naturally open is recommended.

Gesture and Angle

The horizontal rotating angle should not exceed ±10°, elevation should not exceed ±10°, and the depression angle should not exceed ±10°.

Accessories

Masks and colored eyeglasses are not allowed. The frame of the eyeglasses should not shield the eyes and should not reflect light. For persons with thick eyeglasses frame, it is recommended to capture two images, one with eyeglasses and the other one without eyeglasses.

Face

The image must have clear contour, real scale, evenly distributed light, and no shadow.

Image Format

Should be in BMP, JPG or JPEG.

Data Requirement

Should comply with the following requirements:

1) White background with dark-colored apparel.
2) 24-bit true-color mode.
3) JPG format compressed image with not more than 20 KB size.
4) Definition rate between 358 x 441 to 1080 x 1920.
5) The vertical scale of the head and body should be 2:1.
6) The photo should include the captured person's shoulders at the same horizontal level.
7) The captured person should have eyes-open and with clearly seen iris.
8) A plain face or smile is preferred, showing teeth is not preferred.
9) The captured person should be clearly seen, natural in color, and without image obvious twist, no shadow, light spot or reflection in face or background, and appropriate contrast and lightness level.

Appendix 2

Privacy Policy

Notice:

Before using our products and services, please read carefully and understand all the rules and provisions of this Privacy Policy. If you do not agree to the relevant agreement or any of its terms, you must stop using our products and services.

I. Collected Information

To ensure the normal product operation and help the service improvement, we will collect the information voluntarily provided by you or provided as authorized by you during registration and use or generated as a result of your use of services.

1. **User Registration Information:** At your first registration, the feature template (**Fingerprint template/Face template/Palm template**) will be saved on the device according to the device type you have selected to verify the unique similarity between you and the User ID you have registered. You can optionally enter your Name and Code. The above information is necessary for you to use our products. If you do not provide such information, you cannot use some features of the product regularly.

2. **Product information:** According to the product model and your granted permission when you install and use our services, the related information of the product on which our services are used will be collected when the product is connected to the software, including the Product Model, Firmware Version Number, Product Serial Number, and Product Capacity Information. **When you connect your product to the software, please carefully read the privacy policy for the specific software.**

II. Product Security and Management

1. When you use our products for the first time, you shall set the Administrator privilege before performing specific operations. Otherwise, you will be frequently reminded to set the Administrator privilege when you enter the main menu interface. **If you still do not set the Administrator privilege after receiving the system prompt, you should be aware of the possible security risk (for example, the data may be manually modified).**
2. All the functions of displaying the biometric information are disabled in our products by default. You can choose Menu > System Settings to set whether to display the biometric information. If you enable these functions, we assume that you are aware of the personal privacy security risks specified in the privacy policy.

3. Only your user ID is displayed by default. You can set whether to display other user verification information (such as Name, Department, Photo, etc.) under the Administrator

privilege. **If you choose to display such information, we assume that you are aware of the potential security risks (for example, your photo will be displayed on the device interface).**

4. The camera function is disabled in our products by default. If you want to enable this function to take pictures of yourself for attendance recording or take pictures of strangers for access control, the product will enable the prompt tone of the camera. **Once you enable this function, we assume that you are aware of the potential security risks.**

5. All the data collected by our products is encrypted using the AES 256 algorithm. All the data uploaded by the Administrator to our products are automatically encrypted using the AES 256 algorithm and stored securely. If the Administrator downloads data from our products, we assume that you need to process the data and you have known the potential security risk. In such a case, you shall take the responsibility for storing the data. You shall know that some data cannot be downloaded for sake of data security.

6. All the personal information in our products can be queried, modified, or deleted. If you no longer use our products, please clear your personal data.

III. How we handle personal information of minors

Our products, website and services are mainly designed for adults. Without consent of parents or guardians, minors shall not create their own account. If you are a minor, it is recommended that you ask your parents or guardian to read this Policy carefully, and only use our services or information provided by us with consent of your parents or guardian.

We will only use or disclose personal information of minors collected with their parents' or guardians' consent if and to the extent that such use or disclosure is permitted by law or we have obtained their parents' or guardians' explicit consent, and such use or disclosure is for the purpose of protecting minors.

Upon noticing that we have collected personal information of minors without the prior consent from verifiable parents, we will delete such information as soon as possible.

Eco-friendly Operation

The product's "eco-friendly operational period" refers to the time during which this product will not discharge any toxic or hazardous substances when used in accordance with the prerequisites in this manual.

The eco-friendly operational period specified for this product does not include batteries or other components that are easily worn down and must be periodically replaced. The battery's eco-friendly operational period is 5 years.

Hazardous or Toxic substances and their quantities

Component Name	Hazardous/Toxic Substance/Element					
	Lead (Pb)	Mercury (Hg)	Cadmium (Cd)	Hexavalent Chromium (Cr6+)	Polybrominated Biphenyls (PBB)	Polybrominated Diphenyl Ethers (PBDE)
Chip Resistor	×	○	○	○	○	○
Chip Capacitor	×	○	○	○	○	○
Chip Inductor	×	○	○	○	○	○
Diode	×	○	○	○	○	○
ESD component	×	○	○	○	○	○
Buzzer	×	○	○	○	○	○
Adapter	×	○	○	○	○	○
Screws	○	○	○	×	○	○

○ indicates that the total amount of toxic content in all the homogeneous materials is below the limit as specified in SJ/T 11363—2006.

× indicates that the total amount of toxic content in all the homogeneous materials exceeds the limit as specified in SJ/T 11363—2006.

Note: 80% of this product's components are manufactured using non-toxic and eco-friendly materials. The components which contain toxins or harmful elements are included due to the current economic or technical limitations which prevent their replacement with non-toxic materials or elements.