User Manual

F35

Date: December 2023

Doc Version: 1.1

English

Thank you for choosing our product. Please read the instructions carefully before operation. Follow these instructions to ensure that the product is functioning properly. The images shown in this manual are for illustrative purposes only.

For further details, please visit our Company's website www.zkteco.com.

Copyright © 2023 ZKTECO CO., LTD. All rights reserved.

Without the prior written consent of ZKTeco, no portion of this manual can be copied or forwarded in any way or form. All parts of this manual belong to ZKTeco and its subsidiaries (hereinafter the "Company" or "ZKTeco").

Trademark

ZKTeco is a registered trademark of ZKTeco. Other trademarks involved in this manual are owned by their respective owners.

Disclaimer

This manual contains information on the operation and maintenance of the ZKTeco equipment. The copyright in all the documents, drawings, etc. in relation to the ZKTeco supplied equipment vests in and is the property of ZKTeco. The contents hereof should not be used or shared by the receiver with any third party without express written permission of ZKTeco.

The contents of this manual must be read as a whole before starting the operation and maintenance of the supplied equipment. If any of the content(s) of the manual seems unclear or incomplete, please contact ZKTeco before starting the operation and maintenance of the said equipment.

It is an essential pre-requisite for the satisfactory operation and maintenance that the operating and maintenance personnel are fully familiar with the design and that the said personnel have received thorough training in operating and maintaining the machine/unit/equipment. It is further essential for the safe operation of the machine/unit/equipment that personnel has read, understood and followed the safety instructions contained in the manual.

In case of any conflict between terms and conditions of this manual and the contract specifications, drawings, instruction sheets or any other contract-related documents, the contract conditions/documents shall prevail. The contract specific conditions/documents shall apply in priority.

ZKTeco offers no warranty, guarantee or representation regarding the completeness of any information contained in this manual or any of the amendments made thereto. ZKTeco does not extend the warranty of any kind, including, without limitation, any warranty of design, merchantability or fitness for a particular purpose.

ZKTeco does not assume responsibility for any errors or omissions in the information or documents which are referenced by or linked to this manual. The entire risk as to the results and performance obtained from using the information is assumed by the user.

ZKTeco in no event shall be liable to the user or any third party for any incidental, consequential, indirect, special, or exemplary damages, including, without limitation, loss of business, loss of profits, business interruption, loss of business information or any pecuniary loss, arising out of, in connection with, or relating to the use of the information contained in or referenced by this manual, even if ZKTeco has been advised of the possibility of such damages.

This manual and the information contained therein may include technical, other inaccuracies or typographical errors. ZKTeco periodically changes the information herein which will be incorporated into new additions/amendments to the manual. ZKTeco reserves the right to add, delete, amend or modify the information contained in the manual from time to time in the form of circulars, letters, notes, etc. for better operation and safety of the machine/unit/equipment. The said additions or amendments are meant for improvement /better operations of the machine/unit/equipment and such amendments shall not give any right to claim any compensation or damages under any circumstances.

ZKTeco shall in no way be responsible (i) in case the machine/unit/equipment malfunctions due to any non-compliance of the instructions contained in this manual (ii) in case of operation of the machine/unit/equipment beyond the rate limits (iii) in case of operation of the machine and equipment in conditions different from the prescribed conditions of the manual.

The product will be updated from time to time without prior notice. The latest operation procedures and relevant documents are available on http://www.zkteco.com

If there is any issue related to the product, please contact us.

ZKTeco Headquarters

Address	ZKTeco Industrial Park, No. 32, Industrial Road, Tangxia Town, Dongguan, China.
Phone	+86 769 - 82109991
Fax	+86 755 - 89602394

For business related queries, please write to us at: sales@zkteco.com.

To know more about our global branches, visit www.zkteco.com.

About the Company

ZKTeco is one of the world's largest manufacturer of RFID and Biometric (Fingerprint, Facial, Finger-vein) readers. Product offerings include Access Control readers and panels, Near & Far-range Facial Recognition Cameras, Elevator/floor access controllers, Turnstiles, License Plate Recognition (LPR) gate controllers and Consumer products including battery-operated fingerprint and face-reader Door Locks. Our security solutions are multi-lingual and localized in over 18 different languages. At the ZKTeco state-of-the-art 700,000 square foot ISO9001-certified manufacturing facility, we control manufacturing, product design, component assembly, and logistics/shipping, all under one roof.

The founders of ZKTeco have been determined for independent research and development of biometric verification procedures and the productization of biometric verification SDK, which was initially widely applied in PC security and identity authentication fields. With the continuous enhancement of the development and plenty of market applications, the team has gradually constructed an identity authentication ecosystem and smart security ecosystem, which are based on biometric verification techniques. With years of experience in the industrialization of biometric verifications, ZKTeco was officially established in 2007 and now has been one of the globally leading enterprises in the biometric verification industry owning various patents and being selected as the National High-tech Enterprise for 6 consecutive years. Its products are protected by intellectual property rights.

About the Manual

This manual introduces the operations of **F35**.

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.

Document Conventions

Conventions used in this manual are listed below:

GUI Conventions

For Software	
Convention	**Description**
Bold font	Used to identify software interface names e.g. **OK**, **Confirm**, **Cancel**.
>	Multi-level menus are separated by these brackets. For example, File > Create > Folder.
For Device	
Convention	**Description**
< >	Button or key names for devices. For example, press <OK>.
[ ]	Window names, menu items, data table, and field names are inside square brackets. For example, pop up the [New User] window.
/	Multi-level menus are separated by forwarding slashes. For example, [File/Create/Folder].

Symbols

Convention	**Description**
📝	This represents a note that needs to pay more attention to.
💡	The general information which helps in performing the operations faster.
⭐	The information which is significant.
✋	Care taken to avoid danger or mistakes.
⚠	The statement or event that warns of something or that serves as a cautionary example.

Table of Contents

1 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 the system is exposed to water or inclement weather conditions (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 over-heat or fire hazard.
7. **Replacement parts** - When replacement parts are required, 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.

2 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.

3 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.

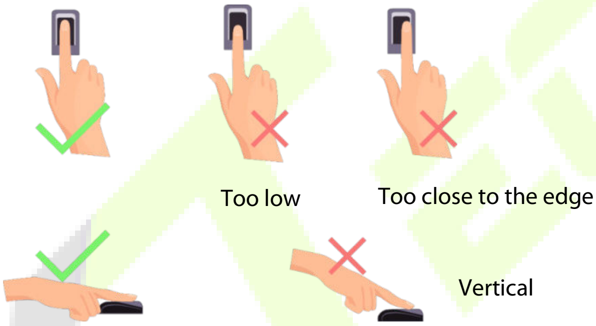
- The warranty service does not cover accidental damage, damage caused by mis-operation, and damage due to independent installation or repair of the product by the user.

4 Instruction for Use

Before getting into the device features and functions, it is recommended to be familiar with the below fundamentals.

4.1 Finger Positioning

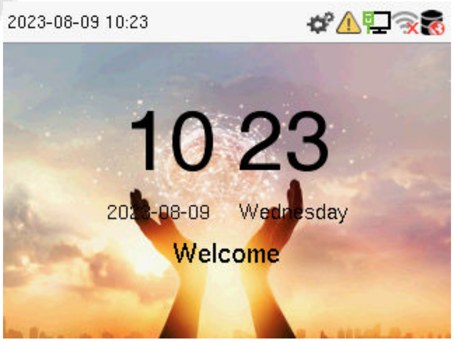
Recommended fingers: The index, middle, or ring finger and avoid using the thumb or pinky fingers, as they are difficult to accurately press onto the fingerprint reader.

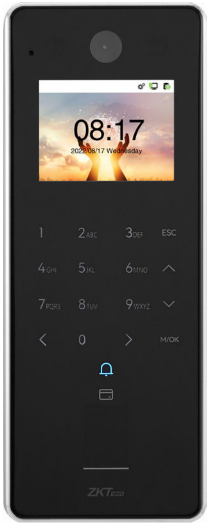


Note: Please use the correct method when pressing your fingers onto the fingerprint reader for registration and identification. Our company will assume no liability for recognition issues that may result from incorrect usage of the product. We reserve the right of final interpretation and modification concerning this point.

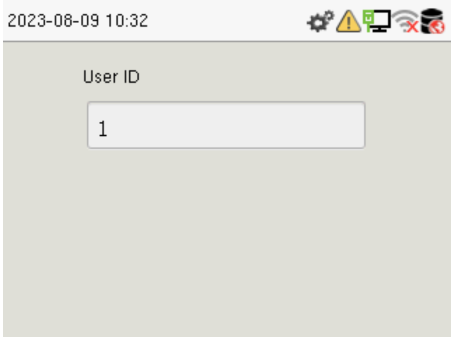
4.2 Standby Interface

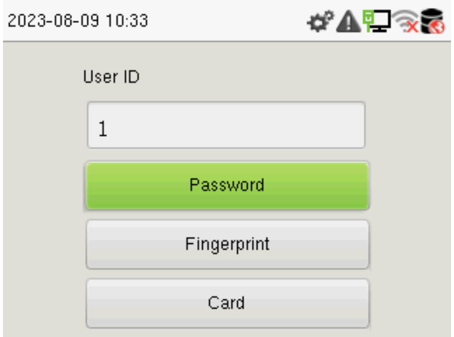
The device uses a 2.4-inch color screen, which all operations are performed through hidden touch keypad. After connecting the power supply, the following standby interface is displayed:



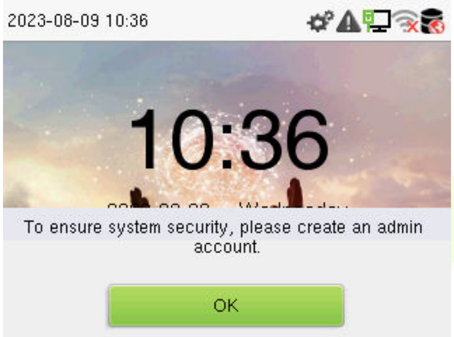


- Enter any number to access the User ID input interface.

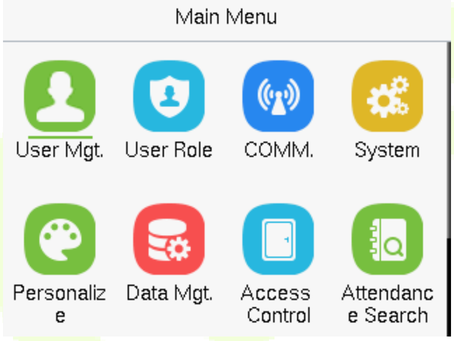




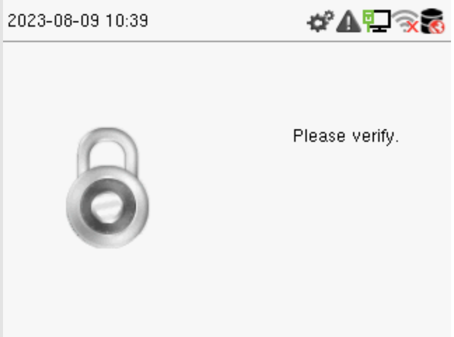
- When there is no Super Administrator set in the device, tap **M/OK** to go to the menu.



To ensure system security, please create an admin account.



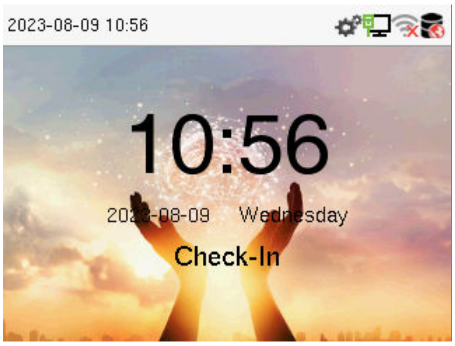
- After adding a Super Administrator on the device, it requires the Super Administrator's verification before opening the menu functions.



Please verify.

<u>Note:</u> For the security of the device, it is recommended to register a super administrator the first time you use the device.

- On the standby interface, the punch state options can also be shown and used directly. The black bold shortcut key mappings will be displayed on the screen if you tap the relevant shortcut key on the hidden touch keypad, as shown in the picture below. For the specific operation method, please see "Shortcut Key Mappings."

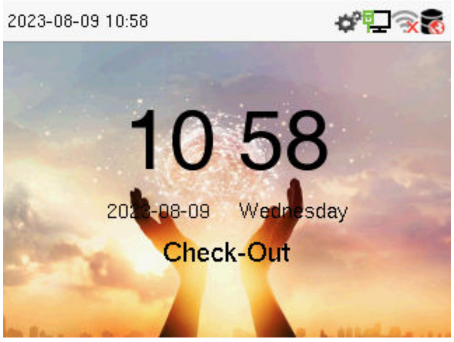


2023-08-09 10:56

10:56

2023-08-09 Wednesday

Check-In



2023-08-09 10:58

10 58

2023-08-09 Wednesday

Check-Out

Note: The punch state options are enabled by default when the device type is set as an attendance terminal.

4.3 Verification Mode

4.3.1 Fingerprint Verification

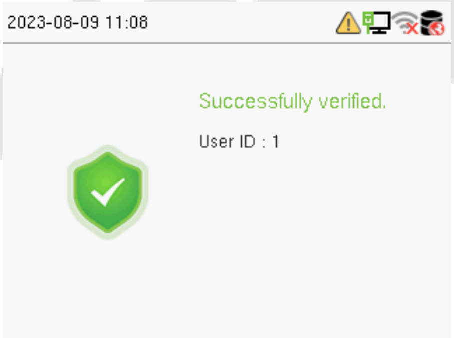
➢ **1: N Fingerprint Verification Mode**

The device compares the current fingerprint with the available fingerprint data stored in its database.

Fingerprint authentication mode is activated when a user places their finger onto the fingerprint scanner.

Please follow the recommended way to place your finger onto the sensor. For details, refer to section Finger Positioning.

Verification is successful:

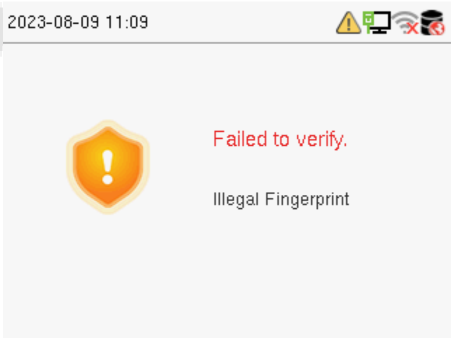


2023-08-09 11:08

Successfully verified.

User ID : 1

Verification is failed:



2023-08-09 11:09

Failed to verify.

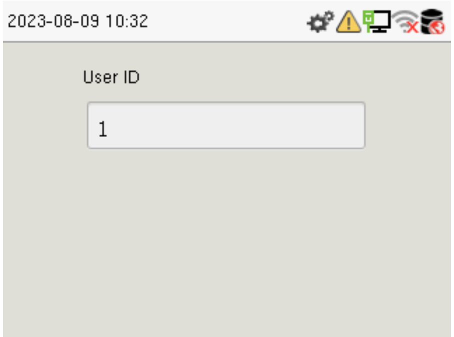
Illegal Fingerprint

➢ **1:1 Fingerprint Verification Mode**

The device compares the current fingerprint with the fingerprints linked to the entered User ID through the virtual keyboard.

In case users are unable to gain access using the 1:N authentication method, they can attempt to verify their identity using the 1:1 verification mode.

Enter the user ID and tap **M/OK** to enter the 1:1 fingerprint verification mode.

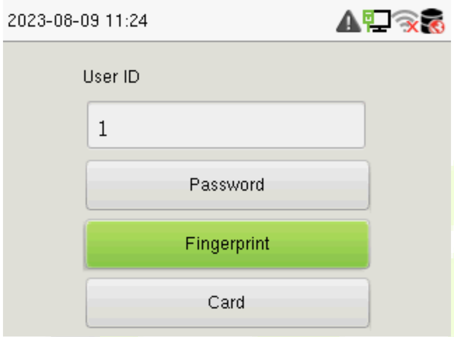


2023-08-09 10:32

User ID

1

If an employee registers a password and card in addition to the fingerprint, the following screen will appear. Select the fingerprint to enter fingerprint verification mode.



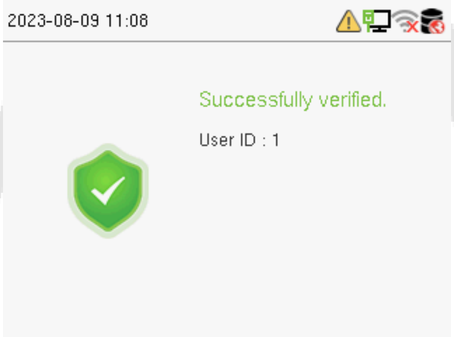
2023-08-09 11:24

User ID

1

Press the fingerprint to verify.

Verification is successful:

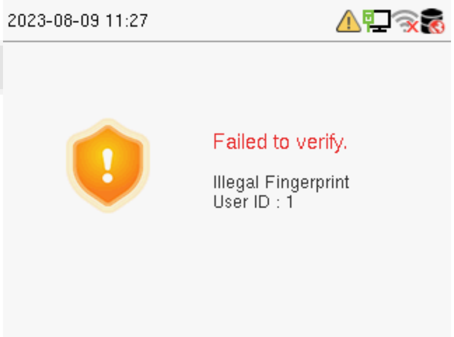


2023-08-09 11:08

Successfully verified.

User ID : 1

Verification is failed:



2023-08-09 11:27

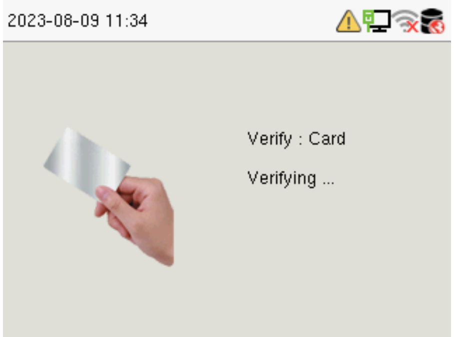
Failed to verify.

Illegal Fingerprint
User ID : 1

4.3.2 Card Verification

- **1: N Card Verification Mode**

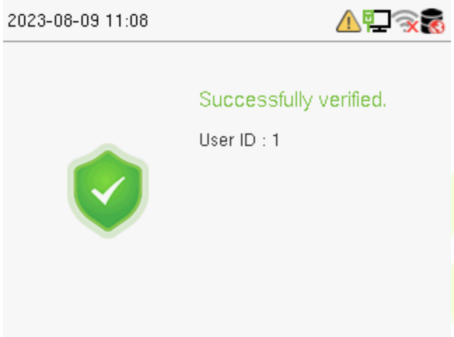
The 1: N Card Verification Mode compares the card number in the card induction area with all the card number data registered in the device. The following screen displays on the card verification screen.



2023-08-09 11:34

Verify : Card

Verifying ...



2023-08-09 11:08

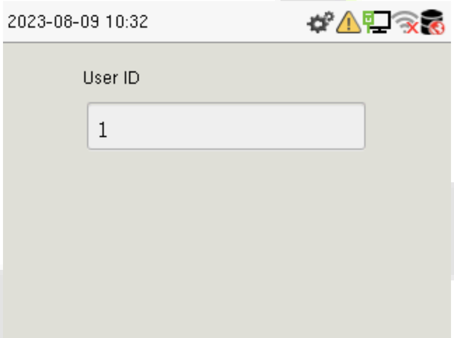
Successfully verified.

User ID : 1

- **1:1 Card Verification Mode**

The 1:1 Card Verification mode compares the card number in the card induction area with the number associated with the employee's User ID registered in the device.

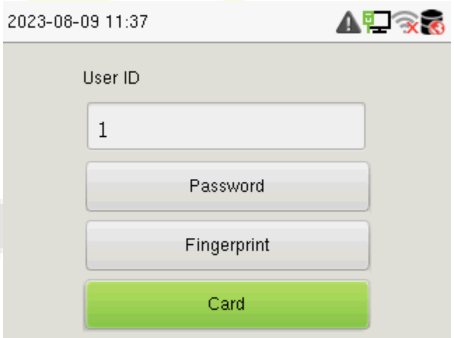
Enter the user ID and tap **M/OK** to enter the 1:1 card verification mode.



2023-08-09 10:32

User ID

1

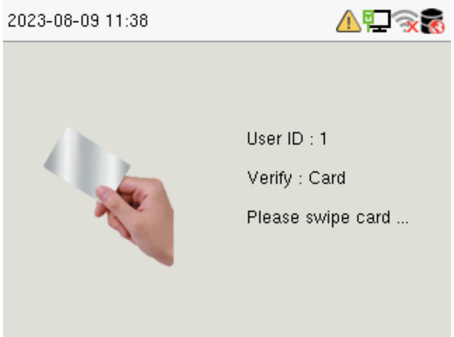


2023-08-09 11:37

User ID

1

If an employee registers a fingerprint and password in addition to the card, the following screen will appear. Select the card to enter card verification mode.

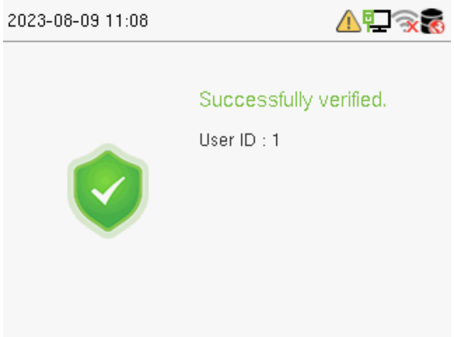


2023-08-09 11:38

User ID : 1

Verify : Card

Please swipe card ...



2023-08-09 11:08

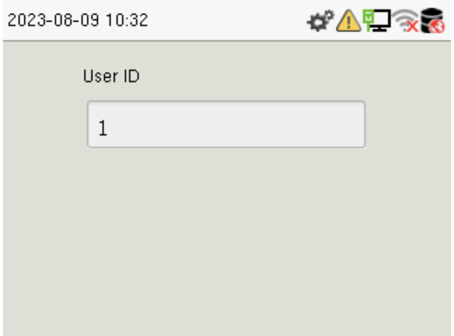
Successfully verified.

User ID : 1

4.3.3 Password Verification

The device compares the entered password with the registered password and User ID.

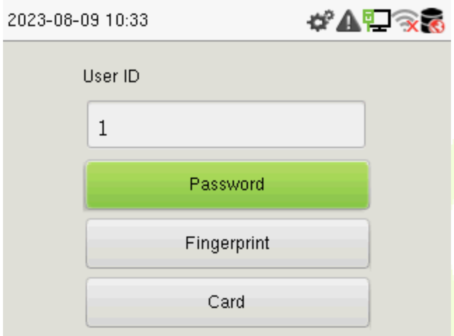
Enter the user ID and tap **M/OK** to enter the 1:1 password verification mode. Then, input the user ID and tap **M/OK**.



2023-08-09 10:32

User ID

1

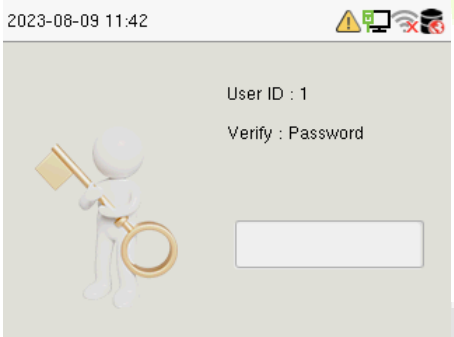


2023-08-09 10:33

User ID

1

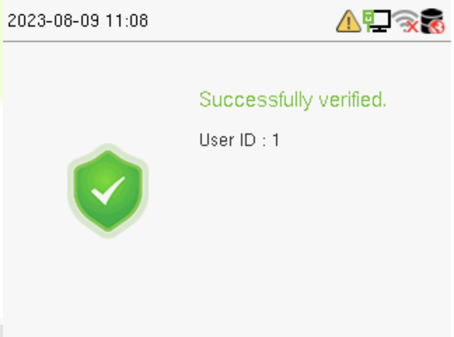
If an employee registers a fingerprint and card in addition to the password, the following screen will appear. Select the password to enter card verification mode.



2023-08-09 11:42

User ID : 1

Verify : Password



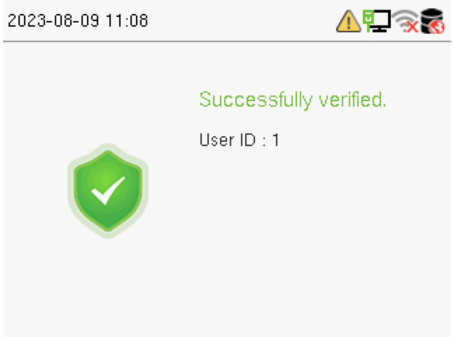
2023-08-09 11:08

Successfully verified.

User ID : 1

Below are the display screens after entering a correct password and a wrong password, respectively.

Verification is successful:

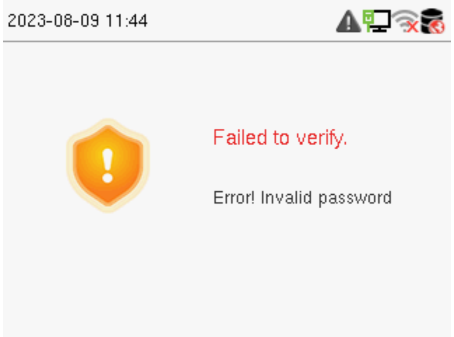


2023-08-09 11:08

Successfully verified.

User ID : 1

Verification is failed:



2023-08-09 11:44

Failed to verify.

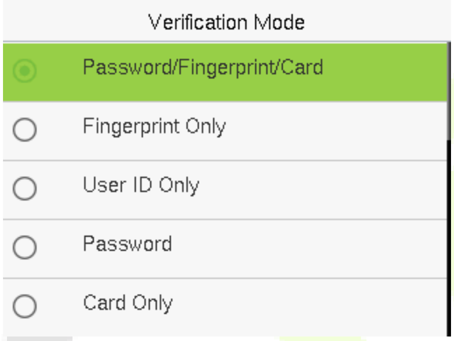
Error! Invalid password

4.3.4 Combined Verification

This device allows you to use different types of verification methods to increase security. There are a total of 15 different verification combinations that can be implemented, as listed below:

Combined Verification Symbol Definition

Symbol	Definition	Explanation
/	or	This method compares the entered verification of a person with the related verification template previously stored to that Personnel ID in the Device.
+	and	This method compares the entered verification of a person with all the verification templates previously stored to that Personnel ID in the Device.



Verification Mode

- ● Password/Fingerprint/Card
- ○ Fingerprint Only
- ○ User ID Only
- ○ Password
- ○ Card Only

Combined Verification Mode set up procedure:

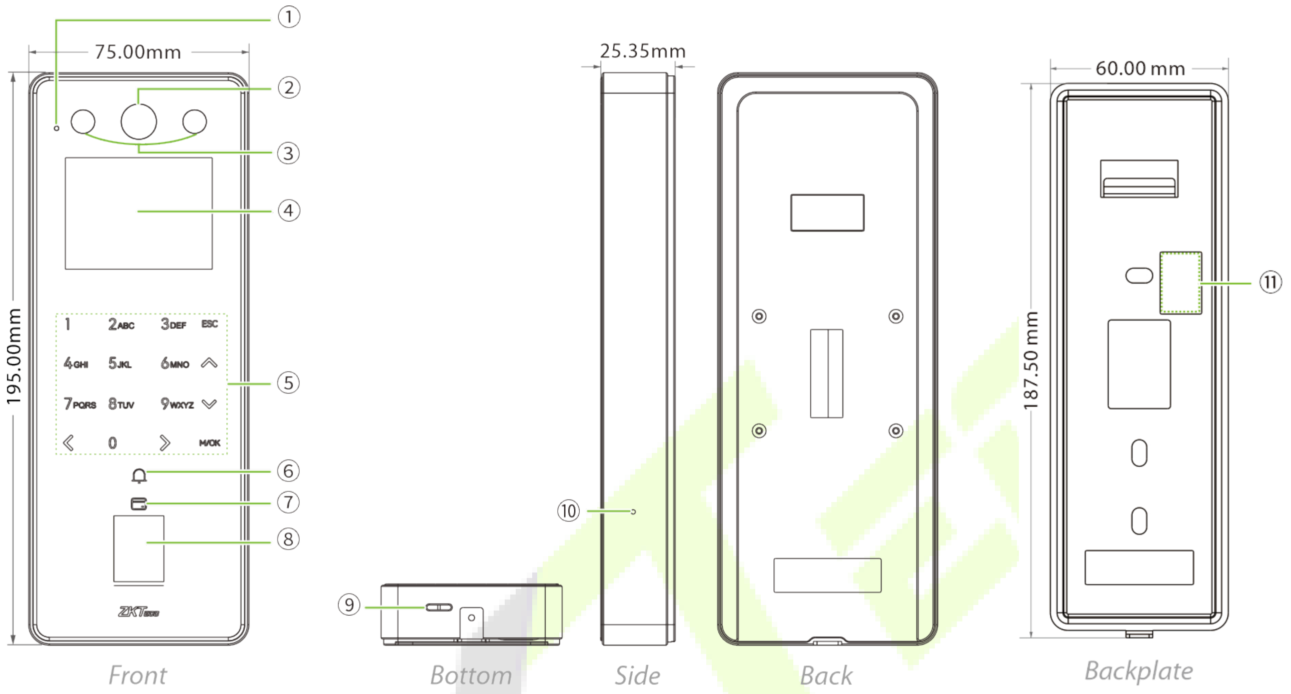
- Combined verification requires personnel to register all the different verification methods. Otherwise, employees will not be able to successfully verify the combined verification process.
- For example, if an employee has only registered for password data but the Device verification mode is set to "Password + Card," the employee will not be able to successfully complete the verification procedure.

Reason:

- This is because the Device compares the password template of the person with the registered verification template (both the Card and the Password) previously stored to that Personnel ID in the Device.
- But, since the employee has only registered their password and not their card, the verification process will not be successful, and the device will display the "Verification Failed."

5 Overview

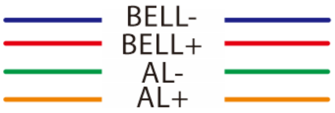
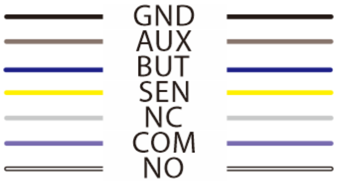
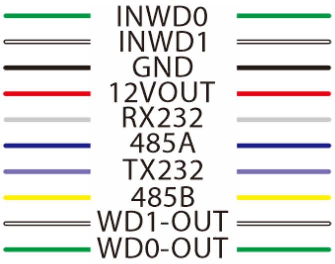
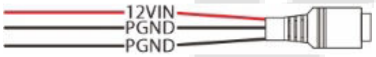
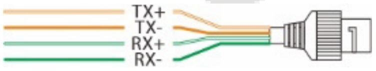
5.1 Appearance



No.	Description
1	Microphone
2	Camera
3	Near-infrared Flash
4	2.4-inch Color Screen
5	Hidden Touch Keypad
6	Doorbell Button
7	Card Reading Area
8	Fingerprint Sensor
9	Speaker
10	Restart Button
11	Magnetic Tamper Switch

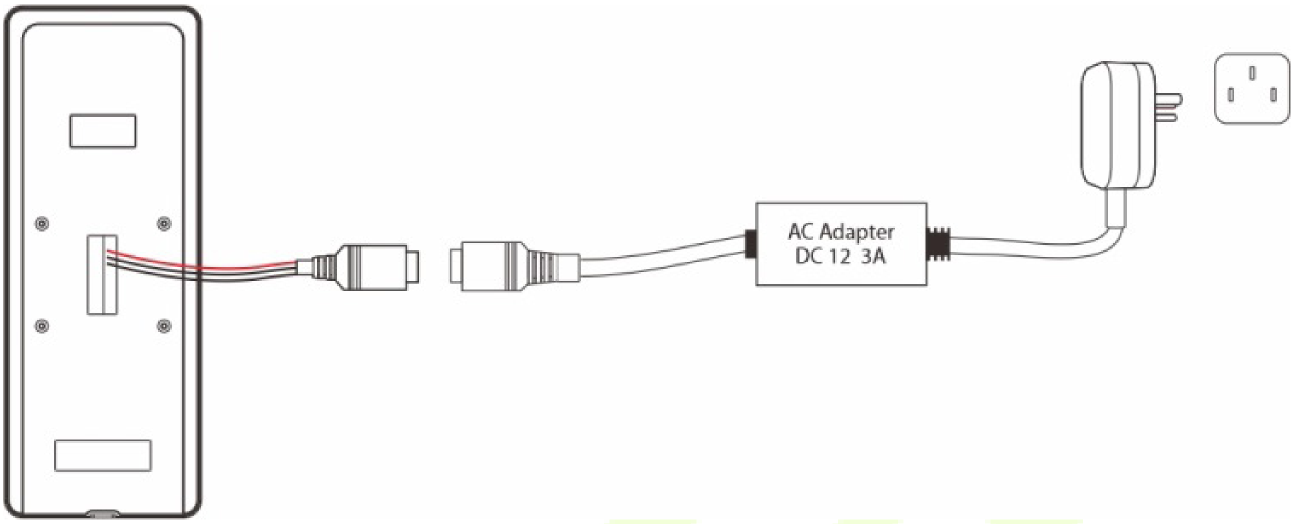
5.2 Terminal and Wiring Description

5.2.1 Terminal Description

Interface	Description	
	BELL-	Bell
	BELL+	
	AL-	Alarm
	AL+	
	GND	Sensor / Exit Button / Auxiliary Input
	AUX	
	BUT	
	SEN	
	NC	Lock
	COM	
	NO	
 INWD0 INWD1 GND 12VOUT RX232 485A TX232 485B WD1-OUT WD0-OUT	INWD0	Wiegand In
	INWD1	
	GND	
	12VOUT	
	RX232	RS232 / RS485
	485A	
	TX232	
	485B	
	WD1-OUT	Wiegand Out
	WD0-OUT	
	12V Power in	
	Network Interface	

5.3 Wiring Description

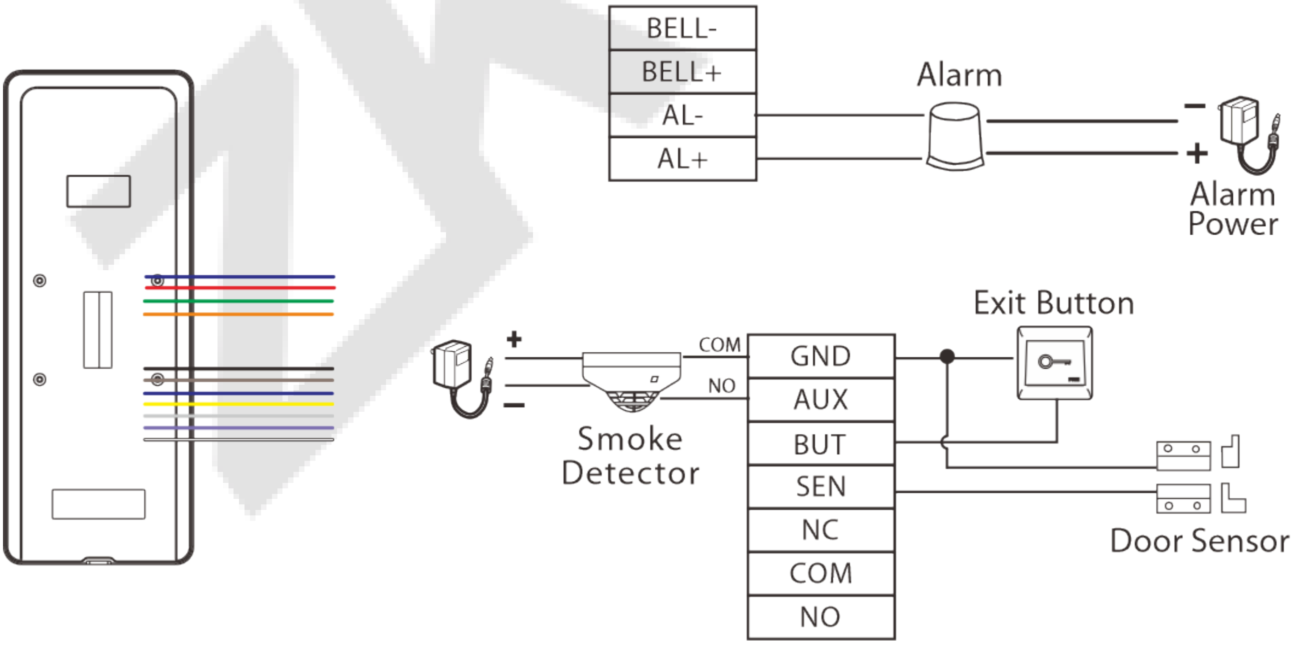
5.3.1 Power Connection



Recommended power supply

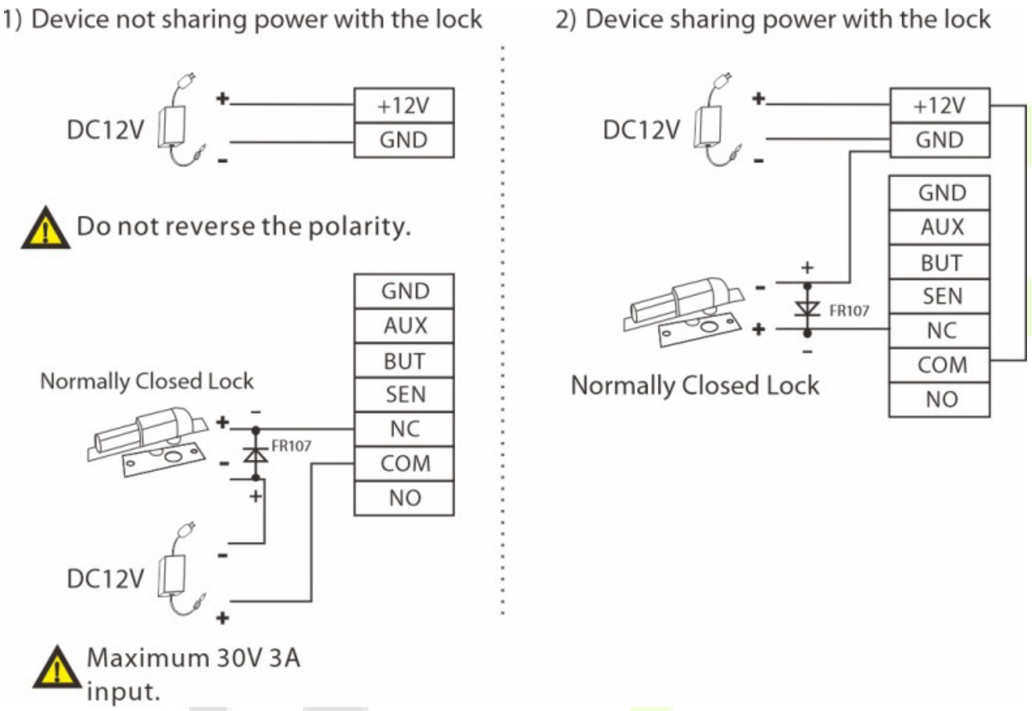
- Rating of 12V and 3A.
- To share the device's power with other devices, use a power supply with higher current ratings.

5.3.2 Door Sensor, Exit Button, Alarm and Auxiliary Connection

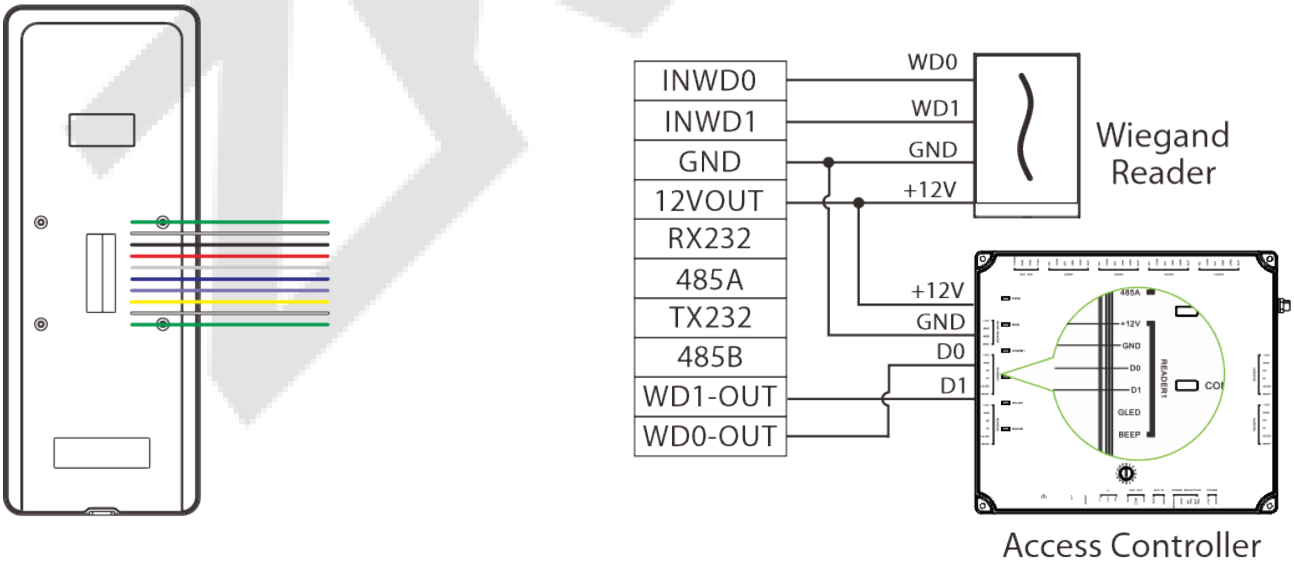


5.3.3 Lock Relay Connection

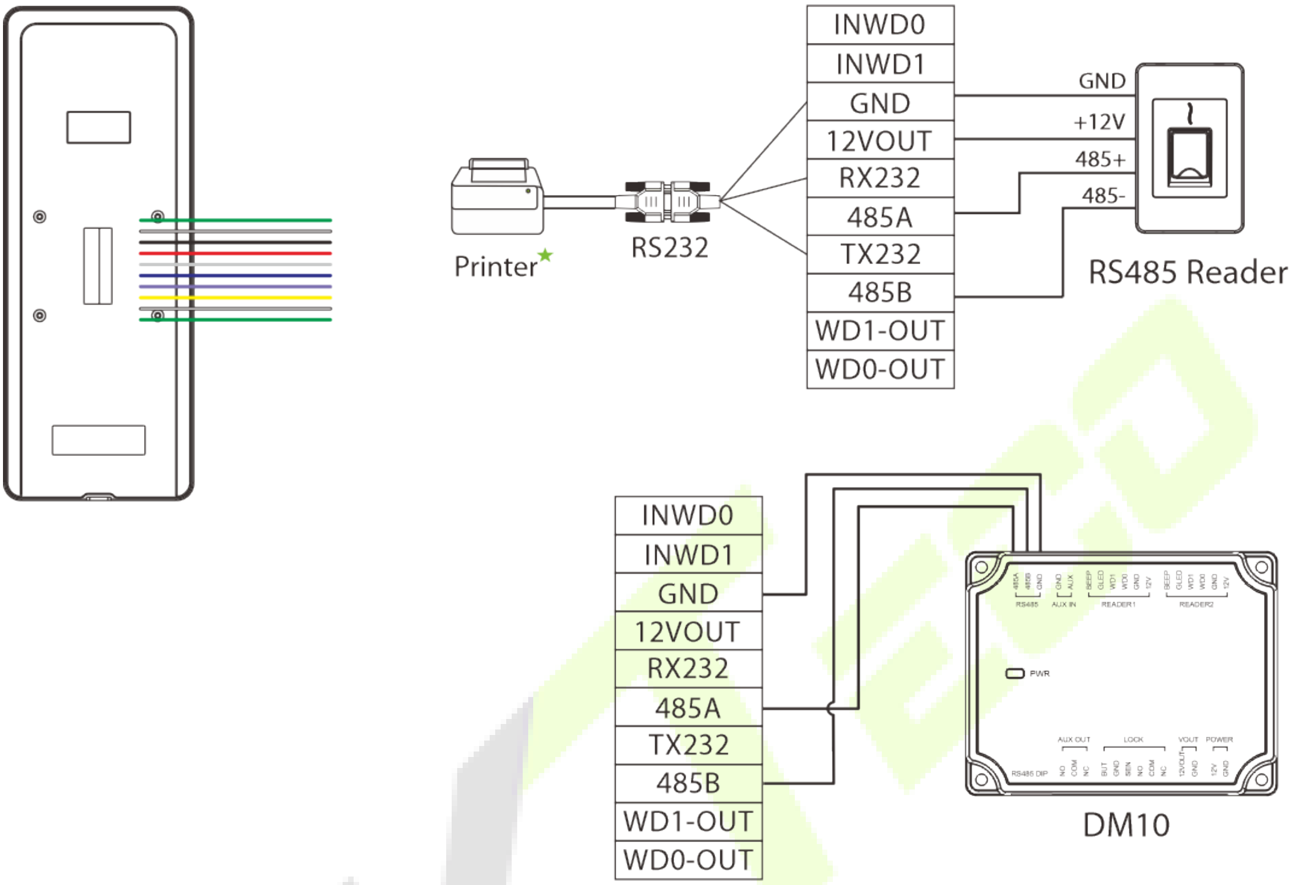
The system supports both Normally Opened Lock and Normally Closed Lock. The NO Lock (normally opened when powered) is connected with ‘NO1’ and ‘COM1’ terminals, and the NC Lock (normally closed when powered) is connected with ‘NC1’ and ‘COM1’ terminals. The power can be shared with the lock or can be used separately for the lock, as shown in the example with NC Lock below:



5.3.4 Wiegand Connection

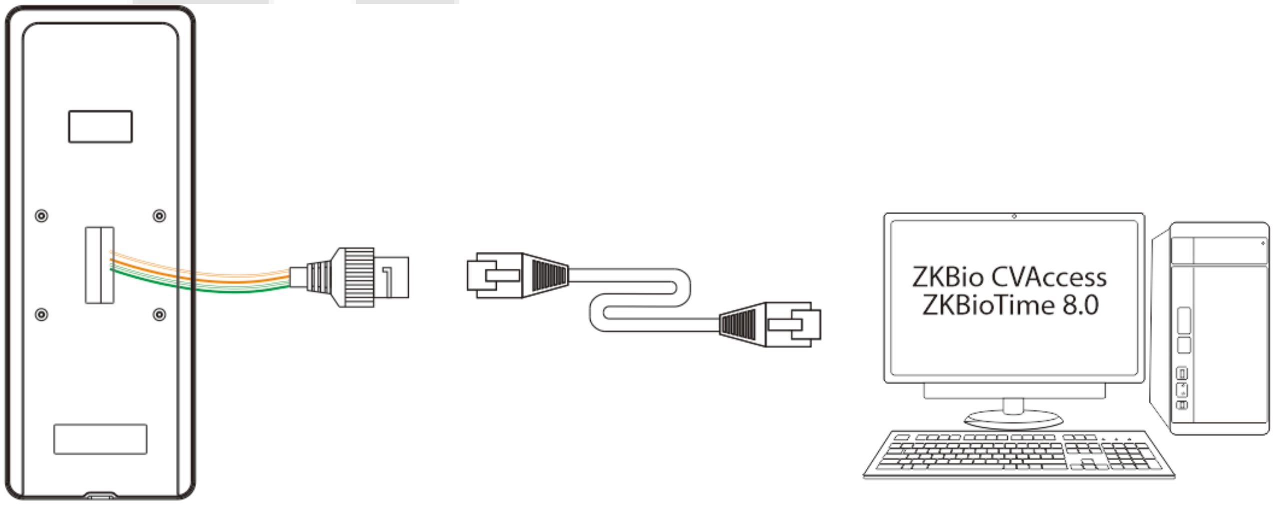


5.3.5 RS485, RS232 and DM10★ Connection



5.3.6 Ethernet Connection

Connect the device to the computer software using an Ethernet cable. An example is shown below:



Default IP address: 192.168.1.201
Subnet mask: 255.255.255.0

IP address: 192.168.1.130
Subnet mask: 255.255.255.0

Note: In a LAN, the IP addresses of the server (PC) and the device must be in the same network segment when connecting to the software.

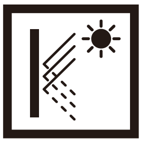
6 Installation

6.1 Installation Environment

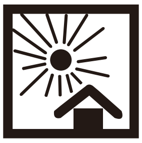
Please refer to the following recommendations for installation.

6.5ft
10ft
window

KEEP DISTANCE



AVOID GLASS REFRACTION

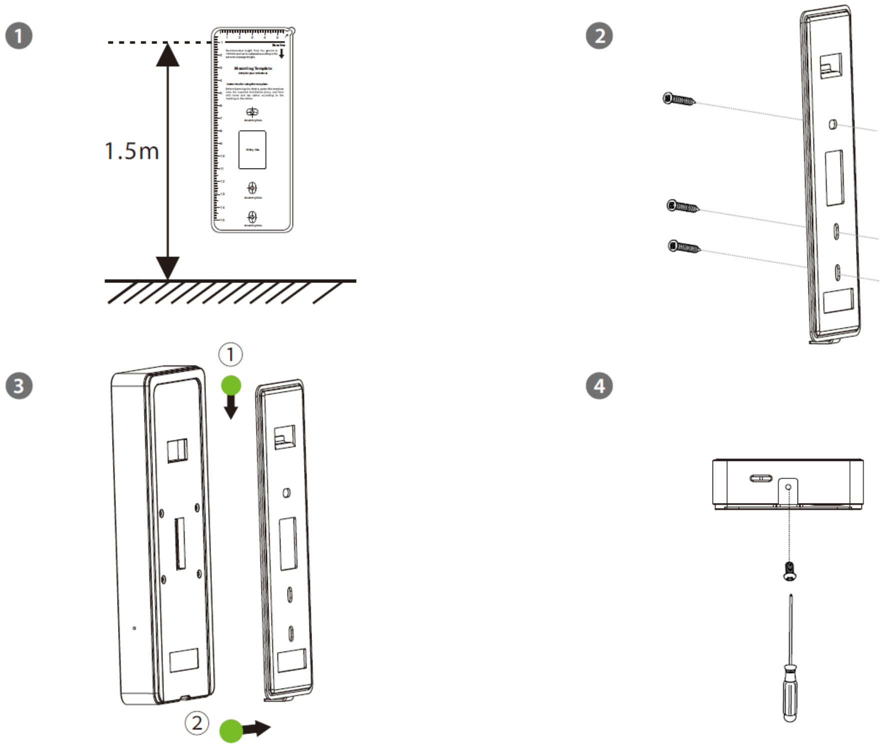


AVOID DIRECT SUNLIGHT AND EXPOSURE

AVOID USE OF ANY HEAT SOURCE NEAR THE DEVICE

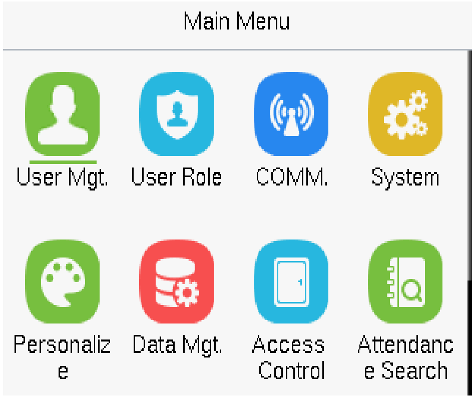
6.2 Device Installation

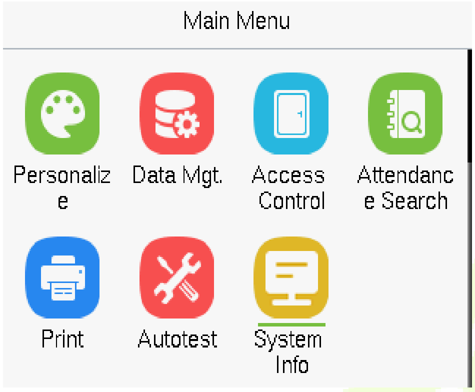
1. Stick the mounting template sticker to the wall and drill holes according to the mounting template sticker.
2. Fix the backplate on the wall using wall mounting screws.
3. Attach the device to the backplate.
4. Attach the device to the backplate with a security screw.



7 Main Menu

Tap **M/OK** on the initial interface to enter the main menu, as shown below:





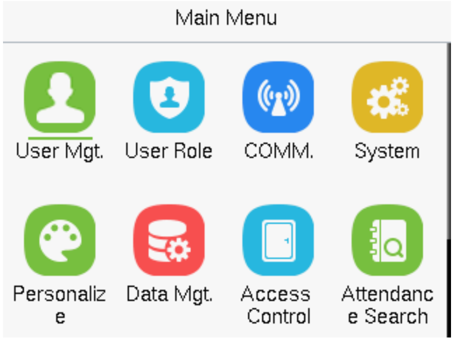
Function Description

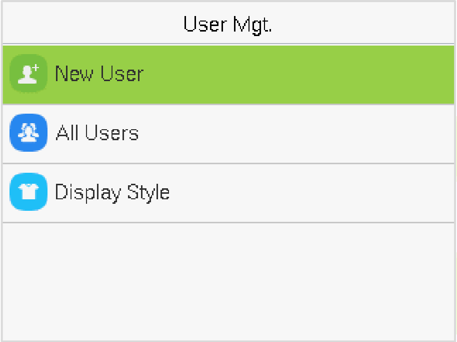
Menu	Description
User Mgt.	To Add, Edit, View, and Delete information of a User.
User Role	To set the permission scope of the custom role and enroller for the users, for example the system's operating rights.
COMM.	To set the relevant parameters of Network, Serial Comm., PC Connection, Wi-Fi★, Cloud Server, Wiegand and Network Diagnosis.
System	To set parameters related to the system, including Date Time, Attendance/Access Logs Settings, Fingerprint, Video Intercom Parameters★, ONVIF Settings★, Device Type Settings, Security Settings and resetting to factory settings.
Personalize	To customize settings of User Interface, Voice, Bell Schedules, Punch State Options and Shortcut Key Mappings settings.
Data Mgt.	To delete the data.
Access Control	To set the parameters of the lock and the relevant access control device including options like Time schedule, Holiday Settings, Combine verification, Anti-Passback Setup, and Duress Option Settings.
Attendance Search	To query the specified event logs.
Print	To set printing information and functions (if the printer is connected to the device).
Autotest	To automatically test whether each module functions properly, including the LCD Screen, Audio, Microphone, Keyboard, fingerprint sensor, camera and Real-Time Clock.
System Info	To view Privacy Policy, Data Capacity and Device and Firmware information of the current device.

8 User Management

8.1 New User Registration

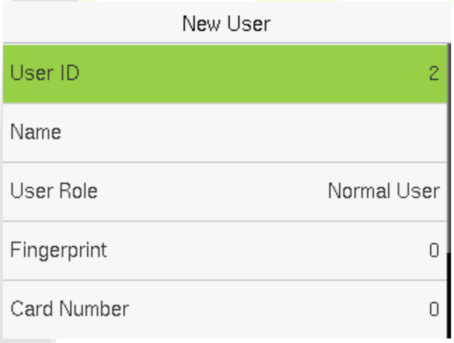
When the device is on the initial interface, press **[M/OK]** button > **User Mgt.** > **New User**.





8.1.1 Register a User ID and Name

Enter the **User ID** and **Name**.


New User

User ID 2

Name

User Role Normal User

Fingerprint 0

Card Number 0

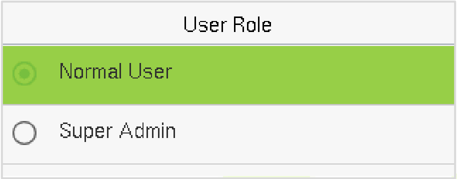
Note:

1. A name can be taken up to 36 characters long.
2. The user ID may contain 1 to 14 digits by default, supporting both numbers and alphabetic characters.
3. During the initial registration, you can modify your ID, but not after registration.
4. If the message "**Duplicated!**" appears, you must choose a different User ID because the one you entered already exists.

8.1.2 User Role

On the **New User** interface, tap on **User Role** to set the user's role as either **Normal User** or **Super Admin**.

- **Super Admin:** The Super Administrator owns all management privileges in the Device.
- **Normal User:** If the Super Admin is registered already in the device, then the Normal Users will not have the privilege to manage the system and can only access authentic verifications.
- **User Defined Roles:** The Normal User can also be assigned custom roles with User Defined Role. The user can be permitted to access several menu options as required.



User Role

● Normal User

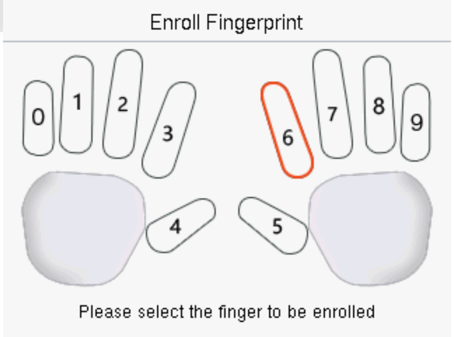
○ Super Admin

Note: If the selected user role is the Super Admin, then the user must pass the identity authentication to access the main menu. The authentication is based on the authentication method(s) that the super administrator has registered.

8.1.3 Register Fingerprint

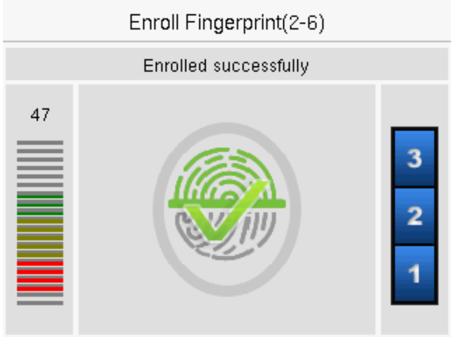
Tap **Fingerprint** in the **New User** interface to enter the fingerprint registration page.

- Select the finger to be enrolled.
- Press the same finger on the fingerprint reader three times.
- Green indicates that the fingerprint was enrolled successfully.



Enroll Fingerprint

Please select the finger to be enrolled



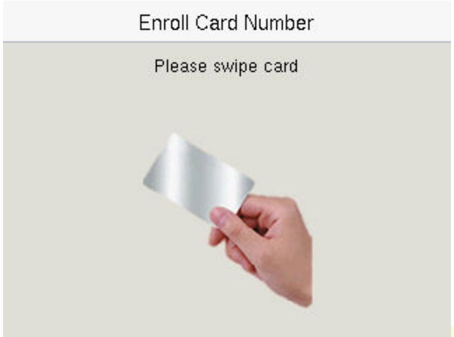
Enroll Fingerprint(2-6)

Enrolled successfully

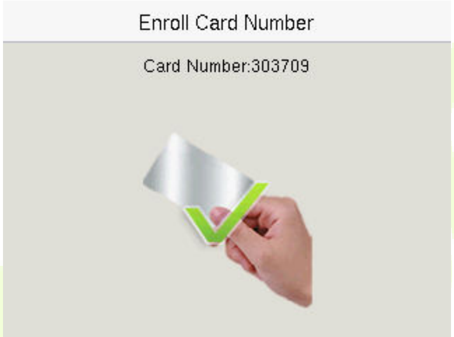
8.1.4 Card Number

Tap **Card Number** in the **New User** interface to enter the card registration page.

- On the card interface, swipe the card under the card reading area. The registration of the card will be successful.
- If the card has already been registered, the message "**Error! Card already enrolled**" appears. The registration interface appears as follows:


Enroll Card Number

Please swipe card

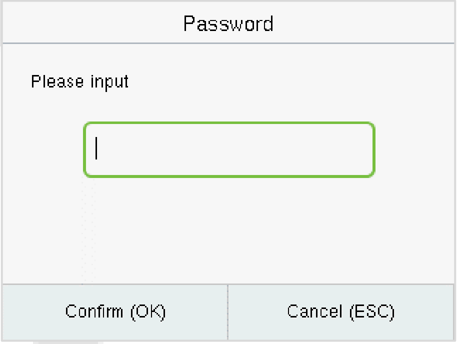

Enroll Card Number

Card Number:303709

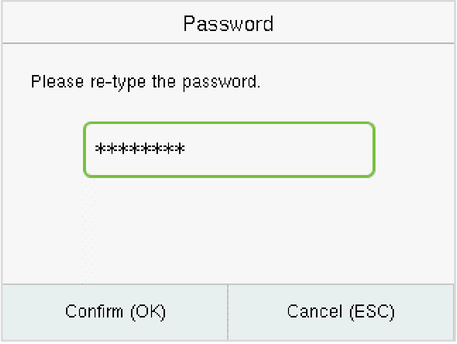
8.1.5 Password

Tap **Password** in the **New User** interface to enter the password registration page.

- On the Password interface, enter the required password and re-enter to confirm it and tap **M/OK**.
- If the re-entered password is different from the initially entered password, then the device prompts the message as "**Password not match!**", where the user needs to re-confirm the password again.
- The password may contain 6 to 8 digits by default.


Password

Please input


Password

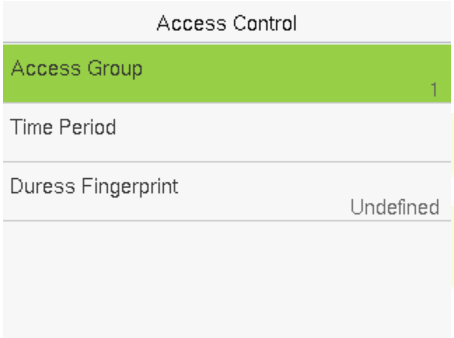
Please re-type the password.

****

8.1.6 Access Control Role

The **Access Control Role** sets the door access privilege for each user. It includes the access group, time period and duress fingerprint.

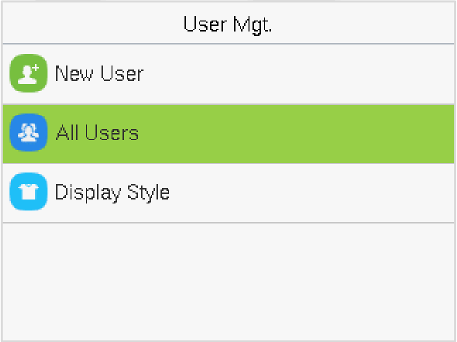
- Tap **Access Control Role** > **Access Group** to assign the registered users to different groups for better management. New users belong to Group 1 by default and can be reassigned to other groups. The device supports up to 99 Access Control groups.
- Tap **Time Period**, to select the time to use.
- The user may specify one or more fingerprints that have been registered as a duress fingerprint(s). When press the finger corresponding to the duress fingerprint on the sensor and pass the verification, the system will immediately generate a duress alarm.

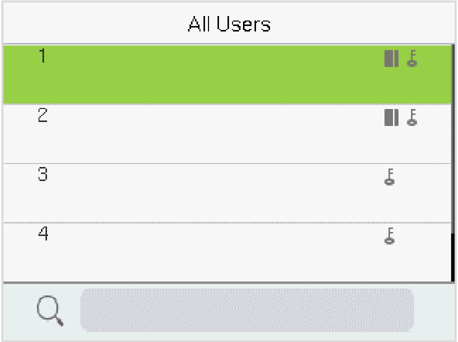


8.2 All Users

When the device is on the initial interface, press **[M/OK]** button > **User Mgt.** > **All Users**.

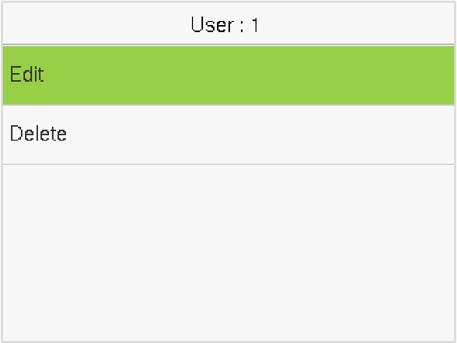
- On the **All-Users** interface, tap on the search bar on the user's list to enter the required retrieval keyword (where the keyword may be the user ID, surname, or full name) and the system will search for the related user information.

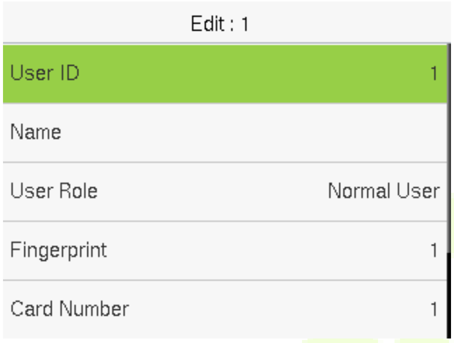




8.2.1 Edit User

On the **All-Users** interface, tap on the required user from the list and tap **Edit** to edit the user information.




Edit : 1

User ID 1

Name

User Role Normal User

Fingerprint 1

Card Number 1

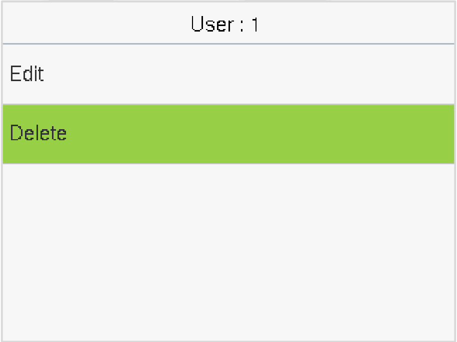
Note: The process of editing the user information is the same as adding a new user, except that the User ID cannot be modified while editing a user. The process in detail refers to "User Registration".

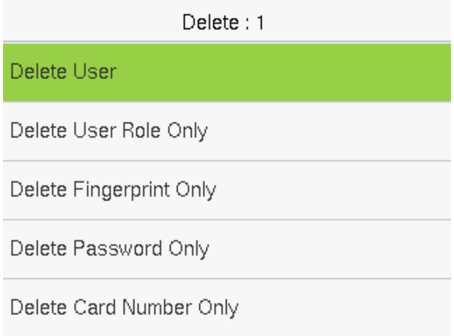
8.2.2 Delete User

On the **All Users** interface, tap on the required user from the list and tap **Delete** to delete the user or specific user information from the device. On the **Delete** interface, tap on the required operation, and then tap **M/OK** to confirm the deletion.

Delete Operations:

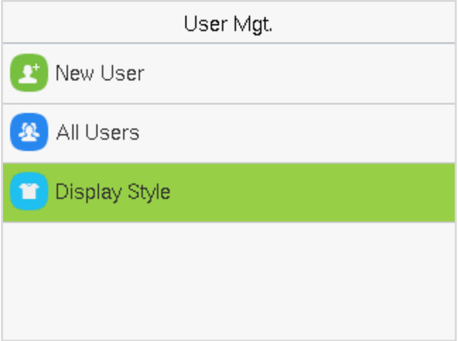
- **Delete User:** Deletes all the user information (deletes the selected User as a whole) from the Device.
- **Delete User Role Only:** Deletes the user's administrator privileges and make the user a normal user.
- **Delete Fingerprint Only:** Deletes the fingerprint information of the selected user.
- **Delete Password Only:** Deletes the password information of the selected user.
- **Delete Card Number Only:** Deletes the card information of the selected user.

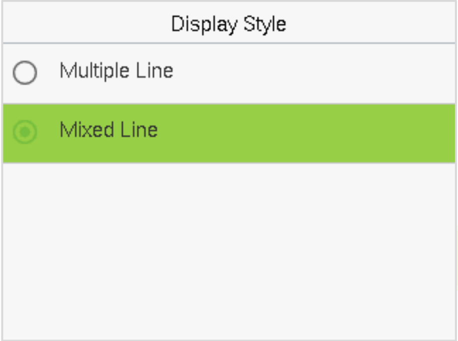




8.3 Display Style

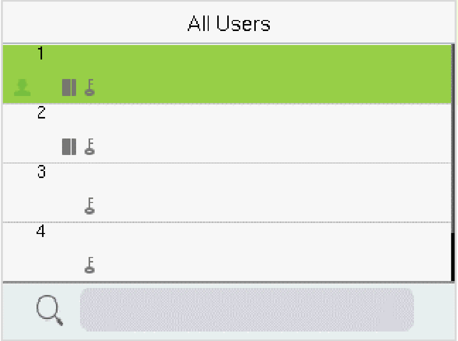
When the device is on the initial interface, press **[M/OK]** button > **User Mgt.** > **Display Style**.



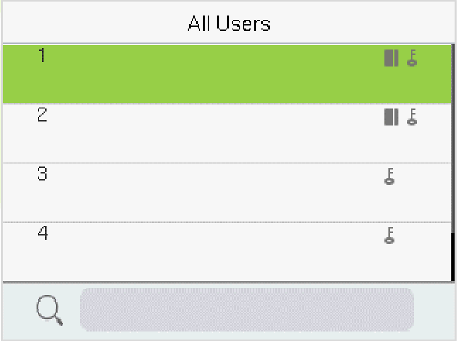


All the Display Styles are shown as below:

Multiple Line:



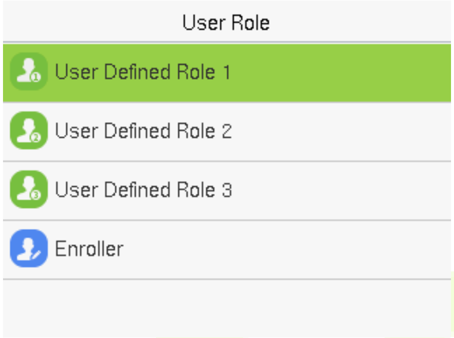
Mixed Line:



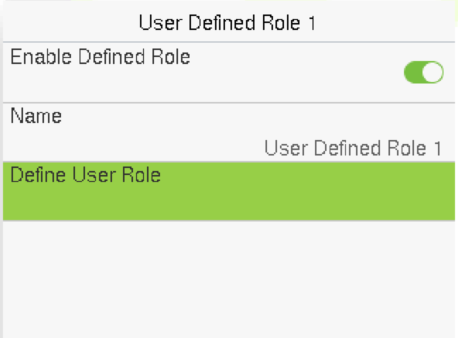
9 User Role

User Role allows you to assign specific permissions to certain users based on their requirements.

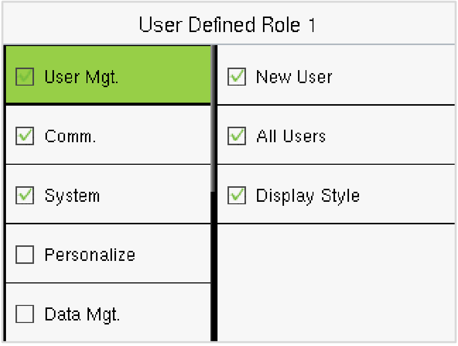
- When the device is on the initial interface, press **[M/OK]** button > **User Role** > **User Defined Role** to set the user defined permissions.
- The permission scope of the custom role can be set up into 3 roles, that is, the custom operating scope of the menu functions of the user.



- On the **User Defined Role** interface, toggle **Enable Defined Role** to enable or disable the user defined role.

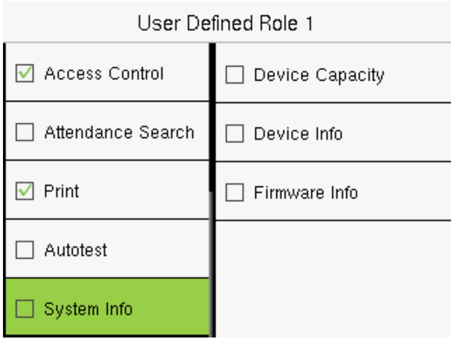


- Then, by selecting on Define User Role, select the required privileges for the new role, and then tap the **M/OK** key.
- When assigning privileges, the main menu function names will be displayed on the left and its sub-menus will be listed on the right.
- First tap on the required **Main Menu** function name, and then select its required sub-menus from the list.



User Defined Role 1

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



User Defined Role 1

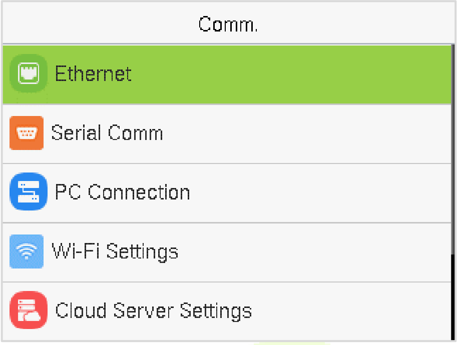
☑ Access Control	□ Device Capacity
□ Attendance Search	□ Device Info
☑ Print	□ Firmware Info
□ Autotest	
□ System Info	

Note: If the User Role is enabled for the Device, tap on **User Mgt.** > **New User** > **User Role** to assign the created roles to the required users. But if there is no super administrator registered in the Device, then the device will prompt "**Please enroll super admin first!**" when enabling the User Role function.

10 Communication

Communication Settings are used to set the parameters of the Network, Serial Comm, PC Connection, Wi-Fi, Cloud Server, Wiegand, and Network Diagnosis.

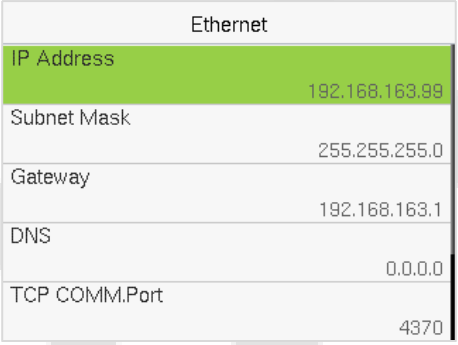
When the device is on the initial interface, press **[M/OK]** button > **COMM.**



10.1 Ethernet

When the device needs to communicate with a PC via the Ethernet, you need to configure network settings and make sure that the device and the PC connecting to the same network segment.

Tap **Ethernet** on the **COMM.** Settings interface to configure the settings.



Ethernet

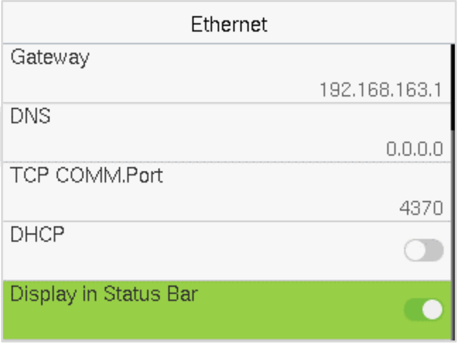
IP Address 192.168.163.99

Subnet Mask 255.255.255.0

Gateway 192.168.163.1

DNS 0.0.0.0

TCP COMM.Port 4370



Ethernet

Gateway 192.168.163.1

DNS 0.0.0.0

TCP COMM.Port 4370

DHCP ○

Display in Status Bar ●

Function Description:

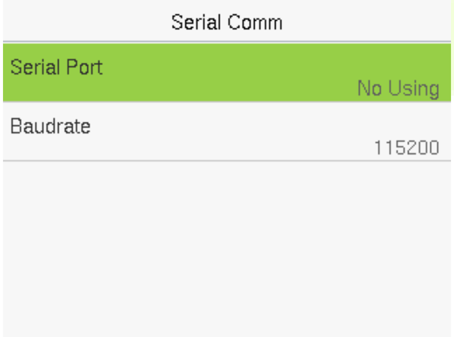
Function Name	Description
IP Address	The default IP address is 192.168.1.201. It can be modified according to the network availability.
Subnet Mask	The default Subnet Mask is 255.255.255.0. It can be modified according to the network availability.
Gateway	The Default Gateway address is 0.0.0.0. It can be modified according to the network availability.

DNS	The default DNS address is 0.0.0.0. It can be modified according to the network availability.
TCP COMM. Port	The default TCP COMM Port value is 4370. It can be modified according to the network availability.
DHCP	Dynamic Host Configuration Protocol dynamically allocates IP addresses for clients via server.
Display in Status Bar	Toggle to set whether to display the network icon on the status bar.

10.2 Serial Comm

Serial Comm function establishes communication with the device through a serial port (Master Unit/Print function).

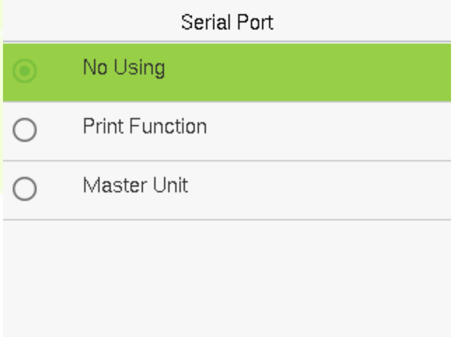
Tap **Serial Comm.** on the **COMM.** Settings interface.



Serial Comm

Serial Port: No Using

Baudrate: 115200



Serial Port

● No Using

○ Print Function

○ Master Unit

Function Description

Function Name	Description
Serial Port	**No Using:** No communication with the device through the serial port. **Master Unit:** When RS485 is used as the function of "**Master Unit**", it can be connected to a reader. **Print Function:** The device can be connected to the printer when RS232 enables the print function.
Baudrate	There are 4 baudrate options at which the data communicates with PC. They are: 115200 (default), 57600, 38400, and 19200. The higher the baudrate, the faster is the communication speed, but also less reliable. Hence, a higher baudrate can be used when the communication distance is short; when the communication distance is long, choosing a lower baudrate is more reliable.

10.3 PC Connection

Comm Key facilitates to improve the security of the data by setting up the communication between the device and the PC. Once the Comm Key is set, a password is required to connect the device to the PC software.

Tap **PC Connection** on the **COMM.** Settings interface to configure the communication settings.

Function Description

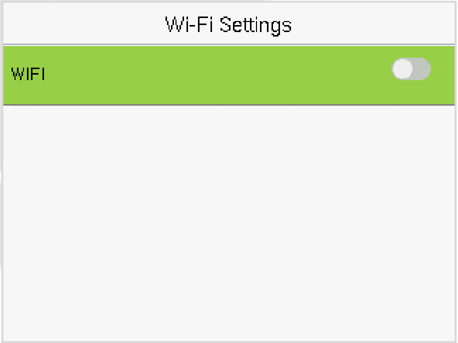
Function Name	Description
Comm Key	The default password is 0 and can be changed. The Comm Key can contain 1 to 6 digits.
Device ID	It is the identification number of the device, which ranges between 1 and 254.

10.4 Wi-Fi Settings★

The device provides a Wi-Fi module, which can be built-in within the device module or can be externally connected.

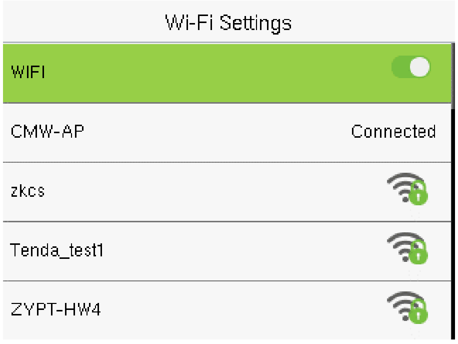
The Wi-Fi module enables data transmission via Wi-Fi (Wireless Fidelity) and establishes a wireless network environment. Wi-Fi is enabled by default in the device. If you don't need to use the Wi-Fi network, you can toggle the Wi-Fi to disable the button.

Tap **Wi-Fi Settings** on the **COMM.** Settings interface to configure the Wi-Fi settings.



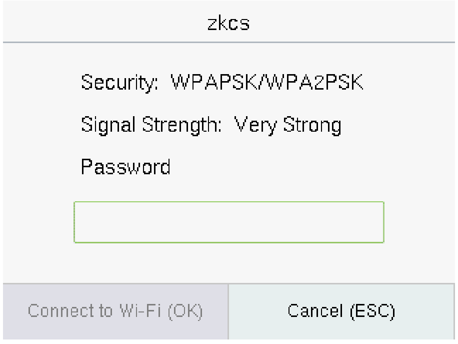
➢ Searching the Wi-Fi Network

- Wi-Fi is enabled in the device by default. Toggle the ● button to enable or disable Wi-Fi.
- Once the Wi-Fi is turned on, the device will search for the available Wi-Fi within the network range.
- Tap on the required Wi-Fi name from the available list and input the correct password in the password interface, and then tap **M/OK**.



Wi-Fi Settings

WIFI	
CMW-AP	Connected
zkcs	
Tenda_test1	
ZYPT-HW4	



zkcs

Security: WPAPSK/WPA2PSK

Signal Strength: Very Strong

Password

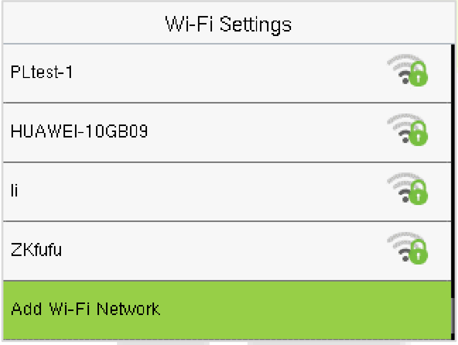
WIFI Enabled: Tap on the required network from the searched network list.

Tap on the password field to enter the password and tap **M/OK.**

- When the Wi-Fi is connected successfully, the initial interface will display the Wi-Fi logo.

Adding Wi-Fi Network Manually

The Wi-Fi can also be added manually if the required Wi-Fi does not show on the list.



Wi-Fi Settings

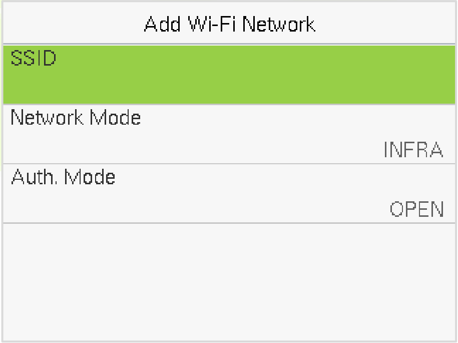
PLtest-1

HUAWEI-10GB09

li

ZKfufu

Add Wi-Fi Network



Add Wi-Fi Network

SSID	
Network Mode	INFRA
Auth. Mode	OPEN

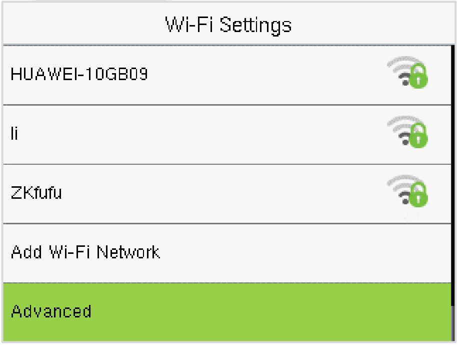
Tap on **Add Wi-Fi Network** to add the Wi-Fi manually.

On this interface, enter the Wi-Fi network parameters. (The added network must exist.)

Note: After successfully adding the Wi-Fi manually, follow the same process to search for the added Wi-Fi name.

Advanced Setting

On the **Wi-Fi Settings** interface, tap on **Advanced** to set the relevant parameters as required.



Wi-Fi Settings

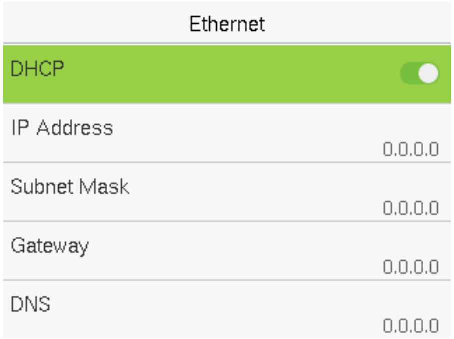
HUAWEI-10GB09

li

ZKfufu

Add Wi-Fi Network

Advanced



Ethernet

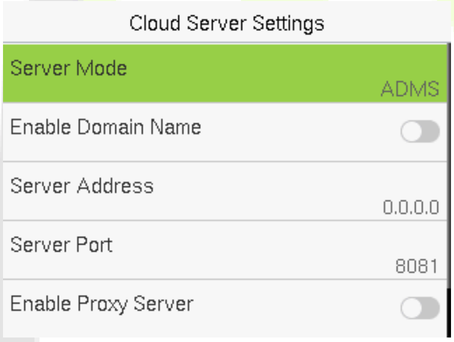
DHCP	
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Gateway	0.0.0.0
DNS	0.0.0.0

Function Description

Function Name	Description
DHCP	Dynamic Host Configuration Protocol (DHCP) dynamically allocates IP addresses to network clients. If the DHCP is enabled, then the IP cannot be set manually.
IP Address	The IP address for the Wi-Fi network, the default is 0.0.0.0. It can be modified according to the network availability.
Subnet Mask	The default Subnet Mask of the Wi-Fi network is 255.255.255.0. It can be modified according to the network availability.
Gateway	The Default Gateway address is 0.0.0.0. It can be modified according to the network availability.
DNS	The default DNS is 0.0.0.0. It can be modified according to the network availability.

10.5 Cloud Server Settings

Tap **Cloud Server Settings** on the **COMM.** Settings interface to connect with the ADMS server.



Cloud Server Settings

Server Mode: ADMS

Enable Domain Name

Server Address: 0.0.0.0

Server Port: 8081

Enable Proxy Server

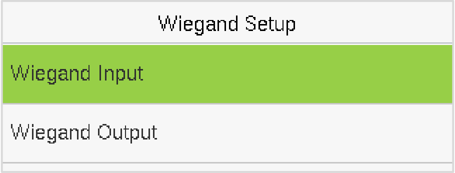
Function Description

Function Name		Description
Enable Domain Name	**Server Address**	Once this mode is turned ON, the domain name mode "http://... " will be used, such as http://www.XYZ.com, while "XYZ" denotes the domain name.
Disable Domain Name	**Server Address**	The IP address of the ADMS server.
	Server Port	Port used by the ADMS server.
Enable Proxy Server		The IP address and the port number of the proxy server is set manually when the proxy is enabled.
HTTPS		Based on HTTP, transmission encryption and identity authentication ensure the security of the transmission process.

10.6 Wiegand Setup

It is used to set the Wiegand input and output parameters.

Tap **Wiegand Setup** on the **COMM.** Settings interface to set up the Wiegand input and output parameters.

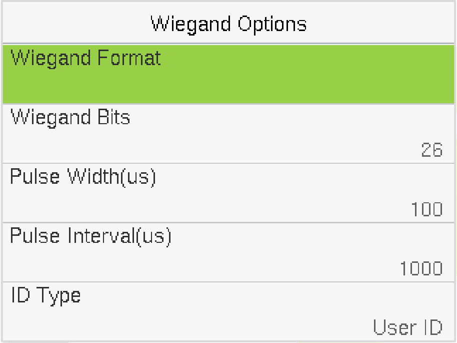


Wiegand Setup

Wiegand Input

Wiegand Output

10.6.1 Wiegand Input



Wiegand Options

Wiegand Format

Wiegand Bits: 26

Pulse Width(us): 100

Pulse Interval(us): 1000

ID Type: User ID

Function Description

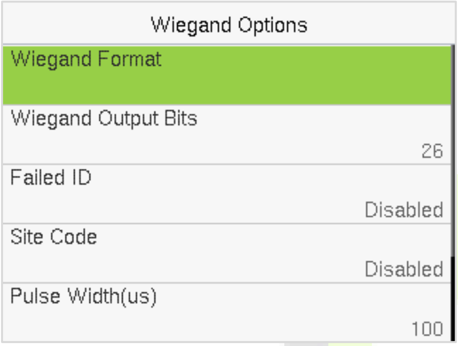
Function Name	Description
Wiegand Format	Its value can be 26 bits, 34 bits, 36 bits, 37 bits, and 50 bits.
Wiegand Bits	The number of bits of the Wiegand data.
Pulse Width(us)	The value of the pulse width sent by Wiegand is 100 microseconds by default, which can be adjusted within the range of 20 to 400 microseconds.
Pulse Interval(us)	The default value is 1000 microseconds and can be adjusted within the range of 200 to 20000 microseconds.
ID Type	Select between the User ID and card number.

Various Common Wiegand Format Description:

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	ESSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCO 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	EFFFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCO 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	OMMMMSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCE 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	EMMMFFFFFFFFFFSSSSSSCCCCCCCCCCCCCCCCO 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	ESSSSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO 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.	

10.6.2 Wiegand Output



Wiegand Options

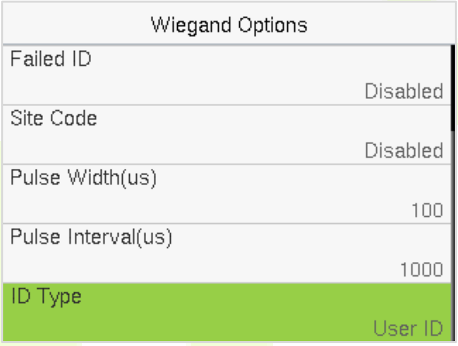
Wiegand Format

Wiegand Output Bits: 26

Failed ID: Disabled

Site Code: Disabled

Pulse Width(us): 100



Wiegand Options

Failed ID: Disabled

Site Code: Disabled

Pulse Width(us): 100

Pulse Interval(us): 1000

ID Type: User ID

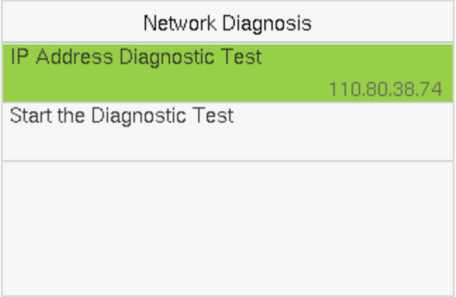
Function Description

Function Name	Description
Wiegand Format	Its value can be 26 bits, 34 bits, 36 bits, 37 bits, and 50 bits.
Wiegand Output Bits	After selecting the required Wiegand format, select the corresponding output bit digits from the Wiegand format.
Failed ID	If the verification fails, the system will send the failed ID to the device and replace the card number or personnel ID with the new one.
Site Code	It is similar to the device ID. The difference is that a site code can be set manually and is repeatable on a different device. The valid value ranges from 0 to 256 by default.
Pulse Width(us)	The time width represents the changes in the quantity of electric charge with regular high-frequency capacitance within a specified time.
Pulse Interval(us)	The time interval between pulses.
ID Type	Select the ID types as either User ID or card number.

10.7 Network Diagnosis

It helps to set the network diagnosis parameters.

Tap **Network Diagnosis** on the **COMM.** Settings interface. Enter the IP address that needs to be diagnosed and tap **Start the Diagnostic Test** to check whether the network can connect to the device.



Network Diagnosis

IP Address Diagnostic Test 110.80.38.74

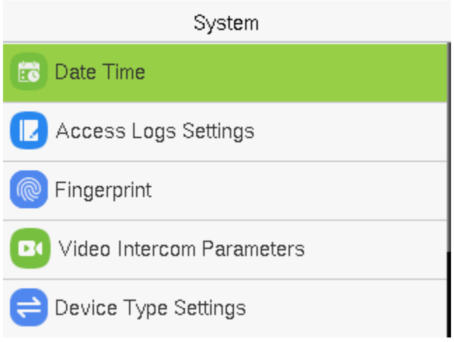
Start the Diagnostic Test

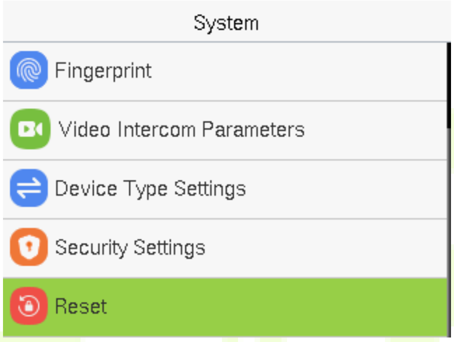
11 System Settings

It helps to set related system parameters to optimize the accessibility of the device.

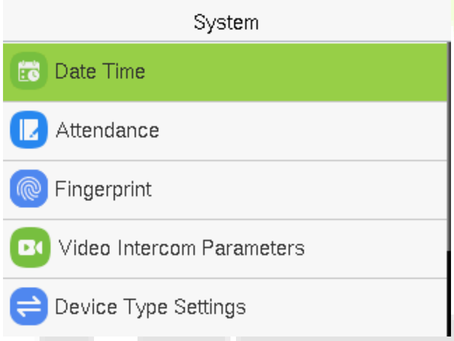
When the device is on the initial interface, press **[M/OK]** button > **System.**

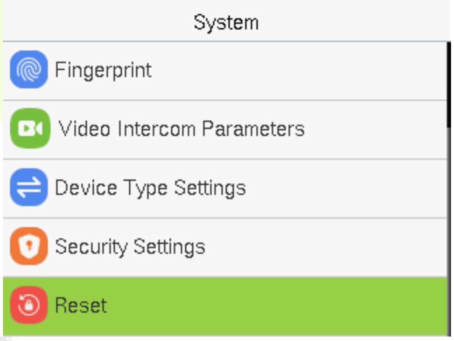
Access Control Terminal:





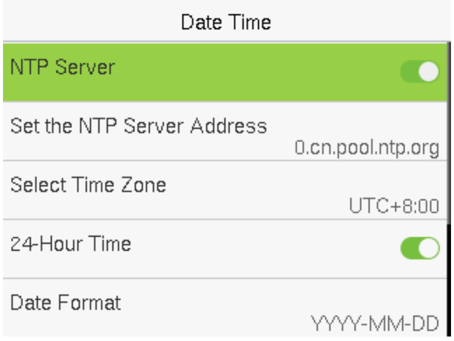
Time Attendance Terminal:





11.1 Date and Time

Tap **Date Time** on the **System** interface to set the date and time.



Date Time

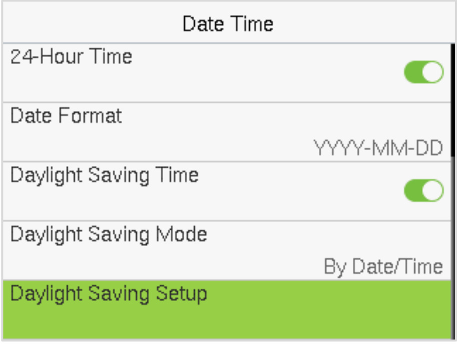
NTP Server

Set the NTP Server Address: 0.cn.pool.ntp.org

Select Time Zone: UTC+8:00

24-Hour Time

Date Format: YYYY-MM-DD



Date Time

24-Hour Time

Date Format: YYYY-MM-DD

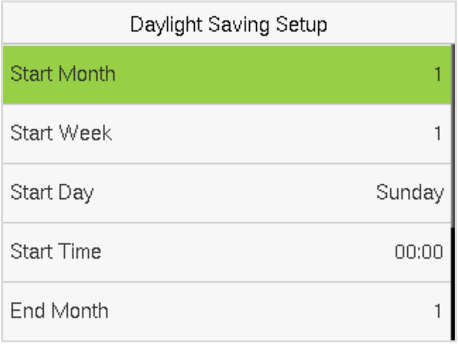
Daylight Saving Time

Daylight Saving Mode: By Date/Time

Daylight Saving Setup

- Tap **NTP Server** to enable automatic time synchronization based on the service address you enter.
- Tap **Manual Date and Time** to manually set the date and time and then tap **Confirm** and save.

- Tap **Select Time Zone** to manually select the time zone where the device is located.
- Enable or disable this format by tapping 24-Hour Time. If enabled, then select the **Date Format** to set the date.
- Tap **Daylight Saving Time** to enable or disable the function. If enabled, tap **Daylight Saving Mode** to select a daylight-saving mode and then tap **Daylight Saving Setup** to set the switch time.



Daylight Saving Setup

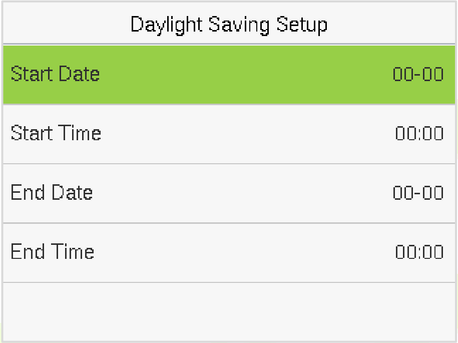
Start Month 1

Start Week 1

Start Day Sunday

Start Time 00:00

End Month 1



Daylight Saving Setup

Start Date 00-00

Start Time 00:00

End Date 00-00

End Time 00:00

Week Mode **Date Mode**

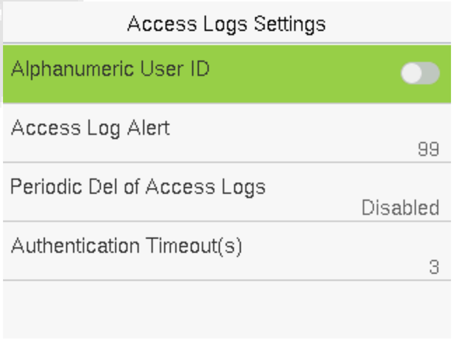
- When restoring the factory settings, the time (24-hour) and date format (YYYY-MM-DD) can be restored, but the device date and time cannot be restored.

Note: For example, if a user sets the time of the device from 18:35 on March 15, 2020 to 18:30 on January 1, 2021. After restoring the factory settings, the time of the device will remain at 18:30 on January 1, 2021.

11.2 Access Logs Settings / Attendance

Tap **Access Logs Settings / Attendance** on the **System** interface.

Access Control Terminal:



Access Logs Settings

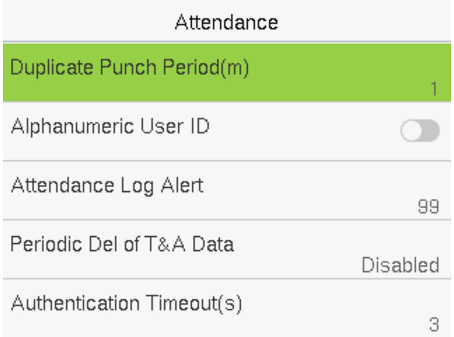
Alphanumeric User ID

Access Log Alert 99

Periodic Del of Access Logs Disabled

Authentication Timeout(s) 3

Time Attendance Terminal:



Attendance

Duplicate Punch Period(m) 1

Alphanumeric User ID

Attendance Log Alert 99

Periodic Del of T&A Data Disabled

Authentication Timeout(s) 3

Function Description of Access Control Terminal:

Function Name	Description
Alphanumeric User ID	Enable/Disable the alphanumeric as User 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.
Authentication Timeout(s)	The amount of time taken to display a successful verification message. Valid value: 1 to 9 seconds.

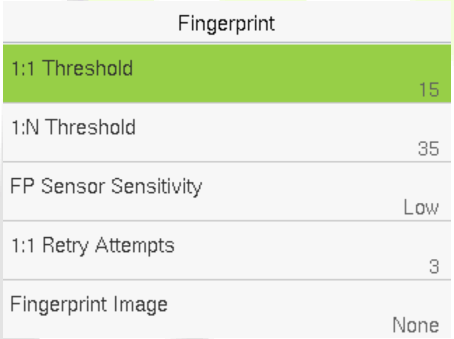
Function Description of Time Attendance Terminal:

Function Name	Description
Duplicate Punch Period(m)	Within a set time period (unit: minutes), the duplicated attendance record will not be reserved (value ranges from 1 to 999999 minutes).
Alphanumeric User ID	Enable/Disable the alphanumeric as User ID.

Attendance Log Alert	When the record space of the attendance 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 T&A Data	When attendance records reach its maximum storage capacity, the device automatically deletes a set of old attendance records. Users may disable the function or set a valid value between 1 and 999.
Authentication Timeout(s)	The amount of time taken to display a successful verification message. Valid value: 1 to 9 seconds.

11.3 Fingerprint

Tap **Fingerprint** on the **System** interface to go to the Fingerprint parameter settings.



Fingerprint

1:1 Threshold 15

1:N Threshold 35

FP Sensor Sensitivity Low

1:1 Retry Attempts 3

Fingerprint Image None

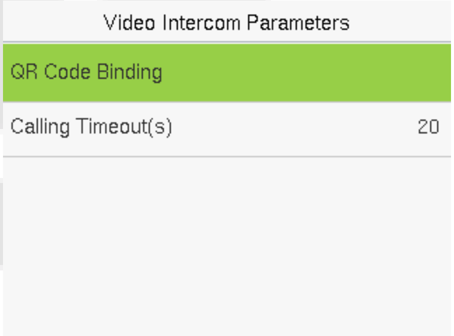
Function Description

Function Name	Description
1:1 Threshold Value	Under 1:1 verification method, the verification will only be successful when the similarity between the acquired fingerprint data and the fingerprint template associated with the entered user ID enrolled in the device is greater than the set value.
1:N Threshold Value	Under 1:N verification method, the verification will only be successful when the similarity between the acquired fingerprint data and the fingerprint templates enrolled in the device is greater than the set value.

FP Sensor Sensitivity	To set the sensibility of fingerprint acquisition. It is recommended to use the default level "**Medium**". When the environment is dry, resulting in slow fingerprint detection, you can set the level to "**High**" to raise the sensibility; when the environment is humid, making it hard to identify the fingerprint, you can set the level to "**Low**".
1:1 Retry Times	In 1:1 Verification, users might forget the registered fingerprint, or press the finger improperly. To reduce the process of re-entering user ID, retry is allowed.
Fingerprint Image	To set whether to display the fingerprint image on the screen during fingerprint enrollment or verification. Four choices are available: **Show for Enroll:** to display the fingerprint image on the screen only during enrollment. **Show for Match:** to display the fingerprint image on the screen only during verification. **Always Show:** to display the fingerprint image on screen during enrollment and verification. **None:** not to display the fingerprint image.

11.4 Video Intercom Parameters★

Tap **Video Intercom Parameters** on the **System** interface.



Video Intercom Parameters

QR Code Binding

Calling Timeout(s) 20

Function Description

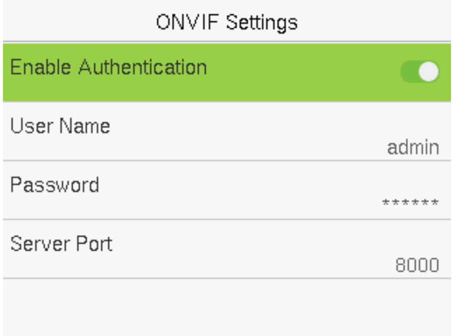
Function Name	Description
QR Code Binding	Use the ZSmart App client to scan the QR code to connect and bind the device.
Calling Timeout (s)	If the call is not answered within a specified time, it exits to the main interface.

For more details, please refer to 22. Connecting to ZSmart App.

11.5 ONVIF Settings★

Note: This function needs to be used with the network video recorder (NVR).

1. Set the device to the same network segment as the NVR.
2. Tap **ONVIF Settings** on the **System** interface.



ONVIF Settings

Enable Authentication

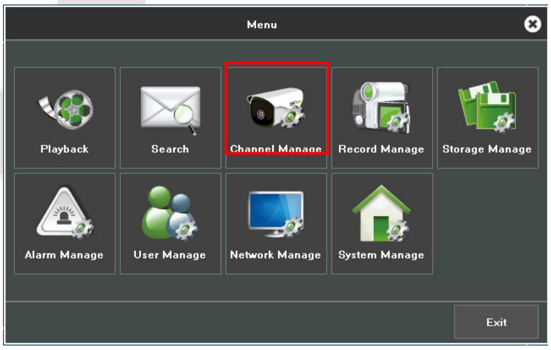
User Name admin

Password ******

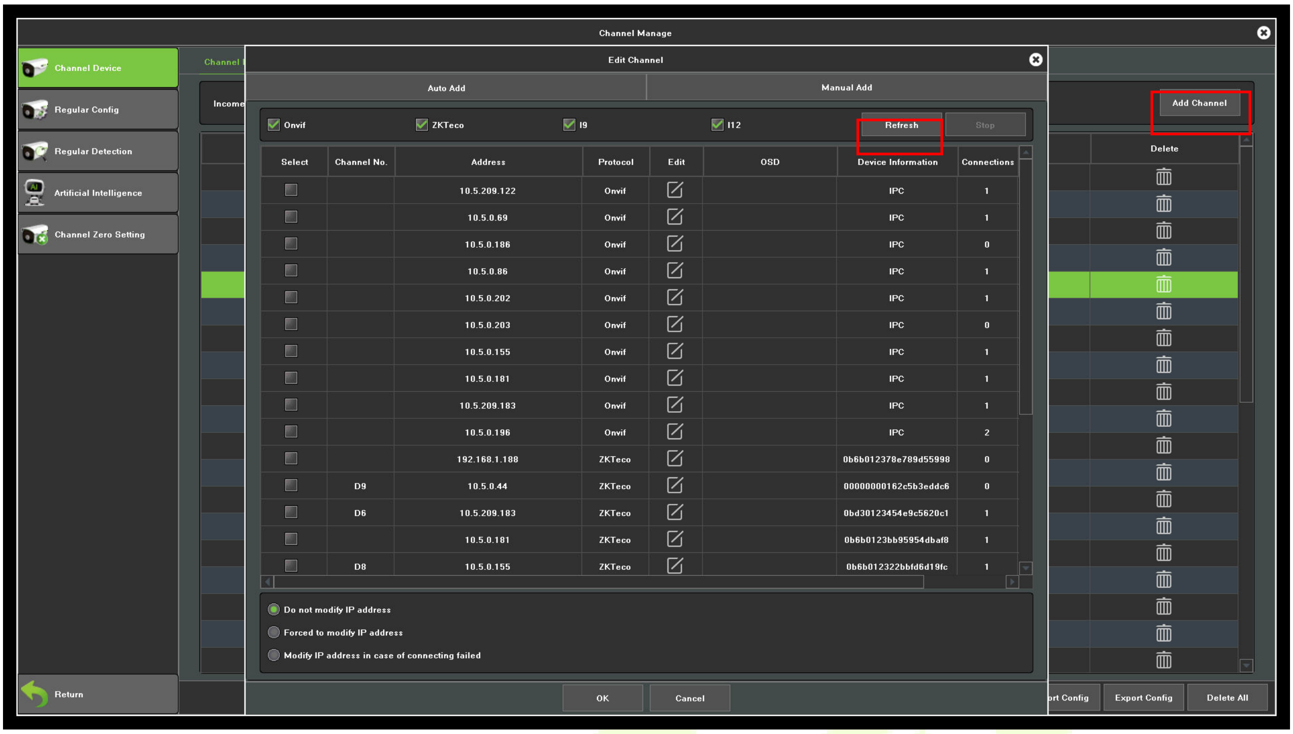
Server Port 8000

Function Name	Description
Enable Authentication	Enable/Disable the Authentication Function. When it is disabled, there is no need to input the User Name and Password when adding the device to the NVR.
User Name	Set the User Name. The default is admin.
Password	Set the password. The default is admin.
Server Port	The default is 8000, and cannot be modified.

3. On the NVR system, click on [**Start**] > [**Menu**], then the main menu will pop up.



4. Click [**Channel Manage**] > [**Add Channel**] > [**Refresh**] to search for the device.



Edit Channel

Auto Add | Manual Add

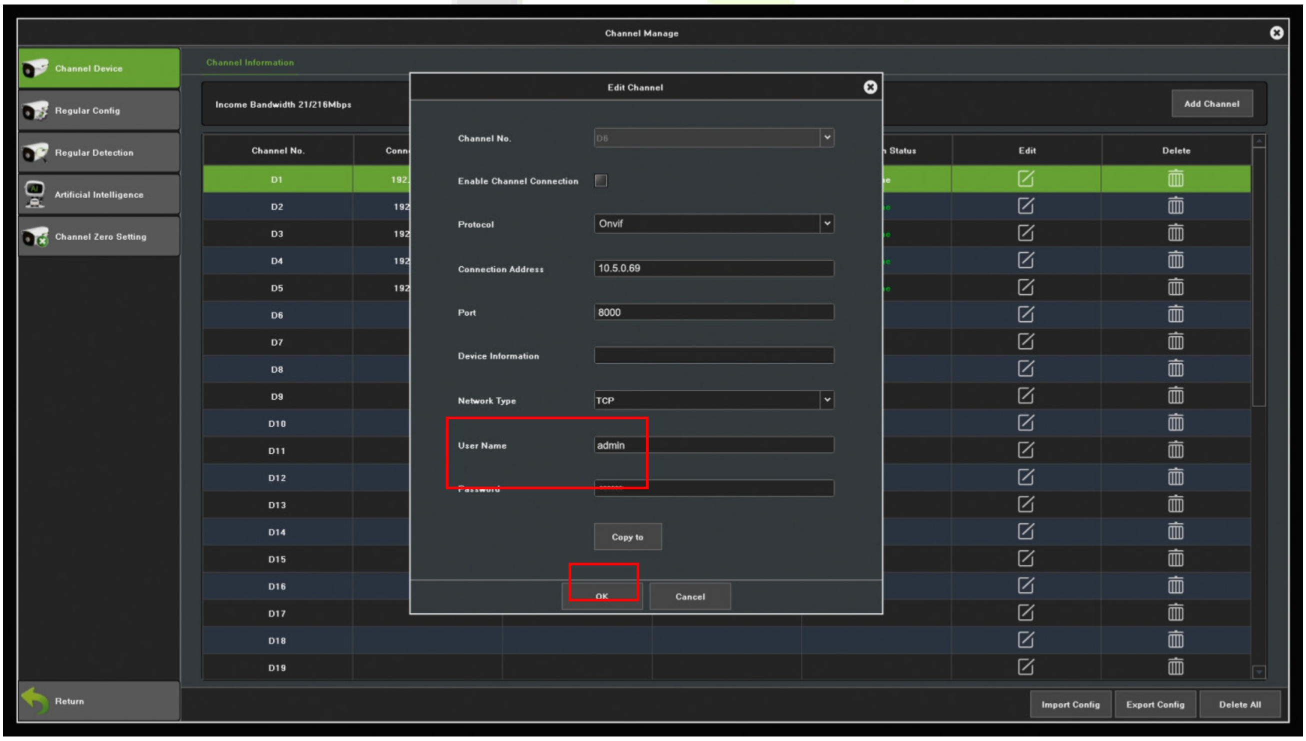
☑ Onvif ☑ ZKTeco ☑ I9 ☑ I12 Refresh Stop

Select	Channel No.	Address	Protocol	Edit	OSD	Device Information	Connections
□		10.5.209.122	Onvif			IPC	1
□		10.5.0.69	Onvif			IPC	1
□		10.5.0.186	Onvif			IPC	0
□		10.5.0.86	Onvif			IPC	1
□		10.5.0.202	Onvif			IPC	1
□		10.5.0.203	Onvif			IPC	0
□		10.5.0.155	Onvif			IPC	1
□		10.5.0.181	Onvif			IPC	1
□		10.5.209.183	Onvif			IPC	1
□		10.5.0.196	Onvif			IPC	2
□		192.168.1.188	ZKTeco			0b6b012378e789d55998	0
□	D9	10.5.0.44	ZKTeco			00000000162c5b3eddc6	0
□	D6	10.5.209.183	ZKTeco			0bd30123454e9c5620c1	1
□		10.5.0.181	ZKTeco			0b6b0123bb95954dbaf8	1
□	D8	10.5.0.155	ZKTeco			0b6b012322bbfd6d19fc	1

● Do not modify IP address
○ Forced to modify IP address
○ Modify IP address in case of connecting failed

OK Cancel

5. Select the checkbox for the device you want to add and edit the parameters in the corresponding text field, then click on **OK** to add it to the connection list.



Edit Channel

Channel No. D6

Enable Channel Connection □

Protocol Onvif

Connection Address 10.5.0.69

Port 8000

Device Information

Network Type TCP

User Name admin

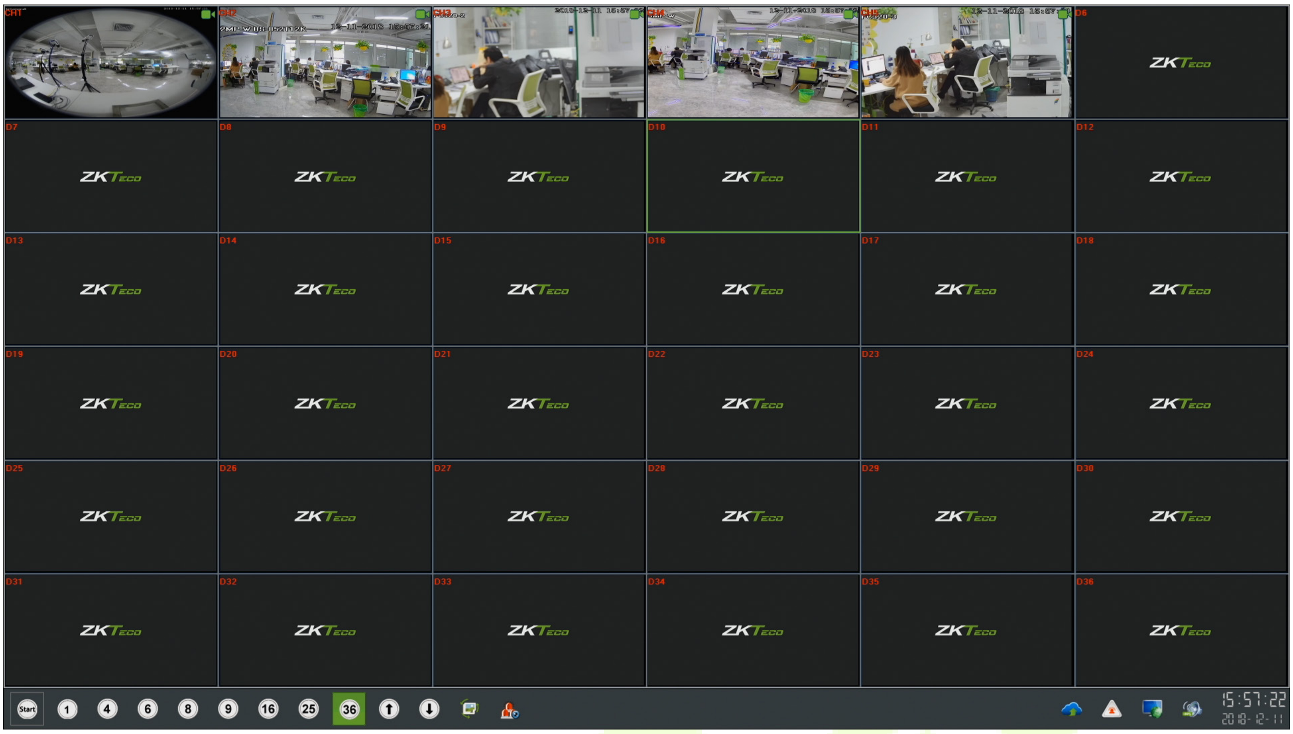
Password ******

Copy to

OK Cancel

Note: The User Name and Password is set in the **ONVIF Settings** of the device.

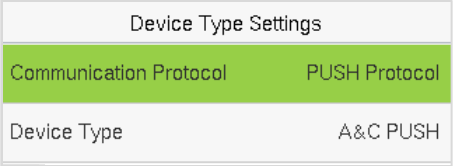
6. After adding successfully, the video image obtaining from the device can be viewed in real-time.



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

11.6 Device Type Settings

Tap **Device Type Setting** on the **System** interface to configure the Device Type Settings.



Device Type Settings

Communication Protocol PUSH Protocol

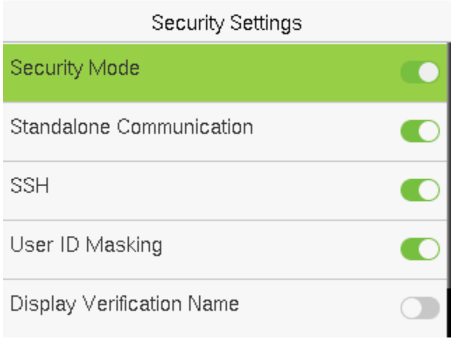
Device Type A&C PUSH

Function Name	Description
Communication Protocol	Set the PUSH protocol.
Device Type	Set the device as an access control terminal or attendance terminal.

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

11.7 Security Settings

Tap **Security Settings** on the **System** interface to go to the Security settings.



Security Settings

Security Mode ●

Standalone Communication ●

SSH ●

User ID Masking ●

Display Verification Name ○

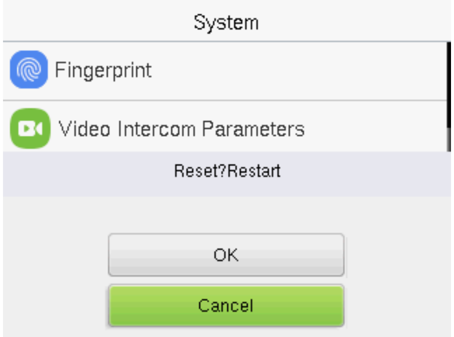
Function Description

Function Name	Description
Security Mode	Select whether to enable the security mode to protect the device and the user's personal information. You can set the device to work offline and hide the user's personal information to prevent leakage during user verification.
Standalone Communication	To avoid being unable to use when the device is offline, you can download the C/S software (such as ZKAccess 3.5) on your computer in advance for offline use.
SSH	SSH is used to enter the background of the device for maintenance.
User ID Masking	When enabled, and then the user is successfully compared and verified, the User ID in the displayed verification result will be replaced with an * to achieve secure protection of sensitive private data.
Display Verification Name	Set whether to display the username in the verification result interface.
Display Verification Mode	Set whether to display the verification mode in the verification result interface.

11.8 Factory Reset

The Factory Reset function restores the device settings such as communication settings and system settings, to the default factory settings (this function does not clear registered user data).

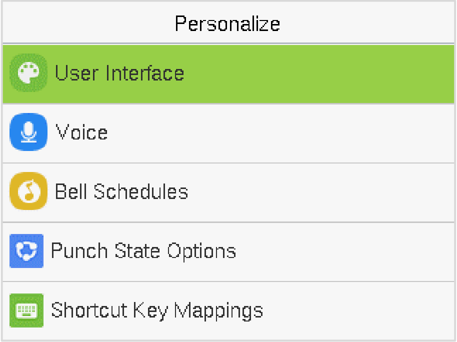
Tap **Reset** on the **System** interface and then tap **OK** to restore the default factory settings.



Reset?Restart

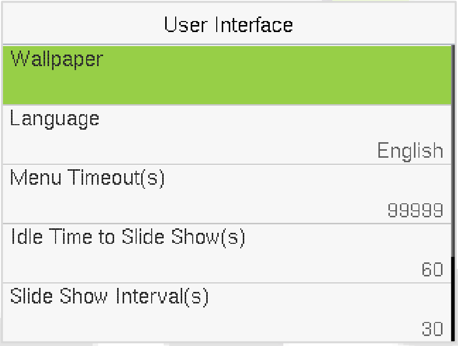
12 Personalize Settings

When the device is on the initial interface, press **[M/OK]** button > **Personalize** to customize the interface settings, voice, bell, punch state options, and shortcut key mappings.



12.1 User Interface

Tap **User Interface** on the **Personalize** interface to customize the display style of the main interface.



User Interface

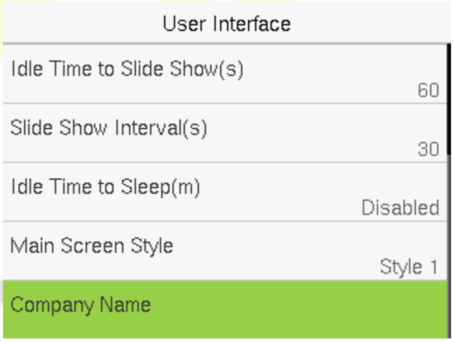
Wallpaper

Language: English

Menu Timeout(s): 99999

Idle Time to Slide Show(s): 60

Slide Show Interval(s): 30



User Interface

Idle Time to Slide Show(s): 60

Slide Show Interval(s): 30

Idle Time to Sleep(m): Disabled

Main Screen Style: Style 1

Company Name

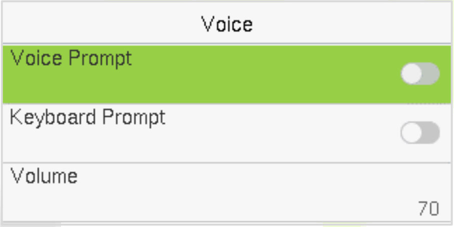
Function Description

Function Name	Description
Wallpaper	It helps to select the main screen wallpaper according to the user preference.
Language	It helps to select the language of the device.
Menu Timeout (s)	When there is no operation, and the time exceeds the set value, the device automatically goes back to the initial interface. The function can either be disabled or set the required 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 is displayed. The function can be disabled, or you may set the value between 3 and 999 seconds.

Slide Show Interval (s)	It is the time interval in switching between 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 the sleep mode is activated, and when there is no operation in the device, then the device will enter standby mode. This function can be disabled or set a value within 1 to 999 minutes.
Main Screen Style	The style of the main screen can be selected according to the user preference.
Company Name	Enter the company name here. When the company name option is turned on in the print information setting, the company name is printed.

12.2 Voice

Tap **Voice** on the **Personalize** interface to configure the voice settings.

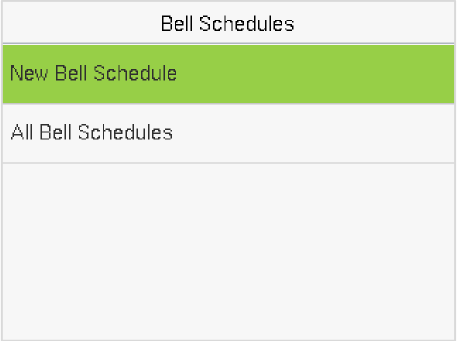


Function Description

Function Name	Description
Voice Prompt	Toggle to enable or disable the voice prompts during function operations.
Keyboard Prompt	Toggle to enable or disable the keypad sounds.
Volume	Adjust the volume of the device which can be set between 0 to 100.

12.3 Bell Schedules

Tap **Bell Schedules** on the **Personalize** interface to configure the Bell settings.



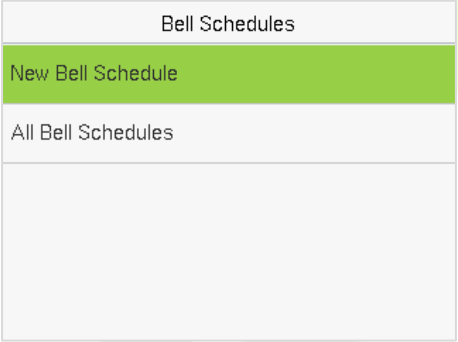
Bell Schedules

New Bell Schedule

All Bell Schedules

- **New Bell Schedule:**

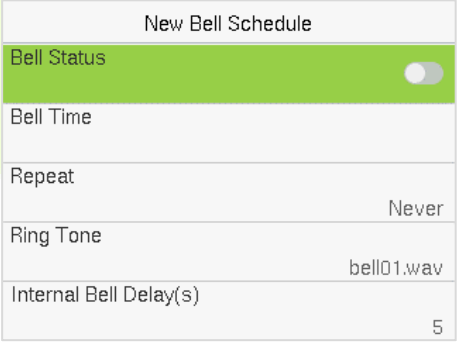
Tap **New Bell Schedule** on the **Bell Schedule** interface to add a new bell schedule.



Bell Schedules

New Bell Schedule

All Bell Schedules



New Bell Schedule

Bell Status ○

Bell Time

Repeat: Never

Ring Tone: bell01.wav

Internal Bell Delay(s): 5

Function Description

Function Name	Description
Bell Status	Toggle to enable or disable the bell status.
Bell Time	Once the required time is set, the device automatically triggers to ring the bell during that time.
Repeat	Set the required number of counts to repeat the scheduled bell.
Ring Tone	Select a ringtone.
Internal Bell Delay(s)	Set the replay time of the internal bell. Valid values range from 1 to 999 seconds.

- **All Bell Schedules:**

Once the bell is scheduled, on the **Bell Schedules** interface, tap **All Bell Schedules** to view the newly scheduled bell.

- **Edit the Scheduled Bell:**

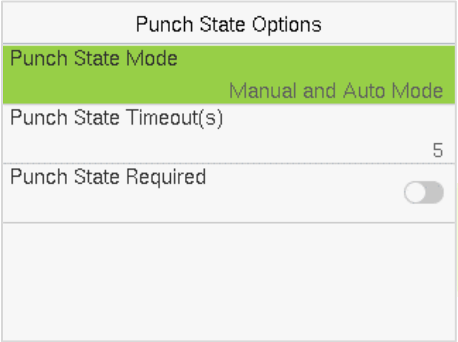
  On the **All Bell Schedules** interface, tap on the required bell schedule, and tap **Edit** to edit the selected bell schedule. The editing method is the same as the operations of adding a new bell schedule.

- **Delete a Bell Schedules:**

  On the **All Bell Schedules** interface, tap the required bell schedule, tap **Delete**, and then tap **Yes** to delete the selected bell.

12.4 Punch States Options

Tap **Punch States Options** on the **Personalize** interface to configure the punch state settings.

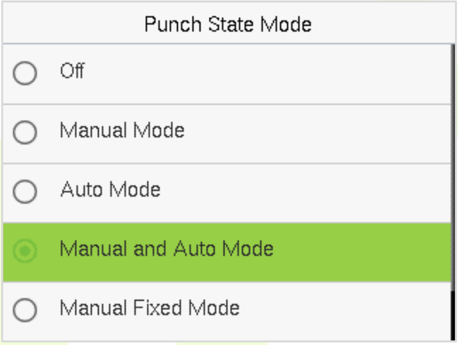


Punch State Options

Punch State Mode: Manual and Auto Mode

Punch State Timeout(s): 5

Punch State Required



Punch State Mode

○ Off

○ Manual Mode

○ Auto Mode

● Manual and Auto Mode

○ Manual Fixed Mode

Function Description

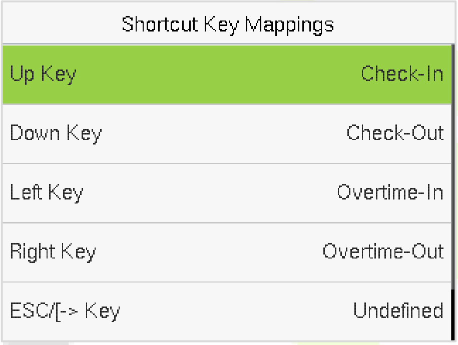
Function Name	Description
Punch State Mode	**Off:** Disable the punch state function. Therefore, the punch state key set under Shortcut Key Mappings menu will become invalid. **Manual Mode:** Switch the punch state key manually, and the punch state key will disappear after Punch State Timeout. **Auto Mode:** The punch state key will automatically switch to a specific punch status according to the predefined time schedule which can be set in the Shortcut Key Mappings. **Manual and Auto Mode:** The main interface will display the auto-switch punch state key. However, the users will still be able to select alternative that is the manual attendance status. After timeout, the manual switching to punch state key will become auto-switch punch state key. **Manual Fixed Mode:** After the punch state key is set manually to a particular punch status, the function will remain unchanged until it is being manually switched again. **Fixed Mode:** Only the manually fixed punch state key will be shown. Users cannot change the status by taping any other keys.
Punch State Timeout(s)	It is the time for which the punch state displays. The value ranges from 5 to 999 seconds.

Punch State Required	Select whether an attendance state needs to be selected after verification. **ON:** Attendance state needs to be selected after verification. **OFF:** Attendance state need not requires to be selected after verification.

12.5 Shortcut Key Mappings

Users may define shortcut keys for attendance status and functional keys which will be defined on the main interface. So, on the main interface, when the shortcut keys are tapped, the corresponding attendance status or the function interface will be displayed directly.

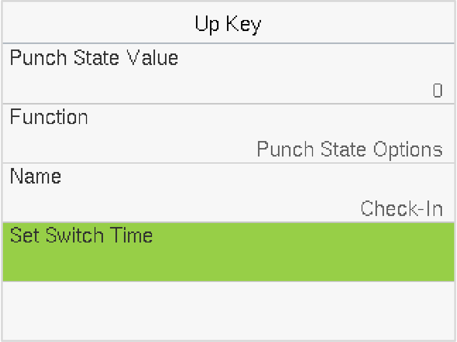
Tap **Shortcut Key Mappings** on the **Personalize** interface to set the required shortcut keys.



Shortcut Key Mappings

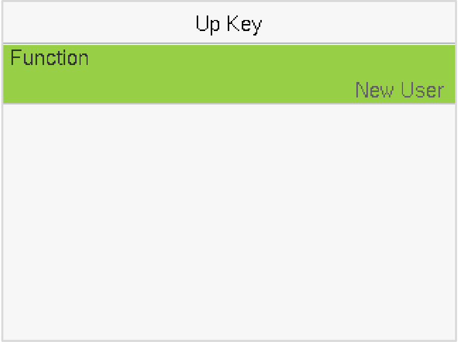
Up Key	Check-In
Down Key	Check-Out
Left Key	Overtime-In
Right Key	Overtime-Out
ESC/[-> Key	Undefined

- On the **Shortcut Key Mappings** interface, tap on the required shortcut key to configure the shortcut key settings.
- On the **Shortcut Key (example, "Up Key") interface,** tap **function** to set the functional process of the shortcut key either as punch state key or function key.
- If the Shortcut key is defined as a function key (such as New user, All users, etc.), the configuration is completed as shown in the image below.



Up Key

Punch State Value	0
Function	Punch State Options
Name	Check-In
Set Switch Time	



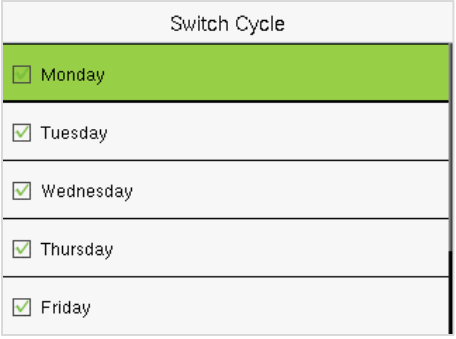
Up Key

Function	New User

- If the Shortcut key is set as a punch state key (such as check in, check out, etc.), then it is required to set the punch state value (valid value 0 to 250), name.

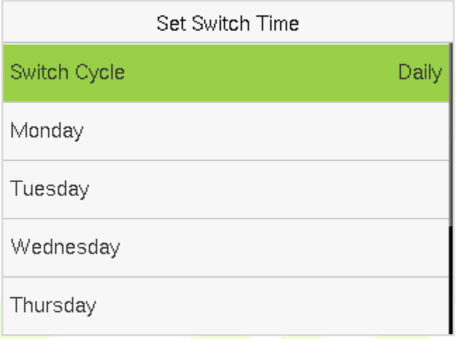
Set the Switch Time

- The switch time is set in accordance with the punch state options.
- When the **Punch State Mode** is set to **Auto Mode**, the switch time should be set.
- On the **Shortcut Key** interface, tap **Set Switch Time** to set the switch time.
- On the **Switch Cycle** interface, select the switch cycle (Monday, Tuesday, etc.) as shown in the image below.



Switch Cycle

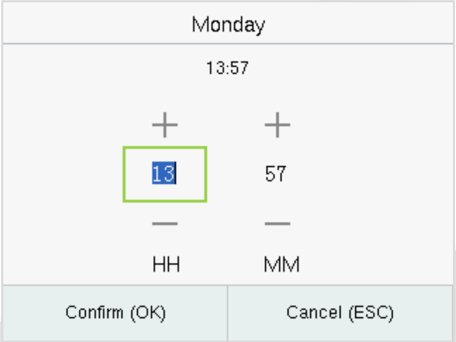
- □ Monday
- ☑ Tuesday
- ☑ Wednesday
- ☑ Thursday
- ☑ Friday



Set Switch Time

- Switch Cycle: Daily
- Monday
- Tuesday
- Wednesday
- Thursday

- Once the Switch cycle is selected, set the switch time for each day, and tap **OK** to confirm, as shown in the image below.

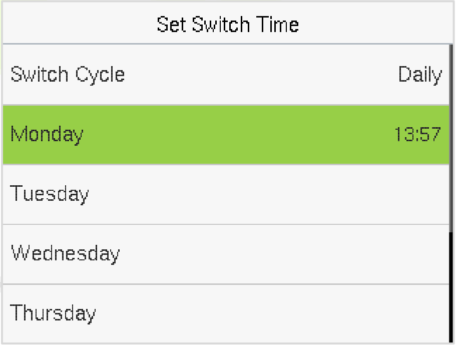


Monday

13:57

HH: 13

MM: 57



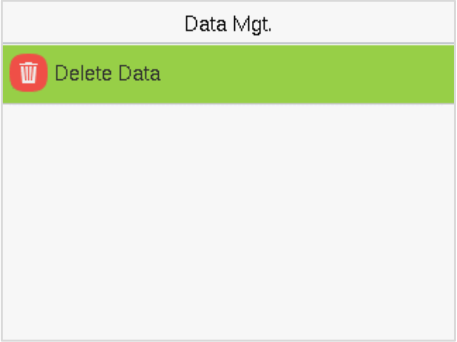
Set Switch Time

- Switch Cycle: Daily
- Monday: 13:57
- Tuesday
- Wednesday
- Thursday

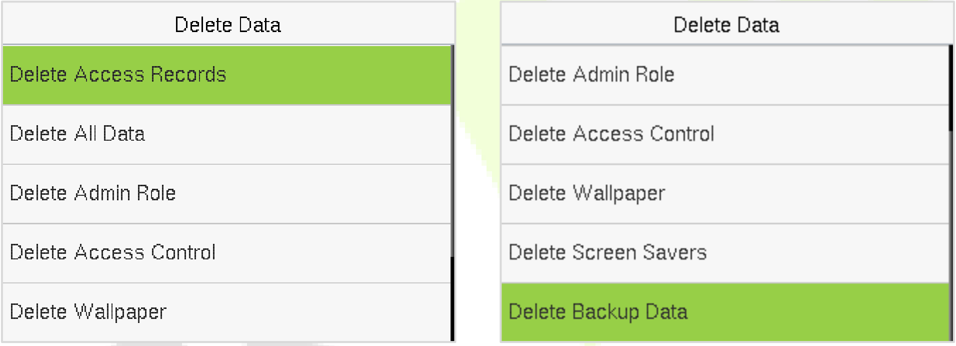
Note: When the function is set to Undefined, the device will not enable the punch state key.

13 Data Management

When the device is on the initial interface, press **[M/OK]** button > **Data Mgt.** to manage the relevant data in the device.



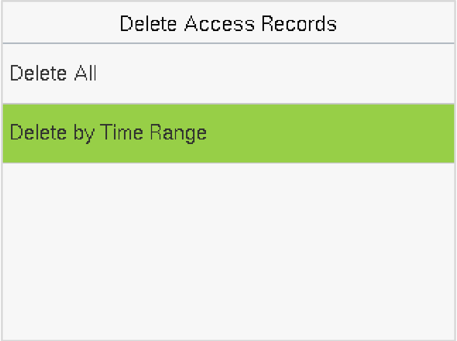
Tap **Delete Data** on the **Data Mgt.** interface to delete the required data.

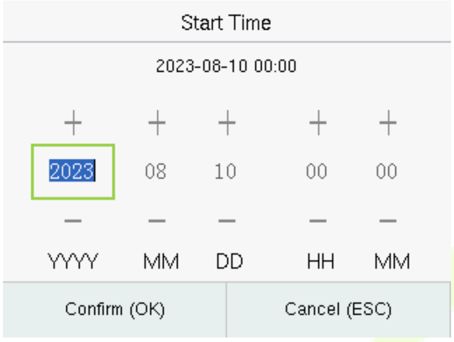


Function Description

Function Name	Description
Delete Access Records / Attendance Data	To delete the access records & attendance data conditionally.
Delete All Data	To delete the information and access records & attendance data of all registered users.
Delete Admin Role	To remove all the administrator privileges.
Delete Access Control	To delete all the access data.
Delete Wallpaper	To delete all the wallpapers in the device.
Delete Screen Savers	To delete all the screen savers in the device.
Delete Backup Data	To delete all the backup data in the device.

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





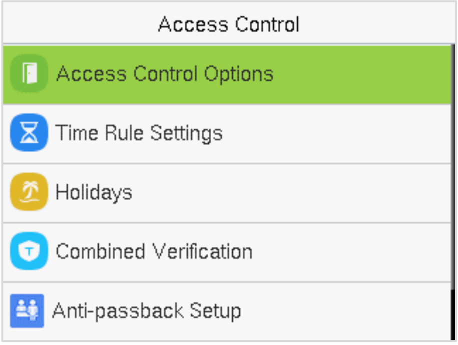
2023-08-10 00:00

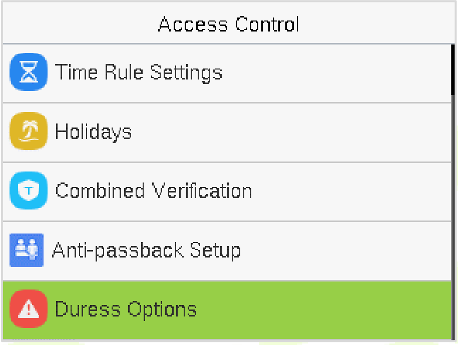
YYYY	MM	DD	HH	MM
2023	08	10	00	00

14 Access Control

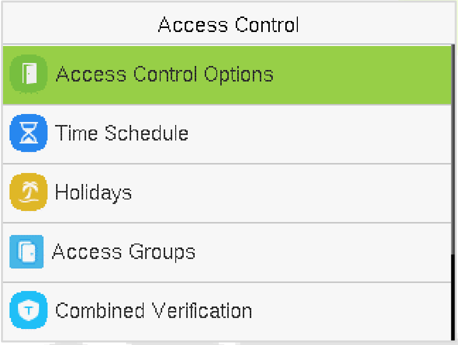
When the device is on the initial interface, press **[M/OK]** button > **Access Control** to set the schedule of the door opening, locks control and to configure other parameters settings related to access control.

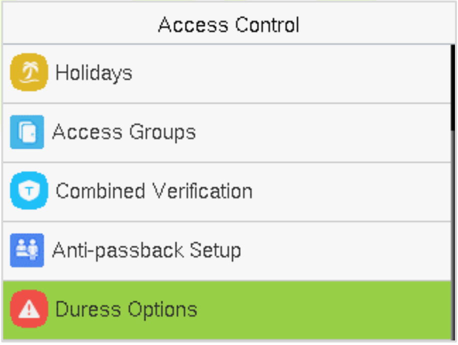
Access Control Terminal:





Time Attendance Terminal:





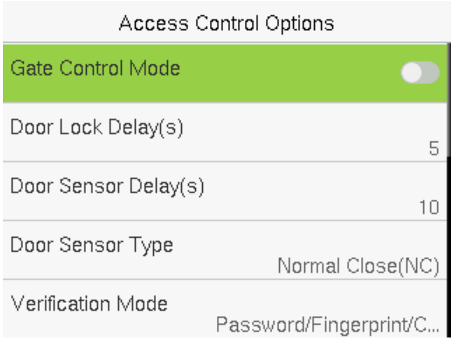
To get access, the registered user must meet the following conditions:

1. The relevant door's current unlock time should be within any valid time zone of the user's time period.
2. The corresponding user's group must be already set in the door unlock combination (and if there are other groups, being set in the same access combo, then the verification of those group's members is also required to unlock the door).
3. In default settings, new users are allocated into the first group with the default group time zone, where the access combo is "1" and is set in unlock state by default.

14.1 Access Control Options

Tap **Access Control Options** on the **Access Control** interface to set the parameters of the control lock of the terminal and related equipment.

Access Control Terminal:



Access Control Options

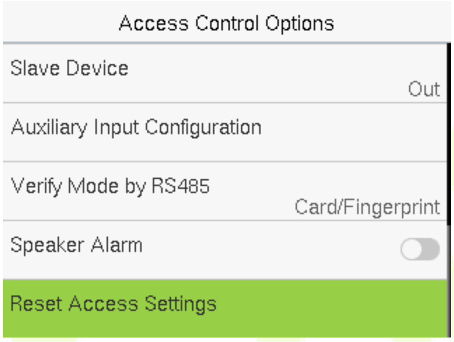
Gate Control Mode

Door Lock Delay(s) 5

Door Sensor Delay(s) 10

Door Sensor Type Normal Close(NC)

Verification Mode Password/Fingerprint/C...



Access Control Options

Slave Device Out

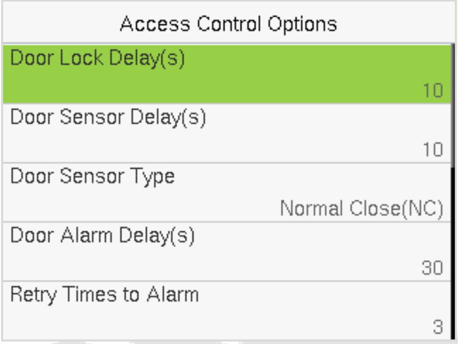
Auxiliary Input Configuration

Verify Mode by RS485 Card/Fingerprint

Speaker Alarm

Reset Access Settings

Time Attendance Terminal:



Access Control Options

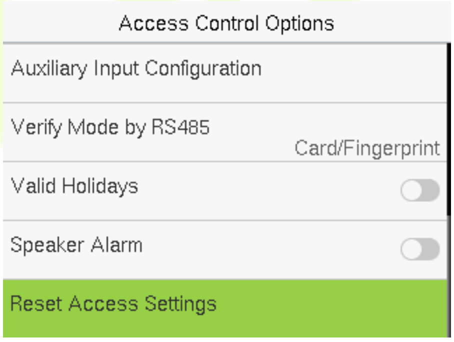
Door Lock Delay(s) 10

Door Sensor Delay(s) 10

Door Sensor Type Normal Close(NC)

Door Alarm Delay(s) 30

Retry Times to Alarm 3



Access Control Options

Auxiliary Input Configuration

Verify Mode by RS485 Card/Fingerprint

Valid Holidays

Speaker Alarm

Reset Access Settings

Function Description of Access Control Terminal:

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 Delay, Door Sensor Delay, 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: 1~99 seconds.
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/Fingerprint/Card, Fingerprint Only, User ID Only, Password, Card Only, Fingerprint/Password, Fingerprint/Card, User ID + Fingerprint, Fingerprint + Password, Fingerprint + Card, Fingerprint + Password + Card, Password + Card, Password/Card, User ID + Fingerprint + Password, Fingerprint + (Card/User ID).
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	When the RS485 reader function is turned on, the verification method is used when the device is used as a master or a slave.
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.

Function Description of Time Attendance Terminal:

Function Name	Description
Door Lock Delay (s)	The length of time that the device controls the electric lock to be in unlock state. Valid value: 0 to 10 seconds.
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 (NO):** It means the door is always left open when electric power is on. **Normally Closed (NC):** It means the door is always left closed when electric power is on.
Door Alarm Delay(s)	When the state of the door sensor is inconsistent with that of the door sensor type, alarm will be triggered after a time period; this time period is the Door Alarm Delay (the value ranges from 1 to 999 seconds).
Retry Times to Alarm	When the number of failed verifications reach the set value (value ranges from 1 to 9 times), the alarm will be triggered. If the set value is None, the alarm will not be triggered after failed verification.
Normal Close Time Period	It is the scheduled time-period for "Normal Close" mode so that the door is always closed during this 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.
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.

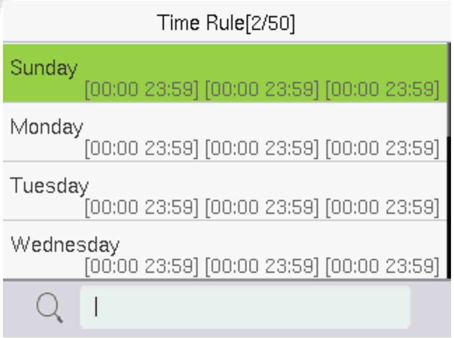
Verify Mode by RS485	When the RS485 reader function is turned on, the verification method is used when the device is used as a master or a slave.
Valid Holidays	To set if **Normal Close Time Period** or **Normal Open Time Period** settings are valid in set holiday time period. Choose [**ON**] to enable the set **NC** or **NO** time period in holiday.
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, door alarm delay, normal close time period, normal open time period, and alarm. However, erased access control data in Data Mgt. is excluded.

14.2 Time Rule Settings / Time Schedule

Tap **Time Rule Settings / Time Schedule** 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.

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



Time Rule[2/50]

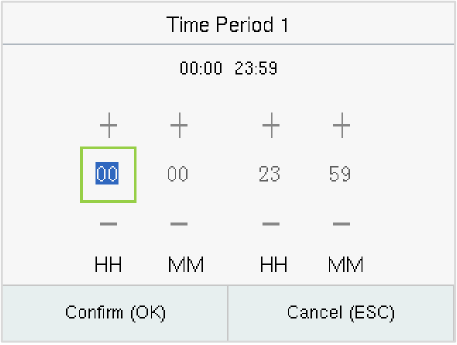
Sunday
[00:00 23:59] [00:00 23:59] [00:00 23:59]

Monday
[00:00 23:59] [00:00 23:59] [00:00 23:59]

Tuesday
[00:00 23:59] [00:00 23:59] [00:00 23:59]

Wednesday
[00:00 23:59] [00:00 23:59] [00:00 23:59]

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



Specify the start and the end time, and then tap **M/OK**.

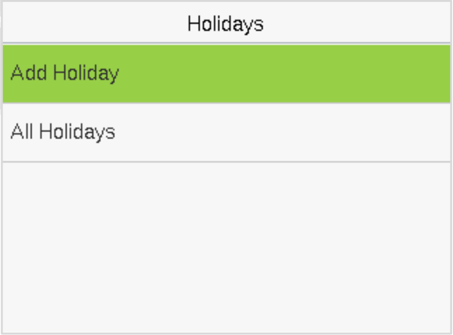
Note:

1. The door is inaccessible for the whole day when the End Time occurs before the Start Time (such as **23:57 to 23:56**).
2. It is the time interval for valid access when the End Time occurs after the Start Time (such as **08:00 to 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.

14.3 Holidays

When there is a holiday, you may need a different access time; however, altering everyone's access time one by one is extremely time-consuming. Thus, a holiday access time that applies to all workers can be set, and the user will be able to open the door during the holidays.

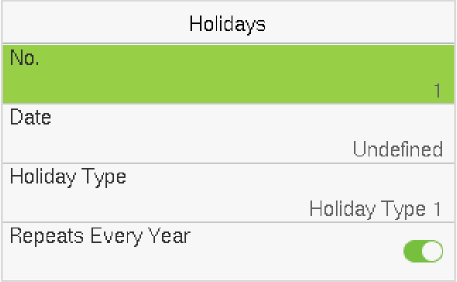
Tap **Holidays** on the **Access Control** interface to set the holiday access.



- **Add a New Holiday:**

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

Access Control Terminal:


Holidays

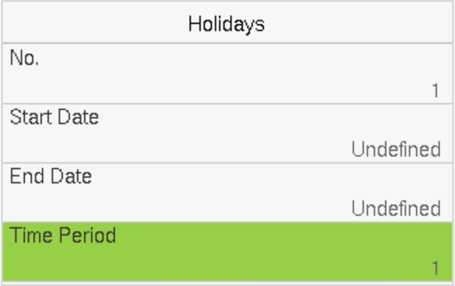
No.
1

Date
Undefined

Holiday Type
Holiday Type 1

Repeats Every Year

Time Attendance Terminal:


Holidays

No.
1

Start Date
Undefined

End Date
Undefined

Time Period
1

- **Edit a Holiday:**

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

- **Delete a Holiday:**

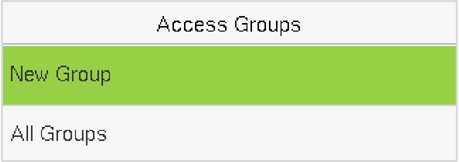
On the **Holidays** interface, select a holiday item to be deleted and tap **Delete**. Tap **M/OK** to confirm the deletion. After deletion, this holiday does not display on the **All Holidays** interface.

14.4 Access Groups

Grouping is to manage users in groups, only for time attendance terminal.

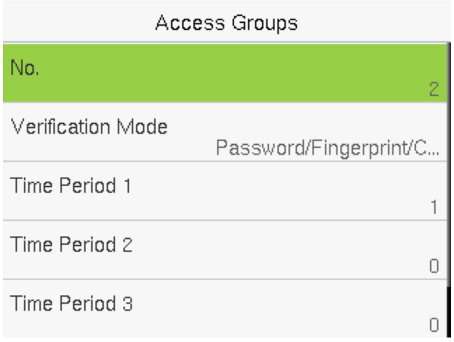
The default time zone for group members is the group time zone, while users can set their personal time zone. When the group verification mode and the user verification mode overlap, the user verification mode takes priority. Each group can set a maximum of 3 time zones; as long as one of them is valid, the group can be successfully verified. The newly enrolled user is assigned to Access Group 1 by default, but can be assigned to another access group.

Tap **Access Groups** on the **Access Control** interface.



- **Add a New Holiday:**

Tap **New Group** on the **Access Group** interface.



Access Groups

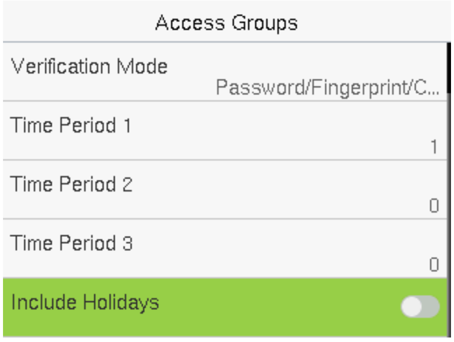
No. 2

Verification Mode Password/Fingerprint/C...

Time Period 1 1

Time Period 2 0

Time Period 3 0



Access Groups

Verification Mode Password/Fingerprint/C...

Time Period 1 1

Time Period 2 0

Time Period 3 0

Include Holidays

Note:

1. The system has a default access group numbered 1, which cannot be deleted but can be modified.
2. A number cannot be modified again after being set.
3. When the holiday is set to be valid, the personnel in a group can open the door only when group time period overlaps with the holiday time period.
4. When the holiday is set to be invalid, the access control time of the personnel in this group is not affected by holidays.

➢ **Edit Group:**

On the **All Group** interface, tap to select the access group item to be modified. Tap **Edit** to modify group parameters.

➢ **Delete a Group:**

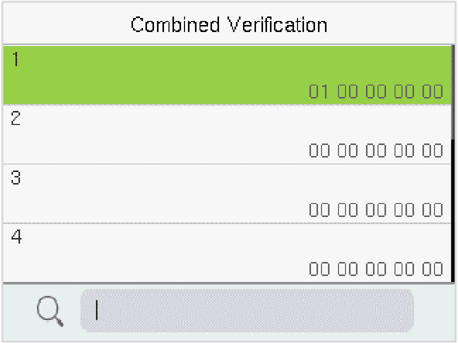
On the **All Group** interface, select an access group item to be deleted and tap **Delete**. Tap **M/OK** to confirm the deletion. After deletion, this group does not display on the **All Group** interface.

14.5 Combined Verification

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 ≤ N ≤ 5** and the number of members N may all belong to one access group or may belong to five different access groups.

Tap **Combined Verification** on the **Access Control** interface to configure the combined verification setting.



Combined Verification

1
01 00 00 00 00

2
00 00 00 00 00

3
00 00 00 00 00

4
00 00 00 00 00

On the combined verification interface, tap the Door-unlock combination to be set, and tap the **up** and **down** arrows to input the combination number, and then tap **M/OK**.

For Example:

- If the **Door-unlock combination 1** is set as (**01 03 05 06 08**). It indicates that the unlock combination 1 consists of 5 people and all the 5 individuals are from 5 groups, namely, AC Group 1, AC Group 3, AC Group 5, AC Group 6, and AC Group 8, respectively.
- If the **Door-unlock combination 2** is set as (**02 02 04 04 07**). It indicates that the unlock 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.
- If the **Door-unlock combination 3** is set as (**09 09 09 09 09**). It indicates that there are 5 people in this combination; all of which are from AC Group 9.
- If the **Door-unlock combination 4** is set as (**03 05 08 00 00**). It indicates that the unlock combination 4 consists of only 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.

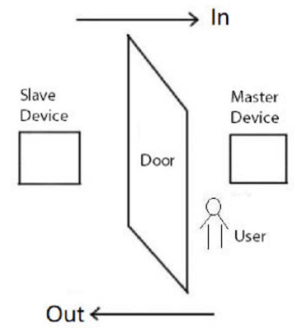
Note: To delete the door-unlock combination, set all Door-unlock combinations to 0.

14.6 Anti-passback Setup

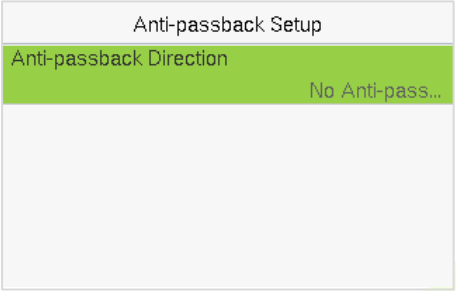
A user may be followed by some person(s) to enter the door without verification, resulting in a security breach. So, to avoid such situations, the Anti-Passback option was developed. Once it is enabled, the check-in and check-out record must occur alternatively to open the door to represent a consistent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

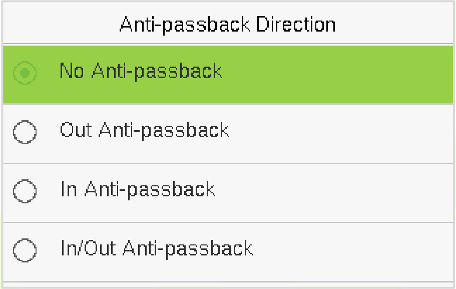


Tap **Anti-passback Setup** on the **Access Control** interface.



Anti-passback Setup

Anti-passback Direction
No Anti-pass...



Anti-passback Direction

● No Anti-passback

○ Out Anti-passback

○ In Anti-passback

○ In/Out Anti-passback

Function Description:

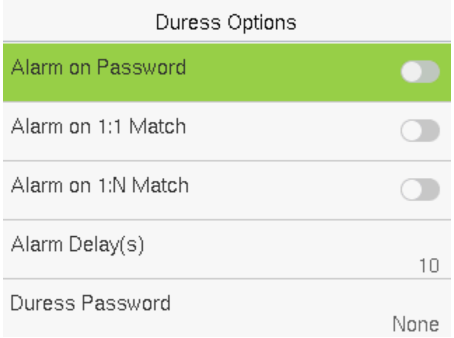
Function Name	Description
Anti-passback Direction	**No Anti-passback:** The Anti-Passback function is disabled, which means successful verification through either the master device or slave device can unlock the door. The attendance state is not saved in this option. **Out Anti-passback:** The user can 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.

14.7 Duress Options Settings

Once a user activates the duress verification function with a specific authentication method(s), and when he/she is under coercion and authenticates using duress verification, the device unlocks the door as usual. At the same time, a signal is sent to activate the alarm as well.

On the **Access Control** interface, tap **Duress Options** to configure the duress settings.

Access Control Terminal:



Duress Options

Alarm on Password

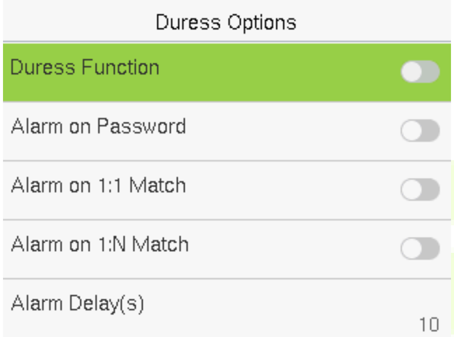
Alarm on 1:1 Match

Alarm on 1:N Match

Alarm Delay(s) 10

Duress Password None

Time Attendance Terminal:



Duress Options

Duress Function

Alarm on Password

Alarm on 1:1 Match

Alarm on 1:N Match

Alarm Delay(s) 10

Function Description of Access Control Terminal:

Function Name	Description
Alarm on Password	When a user uses the password verification method, an alarm signal will be generated, otherwise there will be no alarm signal.
Alarm on 1:1 Match	When a user uses the 1:1 verification method, an alarm signal will be generated, otherwise there will be no alarm signal.
Alarm on 1:N Match	When a user uses the 1:N verification method, an alarm signal will be generated, otherwise there will be no alarm signal.
Alarm Delay (s)	Alarm signal will not be transmitted until the alarm delay time is elapsed. 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 will be generated.

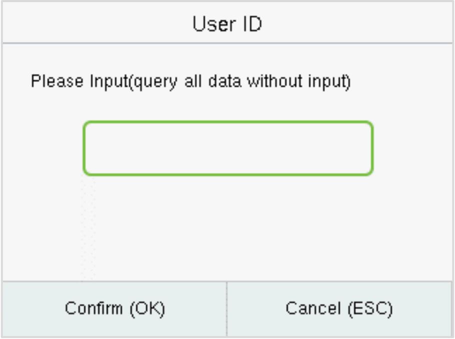
Function Description of Time Attendance Terminal:

Function Name	Description
Duress Function	Enable/Disable the duress function.
Alarm on Password	In [**ON**] state, when a user uses password verification method, alarm will be triggered. In [**OFF**] state, no alarm signal will be triggered.
Alarm on 1:1 Match	When a user uses the 1:1 verification method, an alarm signal will be generated, otherwise there will be no alarm signal.
Alarm on 1:N Match	When a user uses the 1:N verification method, an alarm signal will be generated, otherwise there will be no alarm signal.
Alarm Delay (s)	Alarm signal will not be transmitted until the alarm delay time is elapsed. The value ranges from 1 to 999 seconds.

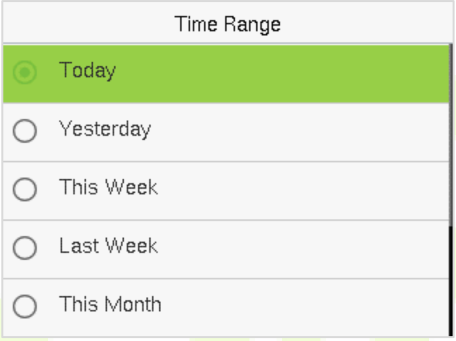
15 Attendance Search

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.

When the device is on the initial interface, press **[M/OK]** button > **Attendance Search** to search for the required event Logs.

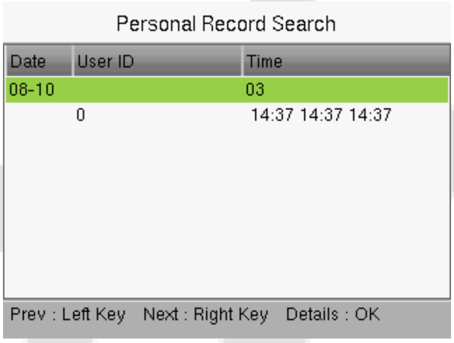

User ID

Please Input(query all data without input)


Time Range

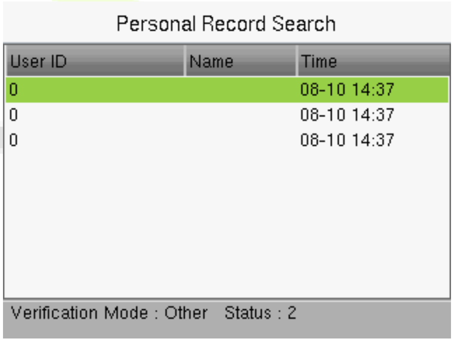
1. Enter the user ID to be searched and tap **M/OK**. If you want to search for records of all users, tap **M/OK** without entering any user ID.

2. Select the time range in which the records need to be searched.


Personal Record Search

Date	User ID	Time
08-10		03
	0	14:37 14:37 14:37

Prev : Left Key Next : Right Key Details : OK


Personal Record Search

User ID	Name	Time
0		08-10 14:37
0		08-10 14:37
0		08-10 14:37

Verification Mode : Other Status : 2

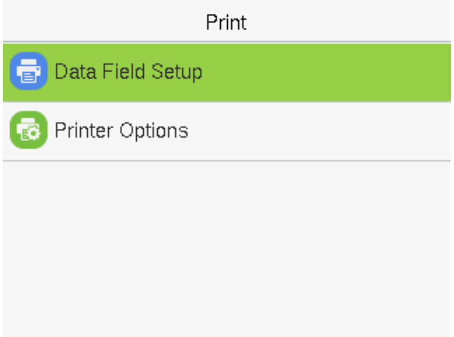
3. Once the record search completes. Tap the record highlighted in green to view its details.

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

16 Print Settings★

Devices with a printing function can print attendance records when a printer is connected.

When the device is on the initial interface, press **[M/OK]** button > **Print**.



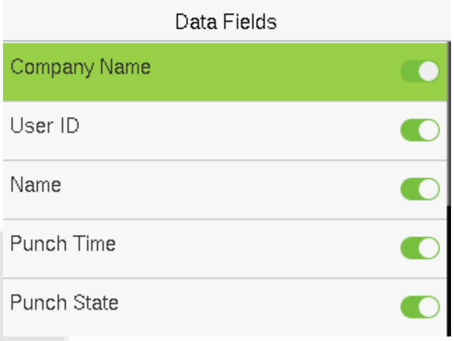
Print

Data Field Setup

Printer Options

16.1 Data Field Setup

Select **Data Field Setup** on the Print interface. Toggle button to turn on/off the fields requiring a print.



Data Fields

Company Name: On

User ID: On

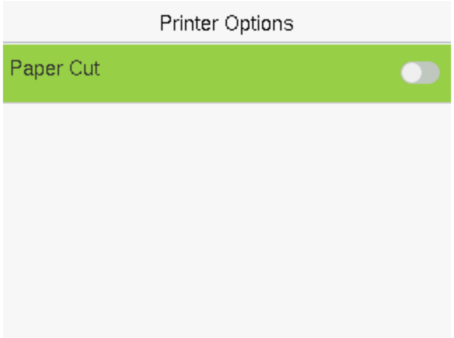
Name: On

Punch Time: On

Punch State: On

16.2 Print Options Settings

Select the **Printer Options** on the **Print** interface. Toggle button to enable or disable the **Paper Cut** function.



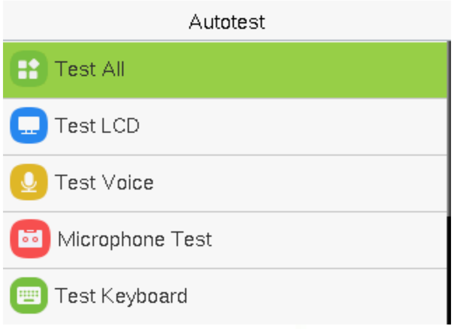
Printer Options

Paper Cut: Off

Remarks: To turn on the **Paper Cut** function, it is required to connect the device with a printer with paper cutting function, so that the printer will cut papers according to the selected printing information while printing.

17 Autotest

When the device is on the initial interface, press **[M/OK]** button > **Autotest**, it enables the system to automatically test whether the functions of various modules are working normally, including the LCD, Voice, Microphone, Keyboard, Fingerprint, Camera and Real-Time Clock (RTC).

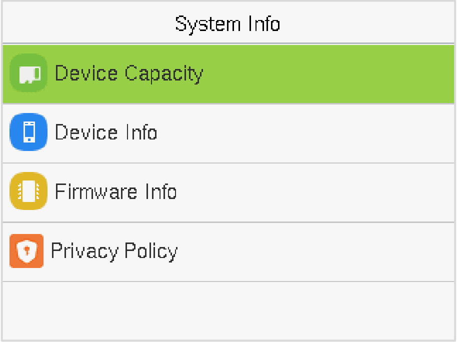


Function Description

Function Name	Description
Test All	To automatically test whether the LCD, Voice, Microphone, Fingerprint, Camera and Real-Time Clock (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 colors normally.
Test Voice	To automatically test whether the audio files stored in the device are complete and the voice quality is good.
Microphone test	To test if the microphone is working properly by speaking into the microphone.
Test Keyboard	The terminal tests whether every key on the keyboard works normally. Tap any key on the **Test Keyboard** interface to check whether the tapped key matches the key displayed on the screen. The keys are displayed as dark grey before and turn blue after tapped. Tap **ESC** to exit the test.
Test Fingerprint Sensor	To test the fingerprint sensor by pressing a finger on the scanner to check if the acquired fingerprint image is clear. When you are pressing a finger on the scanner, the fingerprint image will display on the screen.
Cam Test	To test if the camera functions properly.
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 tap it again to stop counting.

18 System Information

When the device is on the initial interface, press **[M/OK]** button > **System Info** to view the storage status, version information of the device, firmware information and privacy policy.



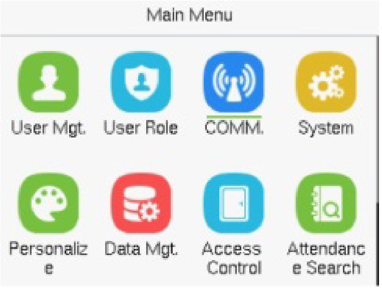
Function Description

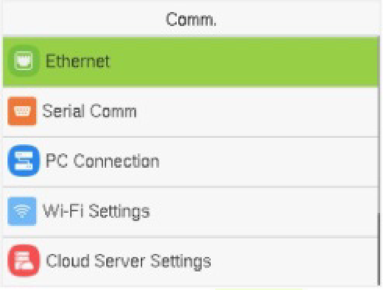
Function Name	Description
Device Capacity	Displays the current device's user storage, fingerprint, card and password storage, administrators and records.
Device Info	Displays the device's name, serial number, MAC address, Fingerprint algorithm, Platform information, MCU Version, Manufacturer, and manufacture date.
Firmware Info	Displays the firmware version and other version information of the device.
Privacy Policy	Display the device's privacy policy.

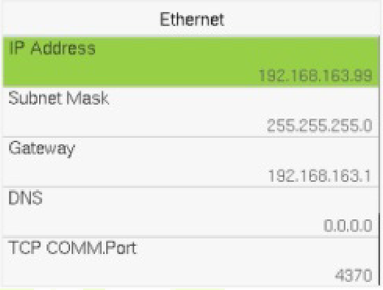
19 Connect to Webserver

19.1 Login Webserver

According to the configured network login, allows the Webserver to remotely view the information of the device (hardware, software, capacity and data, etc.), set up the system (communication, access control and system functions, etc.), add users and upgrade the system.






Ethernet

IP Address 192.168.163.99

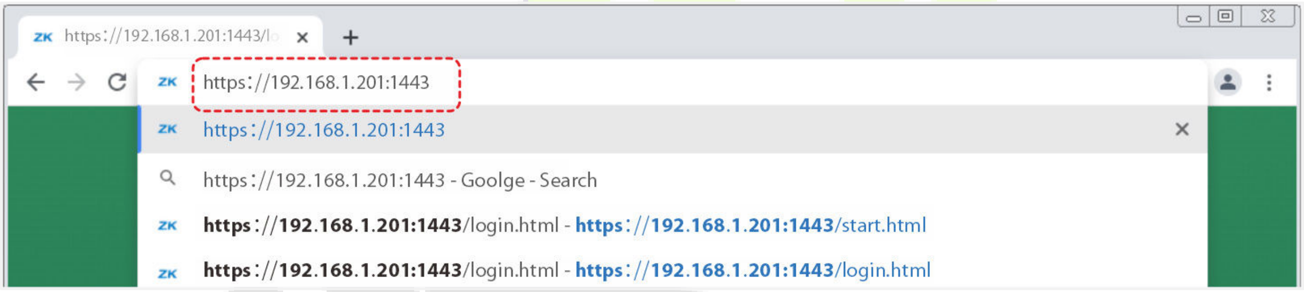
Subnet Mask 255.255.255.0

Gateway 192.168.163.1

DNS 0.0.0.0

TCP COMM.Port 4370

1. Open a browser to enter the address to log in to the WebServer, the address is **https:// Serial IP Address:1443**. For example: **https://192.168.1.201:1443.**


https://192.168.1.201:1443/l

https://192.168.1.201:1443

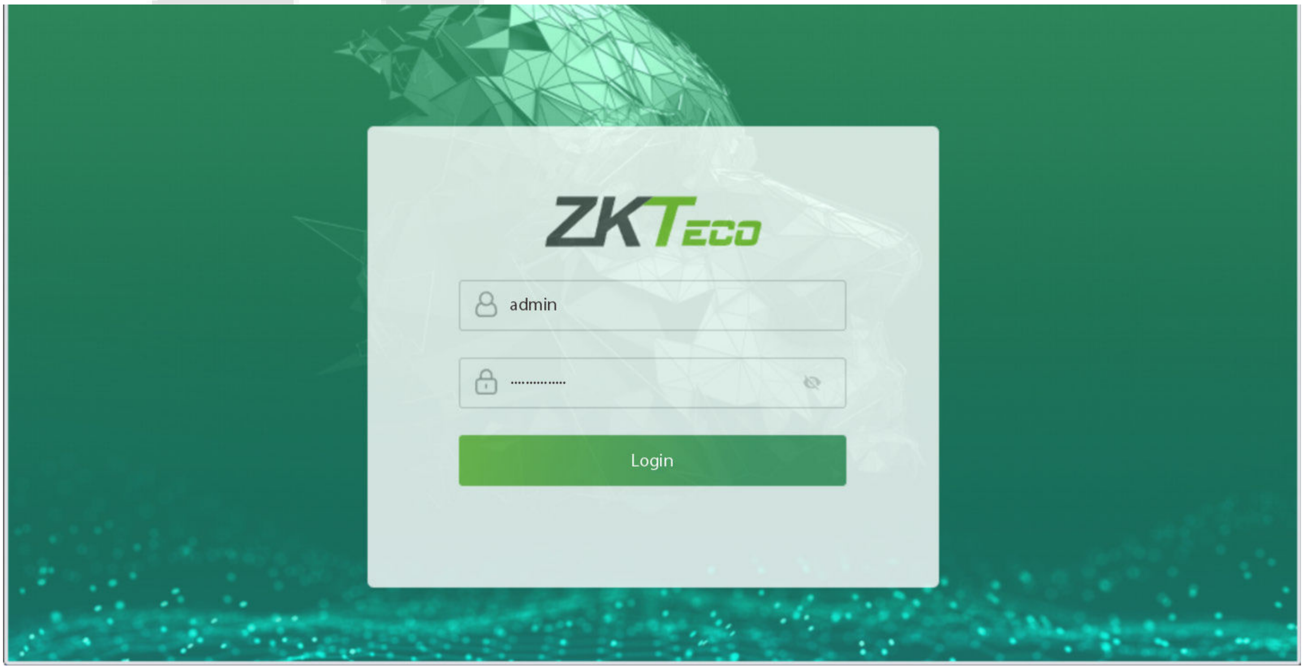
https://192.168.1.201:1443

https://192.168.1.201:1443 - Goolge - Search

https://192.168.1.201:1443/login.html - **https://192.168.1.201:1443**/start.html

https://192.168.1.201:1443/login.html - **https://192.168.1.201:1443**/login.html

2. Enter the WebServer account and password, the default account is: **admin**, password: **admin@123**.


admin

··············

Note:

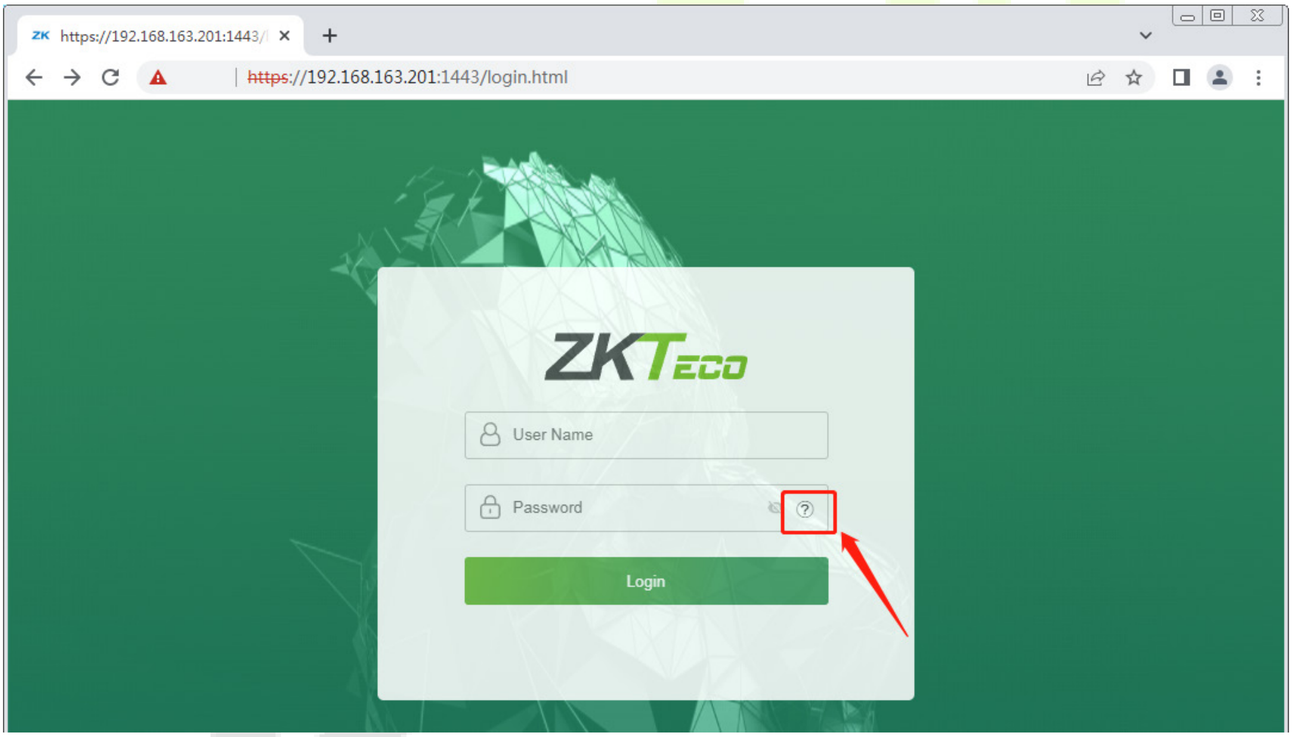
1. After logging in for the first time, it is suggested that the users change their original password, please refer to Change Password.
2. In order to retrieve the password easily, please register a super admin first, please refer to 8.1 User Registration.

19.2 Forgot Password

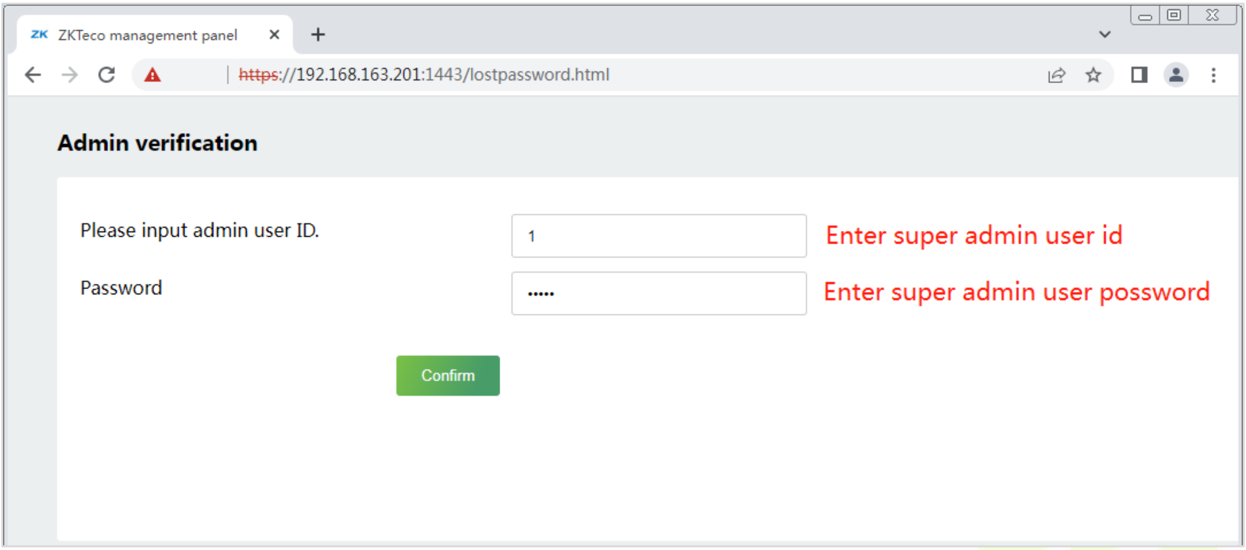
- **Method 1 (When there is a super admin):**

If you forgot the password of WebServer, you could reset it by the registered super admin. The detailed steps are as follows:

1. Click the icon on the login interface.


https://192.168.163.201:1443/
https://192.168.163.201:1443/login.html
ZKTeco
User Name
Password
Login

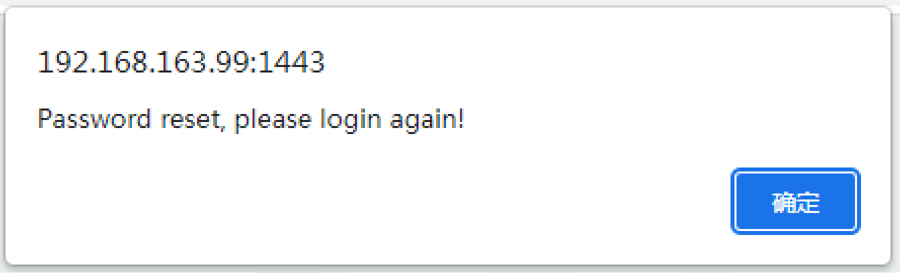
2. On the pop-up page, enter the relevant information of the super admin user as prompted.



Admin verification

Please input admin user ID. 1 Enter super admin user id

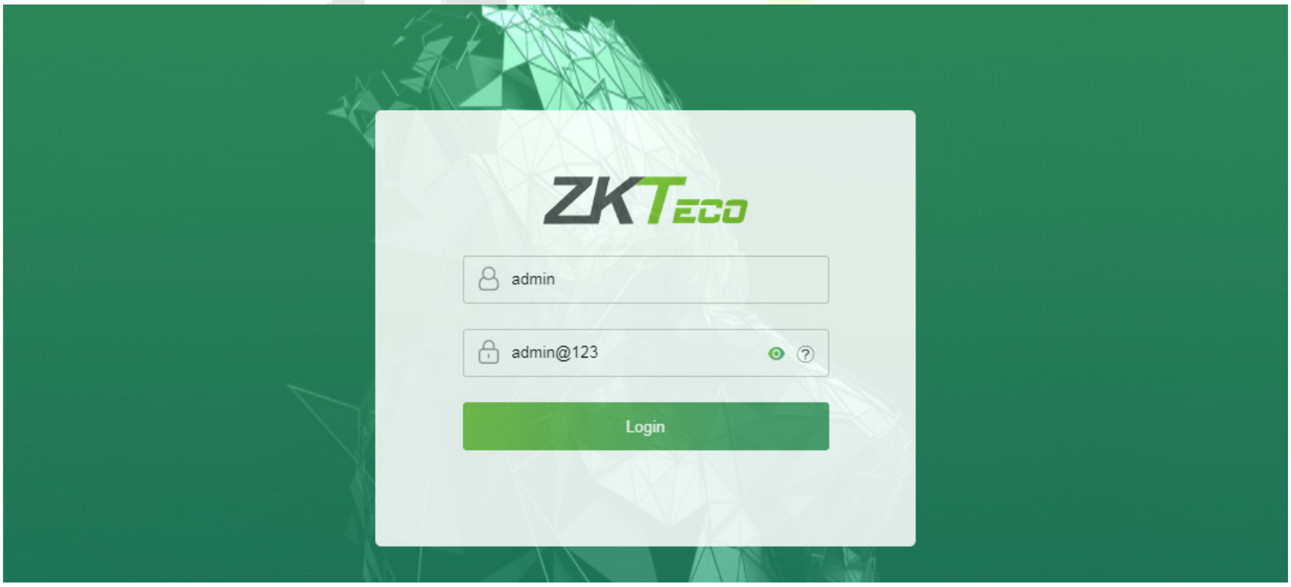
Password ••••• Enter super admin user password



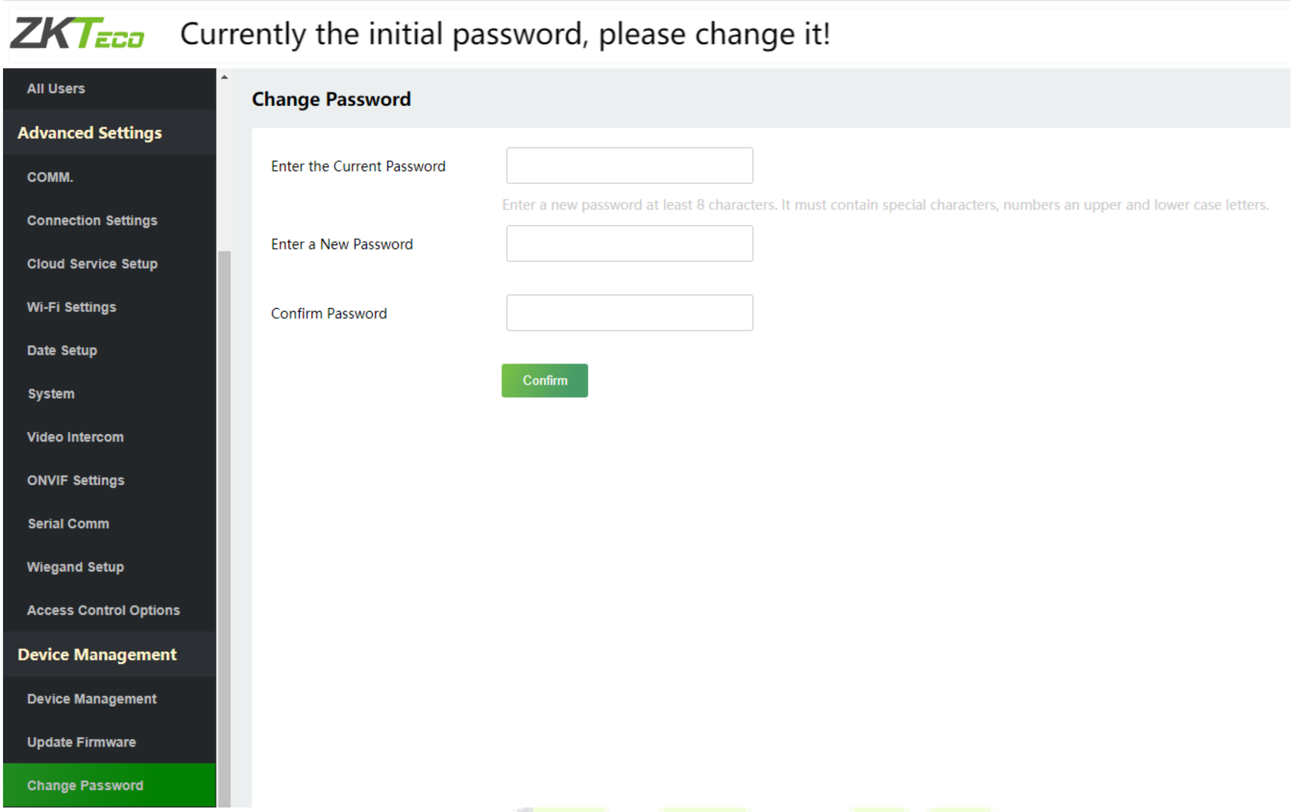
192.168.163.99:1443

Password reset, please login again!

3. After a successful reset, enter the default account and password (account: **admin**, password: **admin@123**) on the login interface to log in.



4. For security reasons, please change your password after successfully logging in.



Currently the initial password, please change it!

Change Password

Enter the Current Password

Enter a new password at least 8 characters. It must contain special characters, numbers an upper and lower case letters.

Enter a New Password

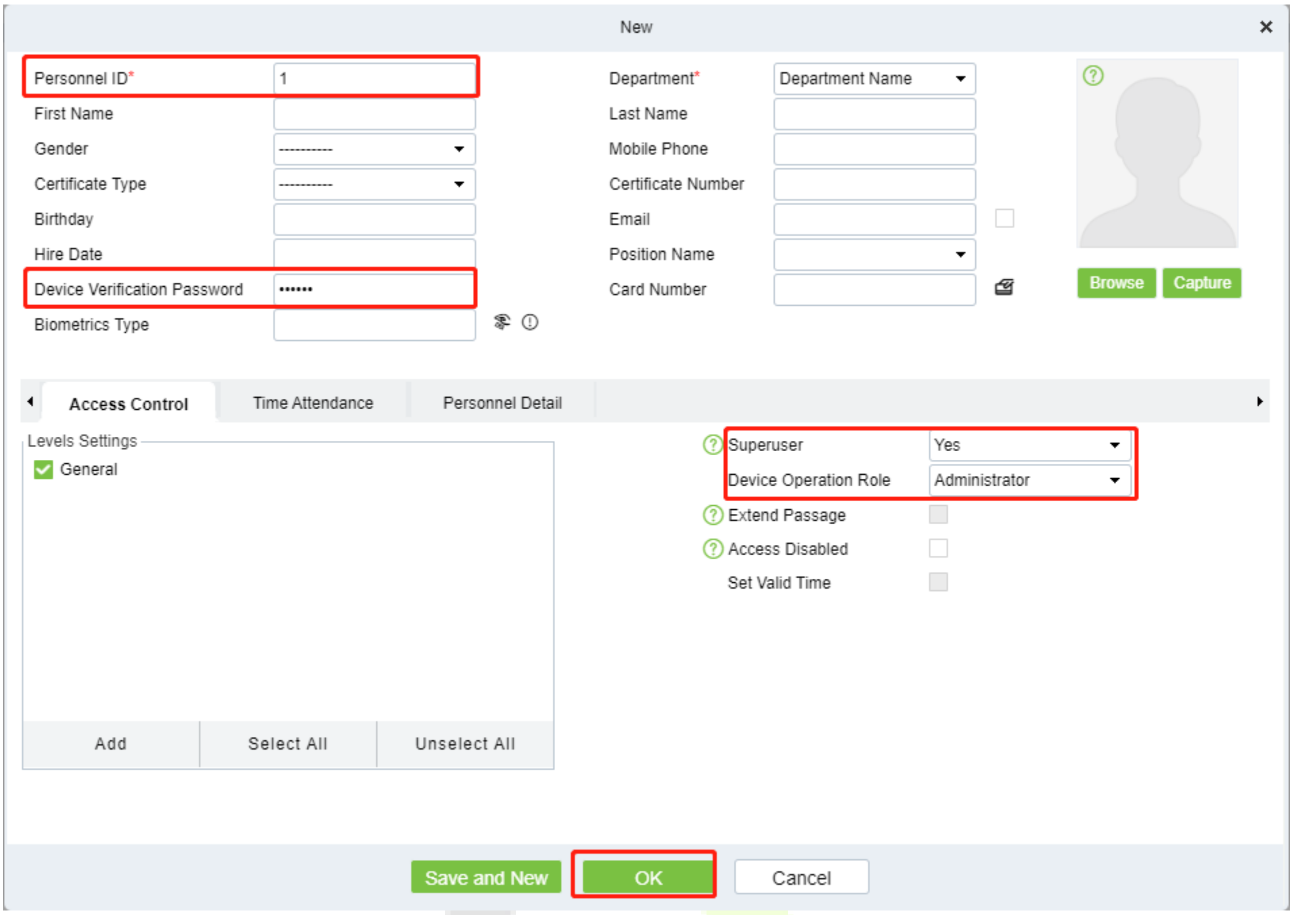
Confirm Password

Note: The super admin must exist.

- **Method 2 (When there is not a super admin):**

If the network of the device is normal and ZKBio CVAccess / ZKBioTime 8.0 has been connected, you can reset the password by sending the super admin account and password from the server.

1. Click **Personnel** > **Person** > **New** on the ZKBio CVAccess / ZKBioTime 8.0 Server; register the super admin information and set the super admin role on the new interface as required.



New

Personnel ID*	1	Department*	Department Name
First Name		Last Name	
Gender	----------	Mobile Phone	
Certificate Type	----------	Certificate Number	
Birthday		Email	
Hire Date		Position Name	
Device Verification Password	••••••	Card Number	
Biometrics Type			

☑ General

Superuser	Yes
Device Operation Role	Administrator
Extend Passage	□
Access Disabled	□
Set Valid Time	□

2. After registering the information of the super admin, click **OK**.

3. Click **Access** > **Device** > **Control** > **Synchronize All Data to Devices** to synchronize all the data to the device including the new users.

Note: For other specific operations, please refer *ZKBio CVAccess User Manual or ZKBioTime8.0 User Manual.*

4. After the data synchronization is successful, you can reset the password with the newly registered super admin. The operation steps are the same as method 1.

- **Method 3:**

If the device has not registered a super admin and cannot connect to the server, please contact our after-sales technicians to help retrieve the password.

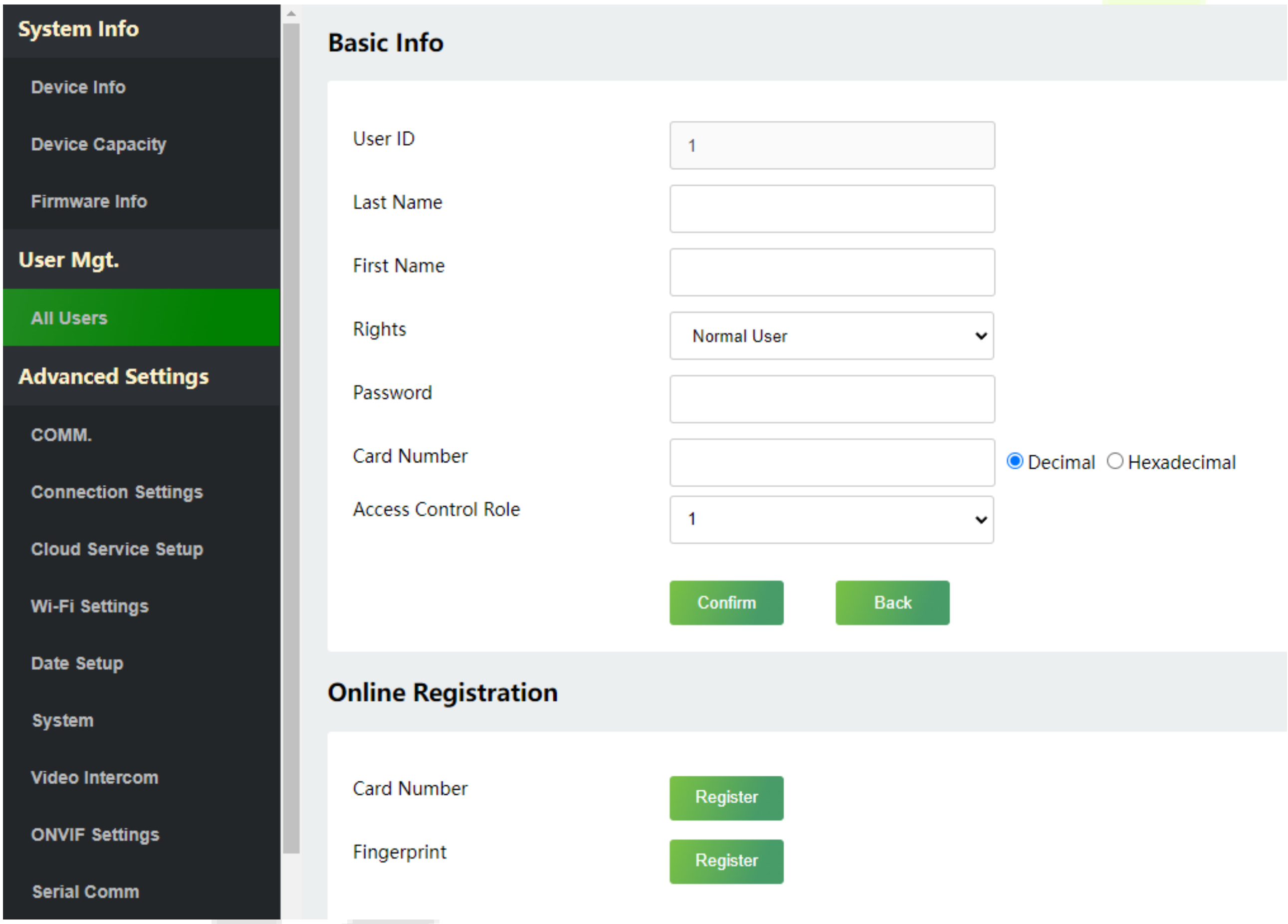
19.3 User Management

19.3.1 User Registration

- **Basic Information**

Click **All Users > New User** on the WebServer.

In this interface, you can register the User ID, Name, Rights, Password, Card Number and Access Control Role of the new user, click **Confirm** to save.



Basic Info

User ID	1
Last Name	
First Name	
Rights	Normal User
Password	
Card Number	● Decimal ○ Hexadecimal
Access Control Role	1

Online Registration

Function Name	Description
User ID	The user ID may contain 1 to 14 characters by default.
Last Name	A name can be up to 63 characters.
First Name	A name can be up to 63 characters.

Rights	Set the role for the user as either Normal User or Super Admin. ● **Super Admin:** The Super Admin owns all management privileges in the WebServer. ● **Normal User:** If the Super Admin is already registered in the WebServer, then the Normal Users will not have the privileges to manage the system and can only access authentication verifications.
Password	Set the user's registration password.
Card Number	Select the type of the card number and enter it manually, after registering the user's card number, the user can swipe the card for verification.
Access Control Role	The Access Control Role sets the door access privilege for each user, new users will be added to Group 1 by default, which can be reassigned to other required groups. The system supports up to 10 access control groups.

Note:

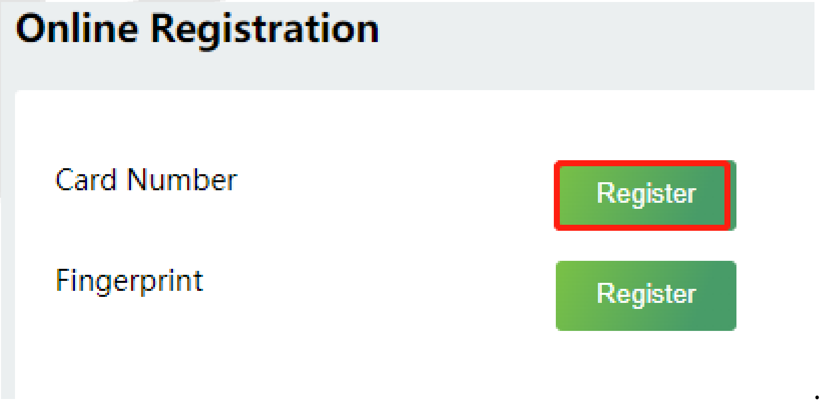
1. During the initial registration, you can modify your ID; you cannot be modifying the registered ID once after the successful registration.
2. If the message **"Registration failed!"** pops up, you must choose a different User ID because the one you entered already exists.

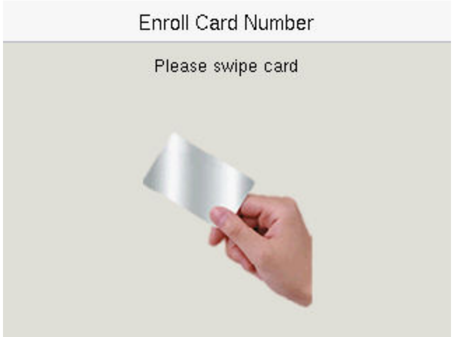
- **Online Registration**

In this interface, you can register the User's Card Number and Fingerprint. The verification mode can only be registered after the basic information is confirmed.

➢ <u>**Register Card Number**</u>

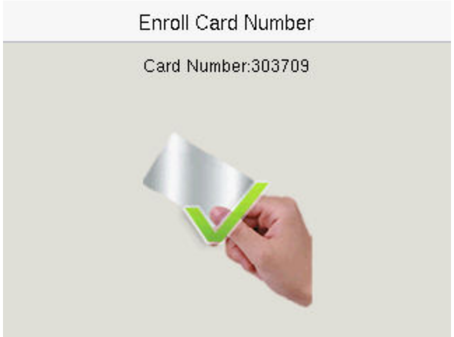
In the current interface, behind the card number bar, click **Register**, and the device will display the card number registration interface in real time, swipe the card underneath the card reading area. The registration of the card will be successful.





Enroll Card Number

Please swipe card

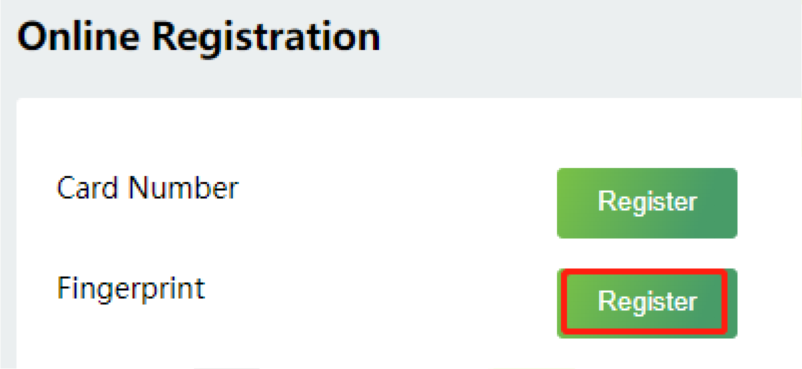


Enroll Card Number

Card Number:303709

- **Register Fingerprint**

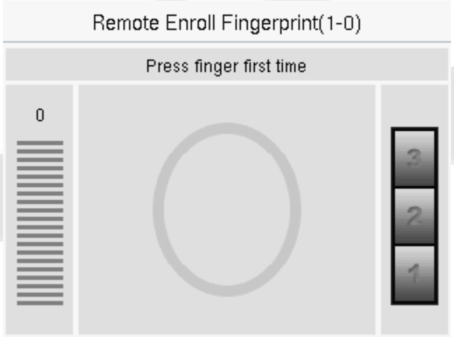
In the current interface, behind the fingerprint bar, click **Register**, and the device will display the fingerprint registration interface in real time, press your finger onto the fingerprint sensor of the device, and follow the instructions to complete the registration.



Online Registration

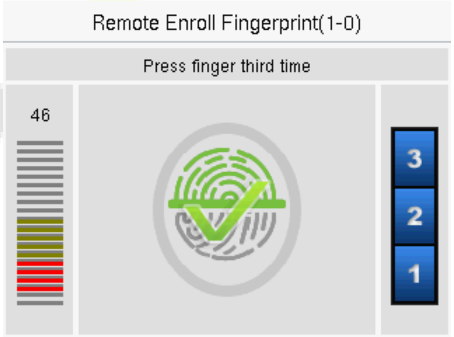
Card Number

Fingerprint



Remote Enroll Fingerprint(1-0)

Press finger first time



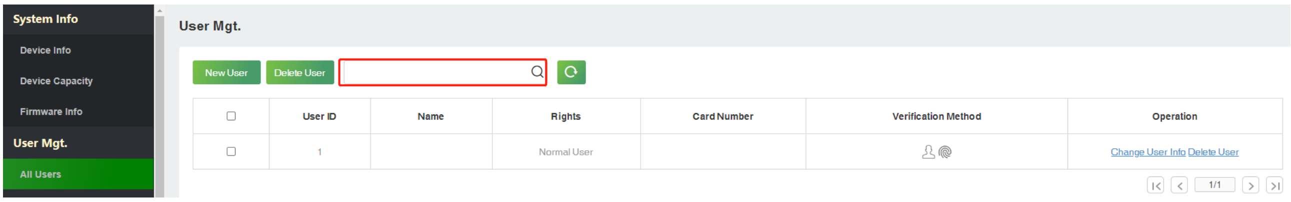
Remote Enroll Fingerprint(1-0)

Press finger third time

For fingerprint pressing operation, please refer to Finger Positioning.

19.3.2 Search for Users

Click **All Users** on the WebServer, click the search bar to enter the required retrieval keyword (where the keyword may be the user ID, surname or full name) and the system will search for the related user information.



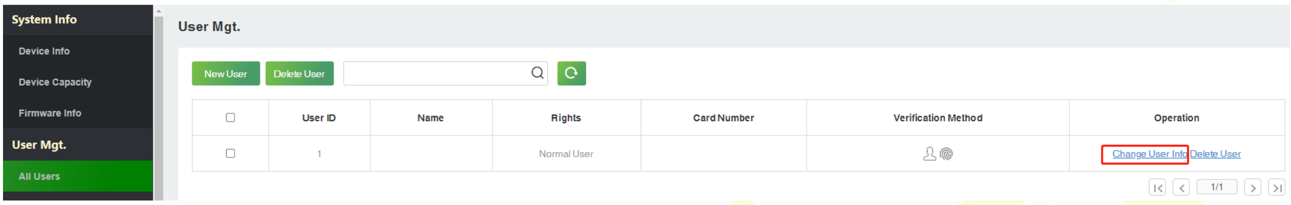
User Mgt.

□	User ID	Name	Rights	Card Number	Verification Method	Operation
□	1		Normal User			Change User Info Delete User

1/1

19.3.3 Edit User

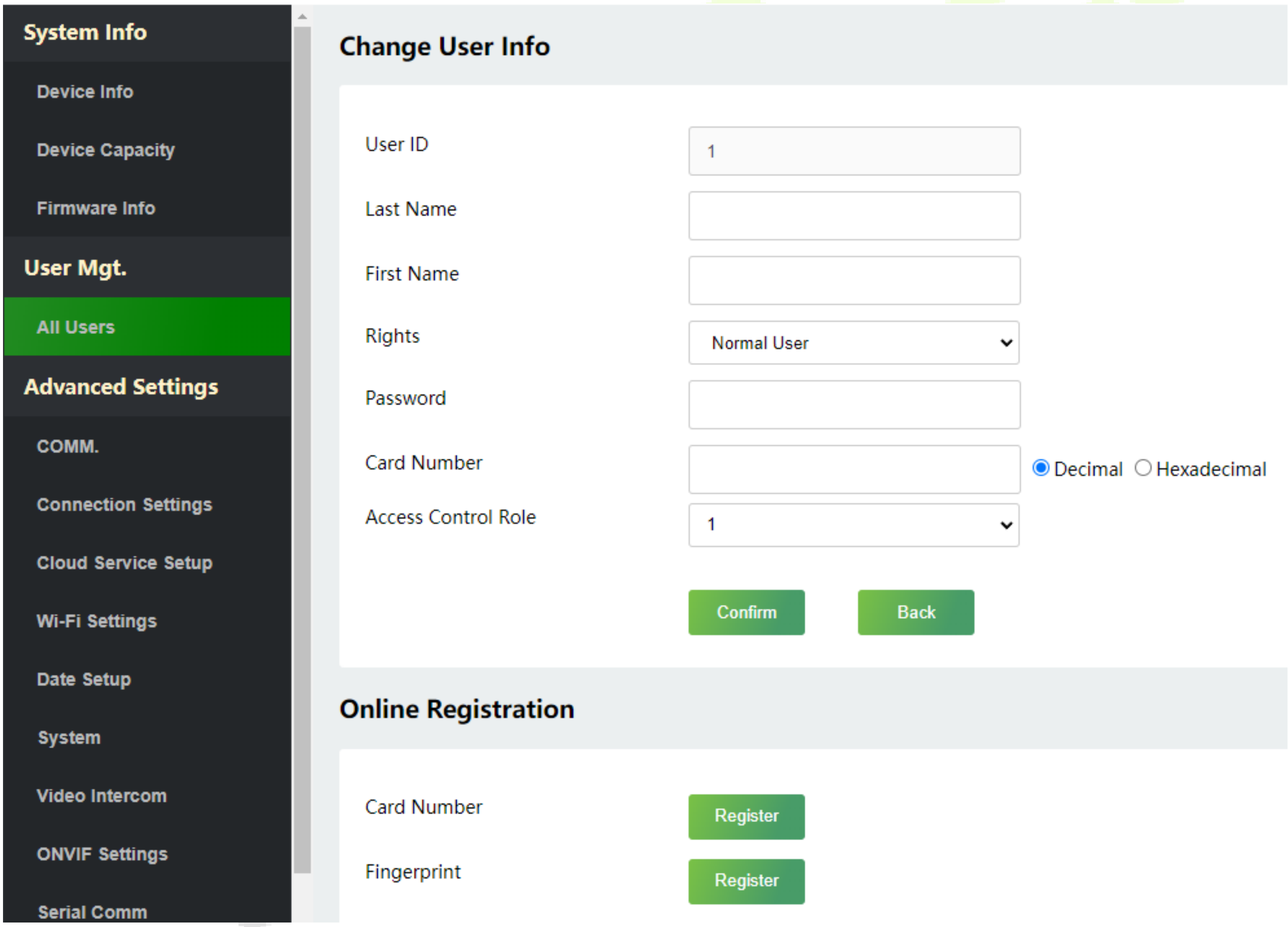
On the **All Users** interface, select the required user from the list and click **Change User Info** to edit the user information.



User Mgt.

□	User ID	Name	Rights	Card Number	Verification Method	Operation
□	1		Normal User			Change User Info Delete User

1/1



Change User Info

User ID	1
Last Name	
First Name	
Rights	Normal User
Password	
Card Number	● Decimal ○ Hexadecimal
Access Control Role	1

Confirm Back

Online Registration

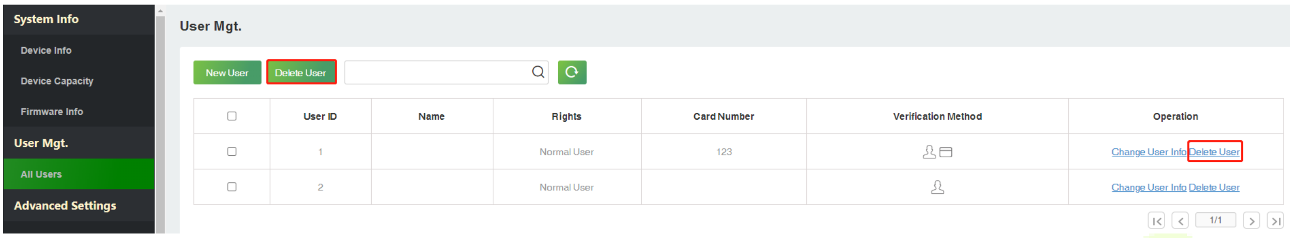
Card Number Register

Fingerprint Register

Note: The process of editing the user information is the same as that of adding a new user, except that the User ID cannot be modified. The process in detail refers to 19.3.1 User Registration.

19.3.4 Delete User

On the **All Users** interface, select the required user from the list and click **Delete User** to delete the user. Here individual deletion and batch deletion is available.



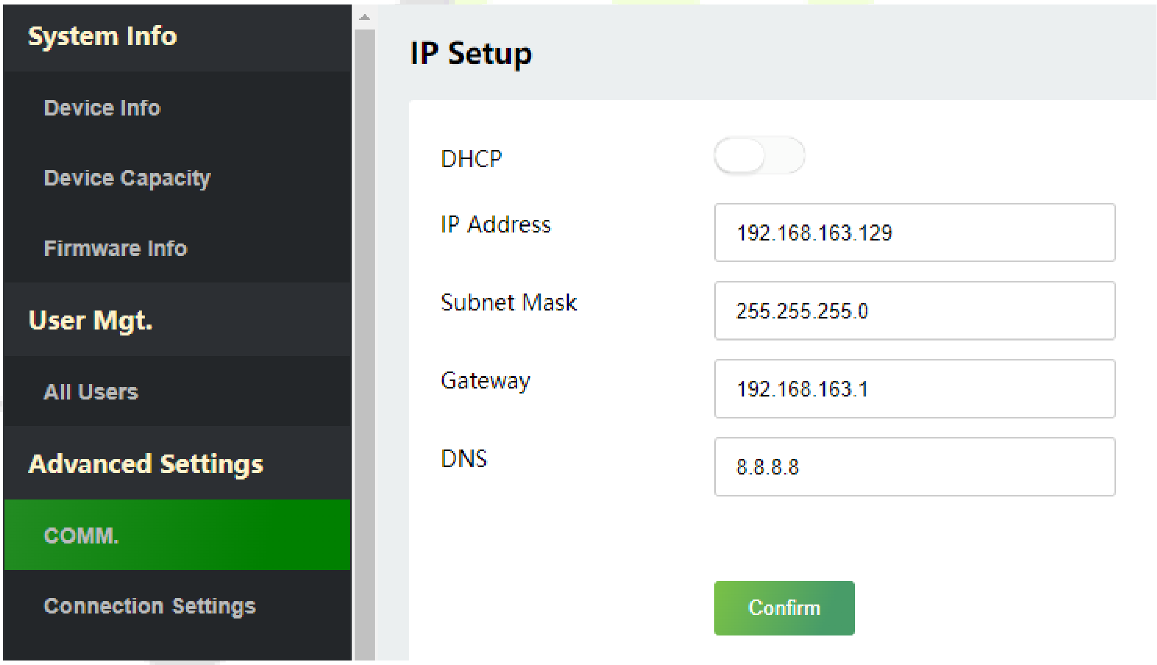
□	User ID	Name	Rights	Card Number	Verification Method	Operation
□	1		Normal User	123	👤 ▭	Change User Info Delete User
□	2		Normal User		👤	Change User Info Delete User

19.4 Advanced Settings

19.4.1 Communication Settings

Click **COMM.** on the WebServer.

Change the IP address of the device as needed, click **Confirm** to save, and the device will automatically synchronize the IP information.



DHCP ○

IP Address 192.168.163.129

Subnet Mask 255.255.255.0

Gateway 192.168.163.1

DNS 8.8.8.8

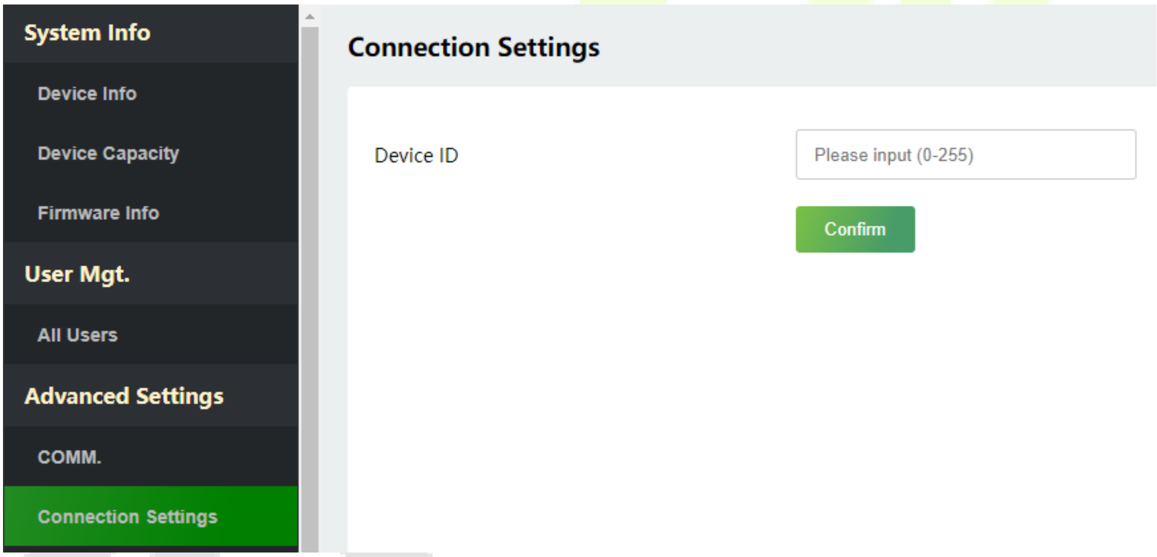
Function Name	Description
DHCP	Select whether to obtain the IP Address by automatically.
IP Address	The default IP address is 192.168.1.201. It can be modified according to network availability.

Subnet Mask	The default Subnet Mask is 255.255.255.0. It can be modified according to network availability.
Gateway	The Default Gateway address is 0.0.0.0. It can be modified according to network availability.
DNS	The default DNS address is 0.0.0.0. It can be modified according to network availability.

Note: After the IP address of the device is changed successfully, you need to log out of the currently WebServer and log in again to the IP address you just changed to connect to the device. For WebServer login details, please refer to Login WebServer.

19.4.2 Connection Settings

Click **Connection Settings** on the WebServer.

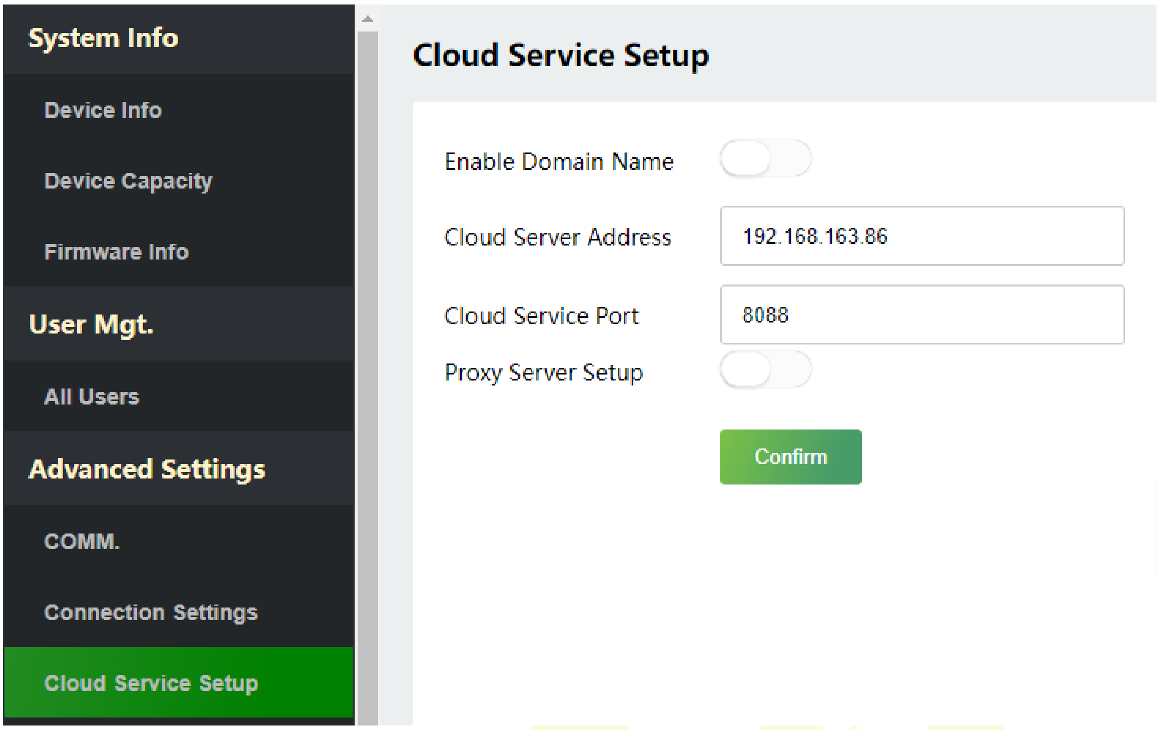


Function Name	Description
Device ID	It is the identification number of the device, which ranges between 0 and 255.

19.4.3 Cloud Service Setup

Click **Cloud Service Setup** on the WebServer.

Cloud Server Setup was used to connect to the ZKBio CVAccess and ZKBioTime 8.0 software, please refer to 12.1 Set the Communication Address.



Cloud Service Setup

Enable Domain Name

Cloud Server Address: 192.168.163.86

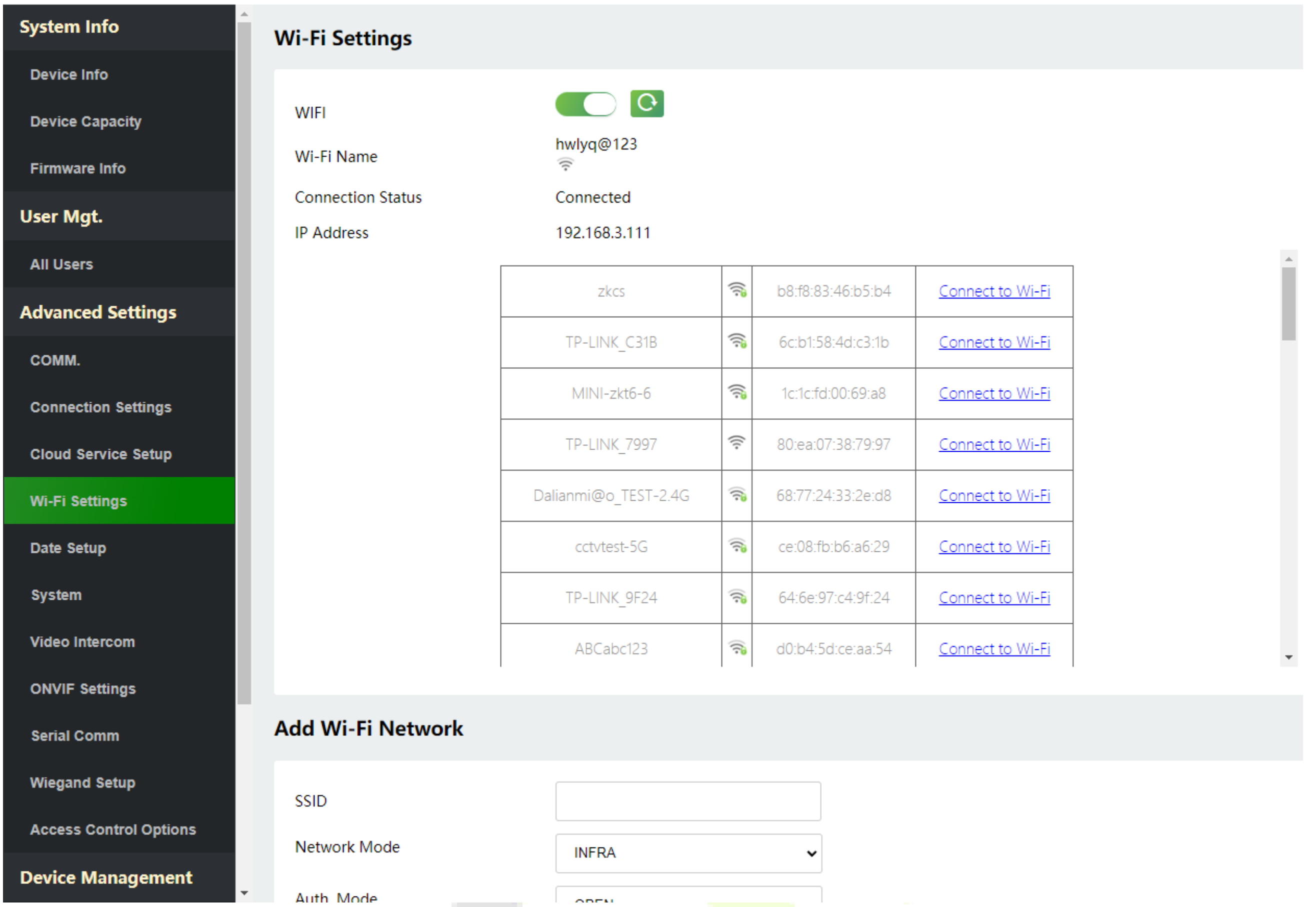
Cloud Service Port: 8088

Proxy Server Setup

Function Name		Description
Enable Domain Name	**Cloud Server Address**	Once 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	**Cloud Server Address**	IP address of the ADMS server.
	Cloud Server Port	Port used by the ADMS server.
Proxy Server Setup		When you choose to enable the proxy, you need to set the IP address and port number of the proxy server.

19.4.4 Wi-Fi Settings★

The device supports the Wi-Fi module, which is built-in within the hardware, to enable data transmission via Wi-Fi and establish a wireless network environment. By default, the Wi-Fi is turned off. The user needs to enable and set the related parameters on the WebServer.



Wi-Fi Settings

WIFI

Wi-Fi Name: hwlyq@123

Connection Status: Connected

IP Address: 192.168.3.111

zkcs	ᯤ	b8:f8:83:46:b5:b4	Connect to Wi-Fi
TP-LINK_C31B	ᯤ	6c:b1:58:4d:c3:1b	Connect to Wi-Fi
MINI-zkt6-6	ᯤ	1c:1c:fd:00:69:a8	Connect to Wi-Fi
TP-LINK_7997	ᯤ	80:ea:07:38:79:97	Connect to Wi-Fi
Dalianmi@o_TEST-2.4G	ᯤ	68:77:24:33:2e:d8	Connect to Wi-Fi
cctvtest-5G	ᯤ	ce:08:fb:b6:a6:29	Connect to Wi-Fi
TP-LINK_9F24	ᯤ	64:6e:97:c4:9f:24	Connect to Wi-Fi
ABCabc123	ᯤ	d0:b4:5d:ce:aa:54	Connect to Wi-Fi

Add Wi-Fi Network

SSID:

Network Mode: INFRA

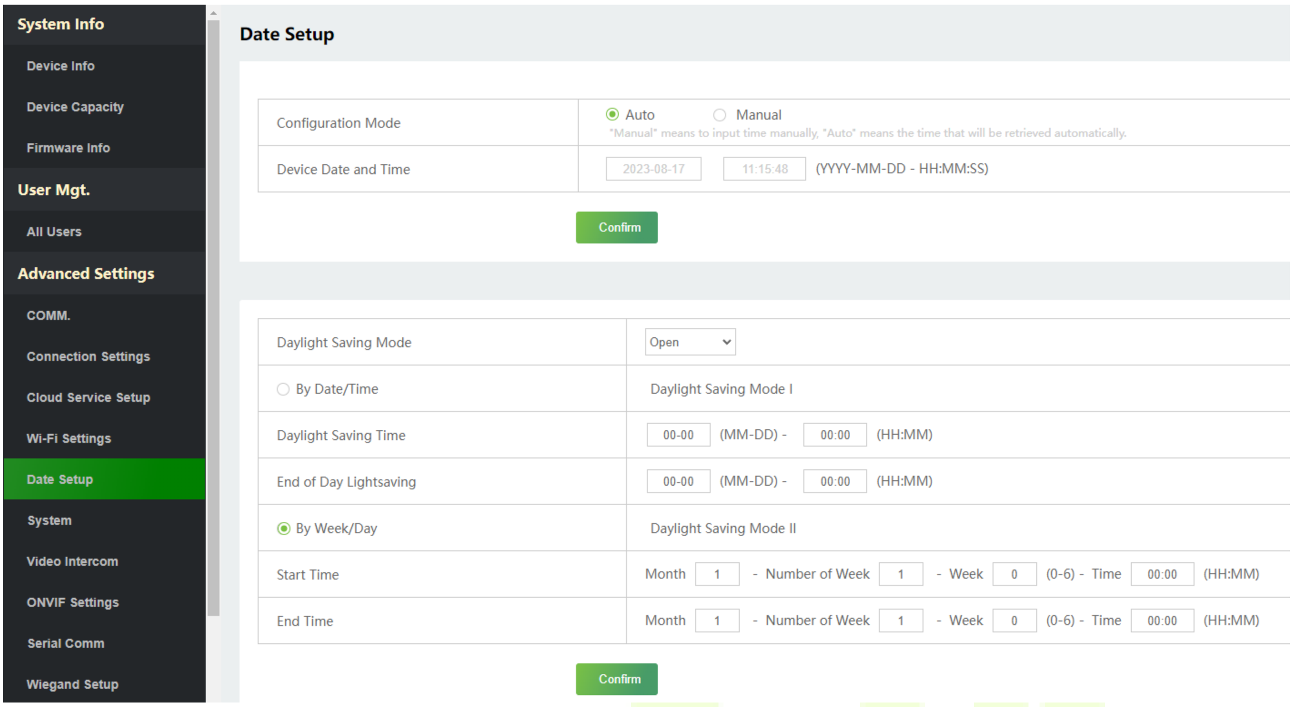
Auth. Mode: OPEN

- Click the button to enable Wi-Fi function.
- When Wi-Fi is enabled, the device will search for the available Wi-Fi within the network range.
- Click **Connect to Wi-Fi** after the required Wi-Fi name from the available list and input the correct password, and then click [**Confirm**].
- After successful verification, the connection status will display "**Connected**".

19.4.5 Date Setup

Click **Date Setup** on the WebServer.

- Click **Manual** to manually set the date and time and click **Confirm** to save.
- Select Open or Close the **Daylight Saving Mode** function. If opened, set the **Daylight Saving Time** and **End of Daylight Saving**.



Date Setup

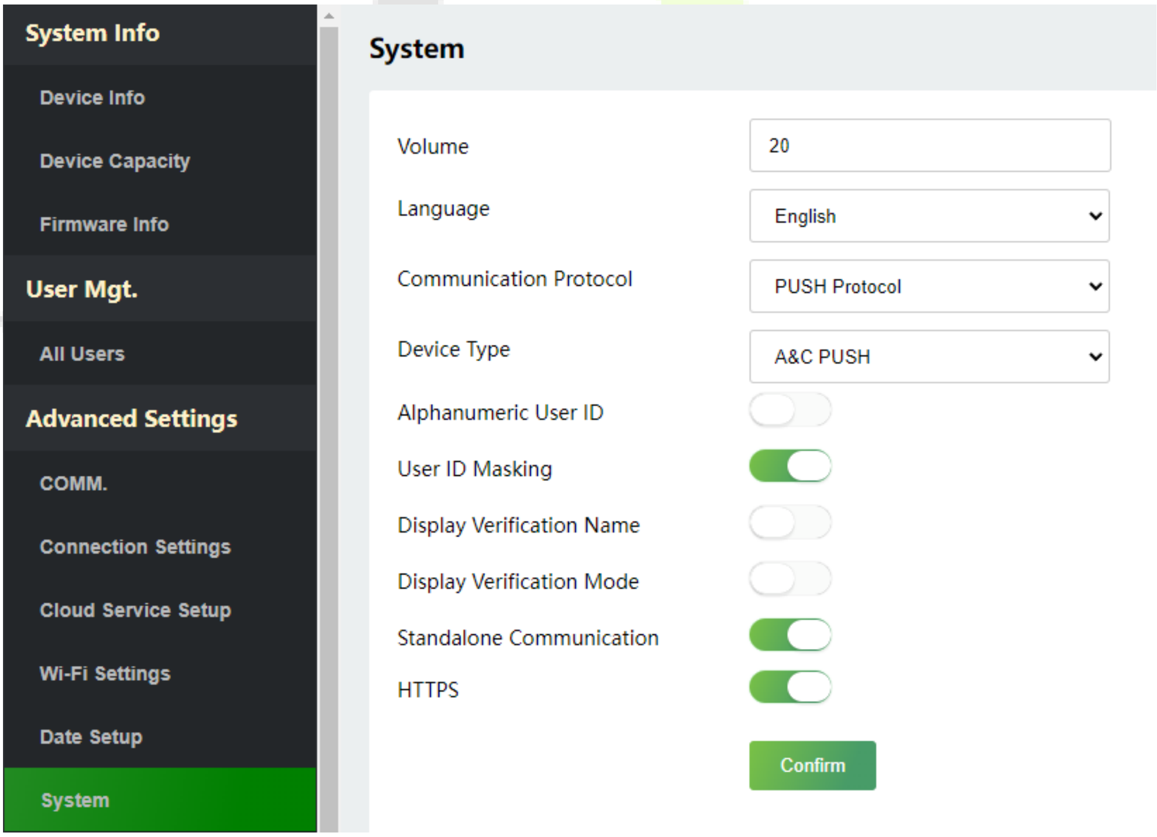
Configuration Mode	● Auto ○ Manual "Manual" means to input time manually, "Auto" means the time that will be retrieved automatically.
Device Date and Time	2023-08-17 11:15:48 (YYYY-MM-DD - HH:MM:SS)

Daylight Saving Mode	Open
○ By Date/Time	Daylight Saving Mode I
Daylight Saving Time	00-00 (MM-DD) - 00:00 (HH:MM)
End of Day Lightsaving	00-00 (MM-DD) - 00:00 (HH:MM)
● By Week/Day	Daylight Saving Mode II
Start Time	Month 1 - Number of Week 1 - Week 0 (0-6) - Time 00:00 (HH:MM)
End Time	Month 1 - Number of Week 1 - Week 0 (0-6) - Time 00:00 (HH:MM)

19.4.6 System Settings

Click **System** on the WebServer.

It helps to set related system parameters to optimize the accessibility of the device.



System

Volume	20
Language	English
Communication Protocol	PUSH Protocol
Device Type	A&C PUSH
Alphanumeric User ID	○
User ID Masking	●
Display Verification Name	○
Display Verification Mode	○
Standalone Communication	●
HTTPS	●

Function Name	Description
Volume	Adjust the volume of the device which can be set between 0 and 100.
Language	Select the language of the WebServer and device.
Communication Protocol	Set the communication protocol of the device.
Device Type	Set the device as an access control terminal or attendance terminal. ***Note:*** After changing the device type, the device will delete all the data and restart, and some functions will be adjusted accordingly.
Alphanumeric User ID	Enable/Disable the alphanumeric as User ID.
User ID Masking	When enabled, and then the user is successfully compared and verified, the User ID in the displayed verification result will be replaced with an * to achieve secure protection of sensitive private data.
Display Verification Name	Set whether to display the username in the verification result interface.
Display Verification Mode	Set whether to display the verification mode in the verification result interface.
Standalone Communication	To avoid being unable to use when the device is offline, you can download the C/S software (such as ZKAccess 3.5) on your computer in advance for offline use.
HTTPS	Based on HTTP, transmission encryption and identity authentication ensure the security of the transmission process.

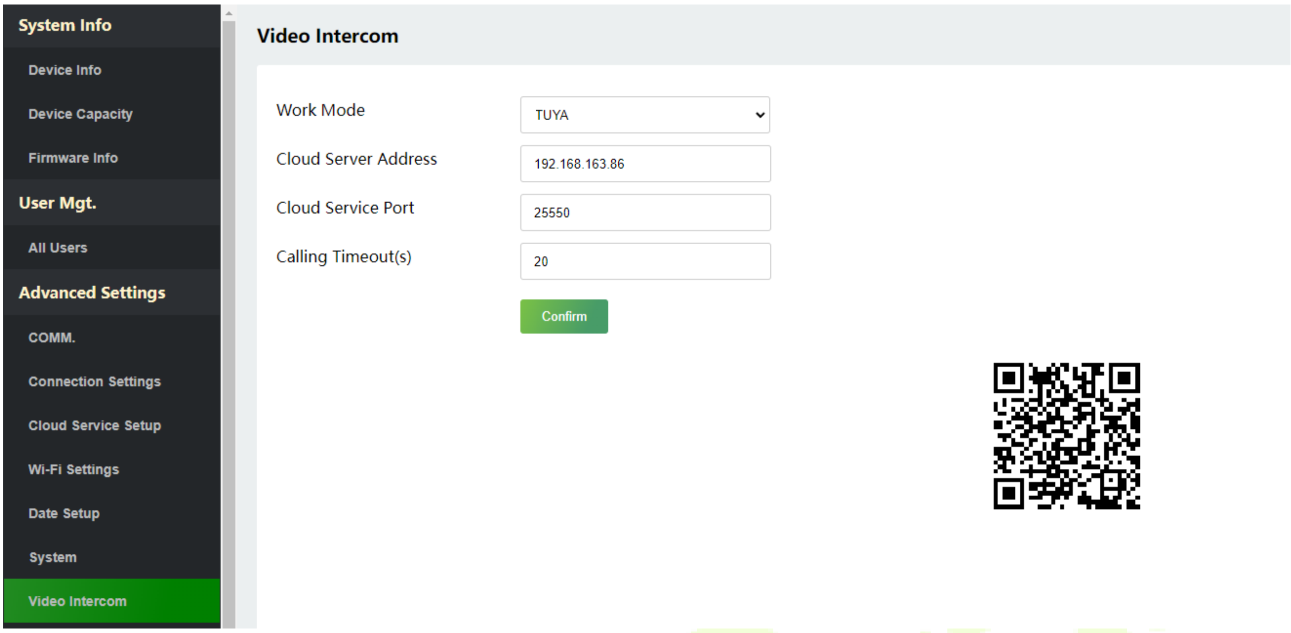
Note:

1. After selecting the language and clicking **Confirm**, the device will automatically reboot and display the changed language.
2. Then WebServer will not display the switched language until the device reboots and log in again.

19.4.7 Video Intercom★

Click **Video Intercom** on the WebServer.

The video intercom function supports WAN, WAN is suitable for mobile phone.



Video Intercom

Work Mode: TUYA

Cloud Server Address: 192.168.163.86

Cloud Service Port: 25550

Calling Timeout(s): 20

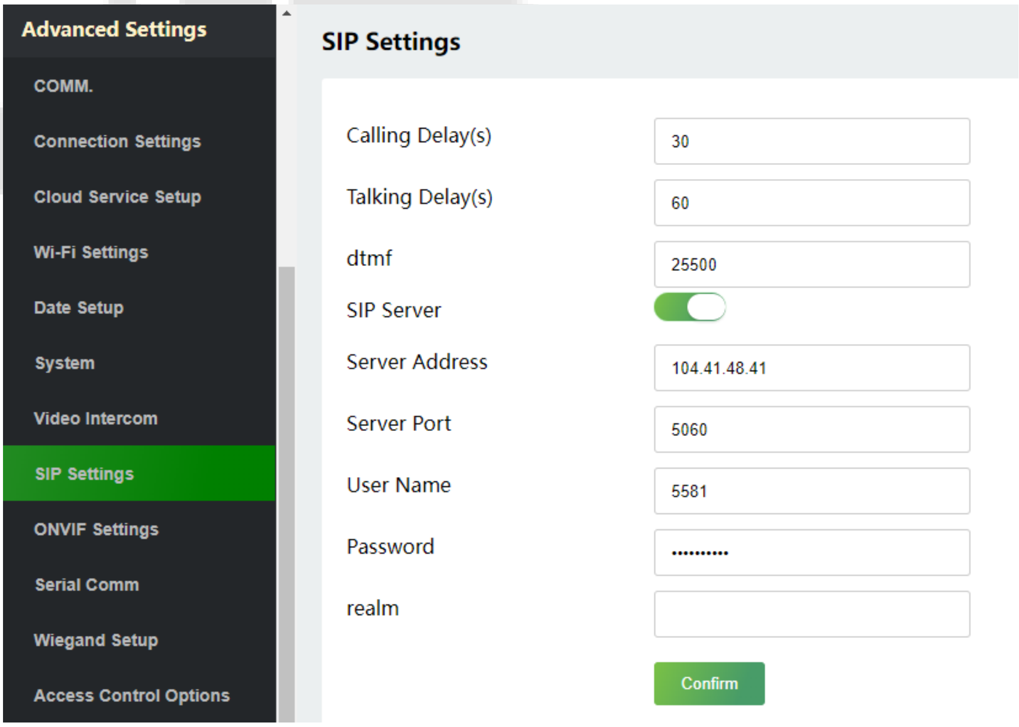
For more details, please refer to 22. Connecting to ZSmart App.

19.4.8 SIP Settings★

Note: This function needs to be used with the indoor station.

Click **SIP Settings** on the WebServer.

- **SIP Settings**



SIP Settings

Calling Delay(s): 30

Talking Delay(s): 60

dtmf: 25500

SIP Server: ●

Server Address: 104.41.48.41

Server Port: 5060

User Name: 5581

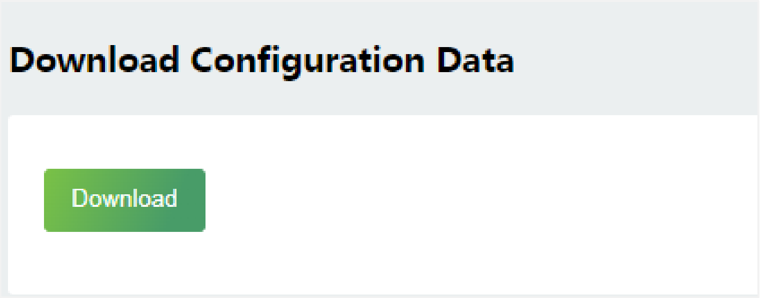
Password: ••••••••••

realm:

Function Name	Description
Calling Delay(s)	Set the time of call, valid value 30 to 60 seconds.
Talking Delay(s)	Set the time of intercom, valid value 60 to 120 seconds.
dtmf	The value should be set as same as the value of DTMF in the indoor station.
SIP Server	Select whether to enable the SIP server. (**Note:** Each time it is switched ON/OFF, the device will restart to take effect.)
Server Address	Enter the server address.
Server Port	Enter the server port.
User Name	Enter the username of server.
Password	Enter the password of server.
Realm	Enter the realm of server.

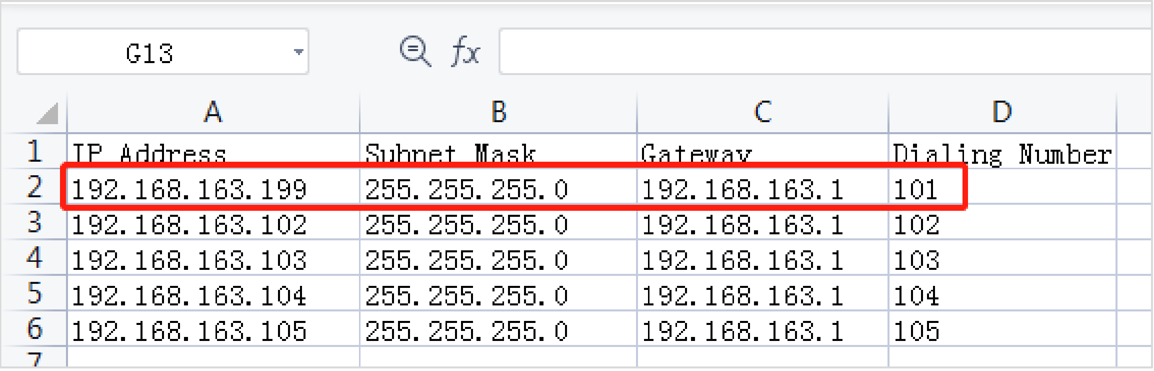
- **Download Configuration Data**

1. Click **Download** to download the file.


Download Configuration Data

2. Open the downloaded file and manually modify the indoor station's communication address and device number.

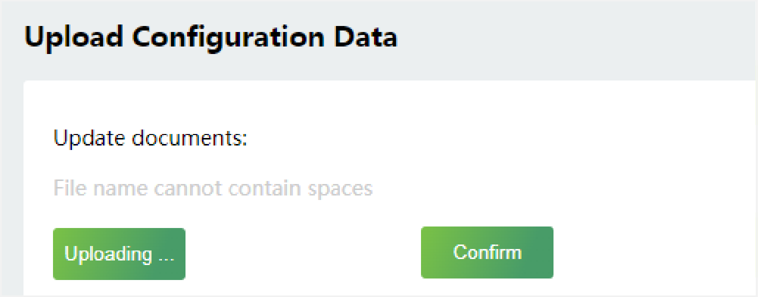
   IP Address/Subnet Mask/Gateway: Must be the same as the indoor station to be connected.
   Dialling Number: Customize the number of the indoor station, you can enter the value on F35 to call the indoor station quickly for video intercom.



	A	B	C	D
1	IP Address	Subnet Mask	Gateway	Dialing Number
2	192.168.163.199	255.255.255.0	192.168.163.1	101
3	192.168.163.102	255.255.255.0	192.168.163.1	102
4	192.168.163.103	255.255.255.0	192.168.163.1	103
5	192.168.163.104	255.255.255.0	192.168.163.1	104
6	192.168.163.105	255.255.255.0	192.168.163.1	105
7				

- **Upload Configuration Data**

1. Once the form is set up and saved, click **Uploading...** to upload the configuration form.



Upload Configuration Data

Update documents:

File name cannot contain spaces

Uploading ... Confirm

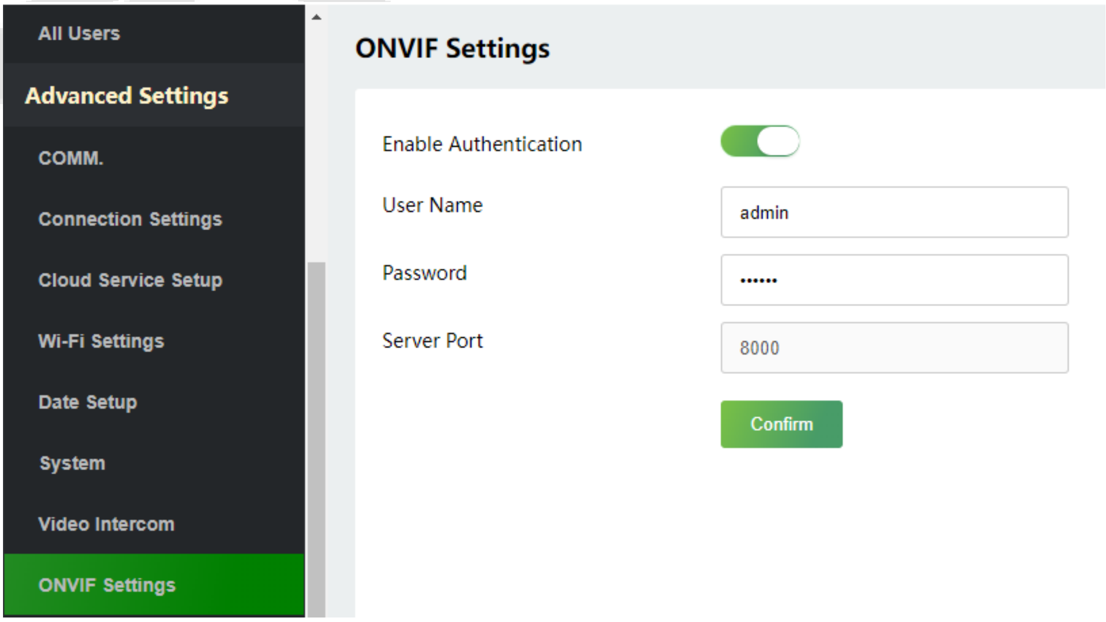
2. Click **Confirm** to sync the parameters to F35.

For more details, please refer to 23. Connecting to SIP.

19.4.9 ONVIF Settings★

Note: This function needs to be used with the network video recorder (NVR).

Click **ONVIF Settings** on the WebServer.



ONVIF Settings

Enable Authentication: on

User Name: admin

Password: ••••••

Server Port: 8000

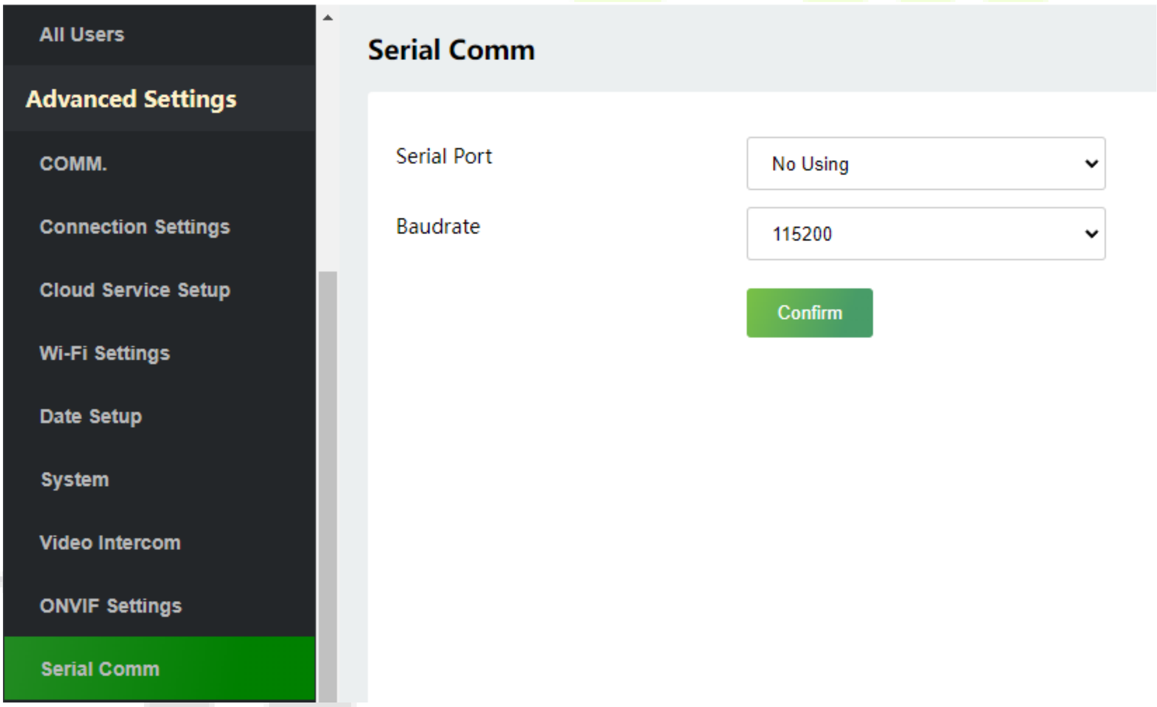
Confirm

Function Name	Description
Enable Authentication	Enable/Disable the Authentication Function. When it is disabled, there is no need to input the User Name and Password when adding the device to the NVR.
User Name	Set the User Name. The default is admin.
Password	Set the password.
Server Port	The default is 8000, and cannot be modified.

For more details, please refer to 11.5 ONVIF Settings.

19.4.10 Serial Comm

Click **Serial Comm** on the WebServer.



Serial Comm

Serial Port: No Using

Baudrate: 115200

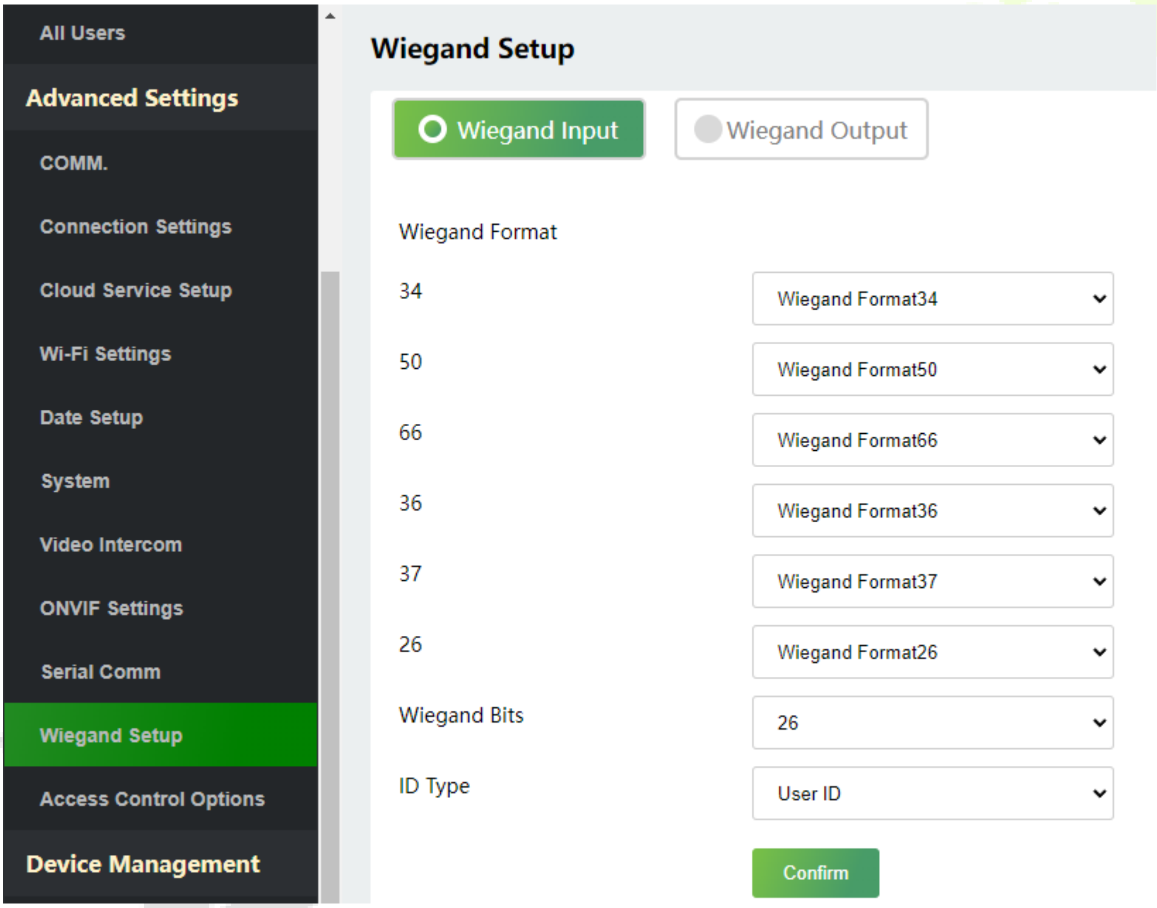
Function Name	Description
Serial Port	**No Using:** No communication with the device through the serial port. **Master Unit:** When RS485 is used as the function of "**Master Unit**", it can be connected to a reader. **Print Function:** The device can be connected to the printer when RS232 enables the print function.

Baudrate	There are 4 baudrate options at which the data communicates with PC. They are: 115200 (default), 57600, 38400, and 19200. The higher the baudrate, the faster is the communication speed, but also less reliable. Hence, a higher baudrate can be used when the communication distance is short; when the communication distance is long, choosing a lower baudrate is more reliable.

19.4.11 Wiegand Setup

Click **Wiegand Setup** on the WebServer.

It is used to set the Wiegand input and output parameters.



Wiegand Setup

● Wiegand Input ○ Wiegand Output

Wiegand Format

34	Wiegand Format34
50	Wiegand Format50
66	Wiegand Format66
36	Wiegand Format36
37	Wiegand Format37
26	Wiegand Format26
Wiegand Bits	26
ID Type	User ID

Confirm

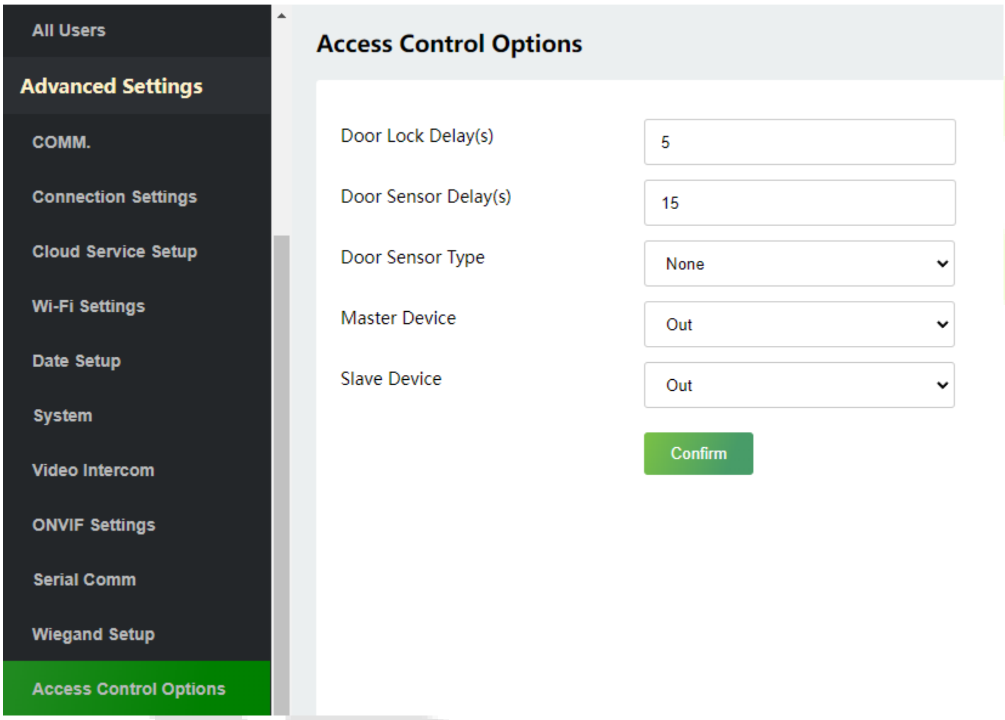
Function Name	Description
Wiegand Format	Its value can be 26 bits, 34 bits, 36 bits, 37 bits, 50 bits and 60 bits.
Wiegand Bits	The number of bits of the Wiegand data.
ID Type	Select between the User ID and card number.

19.4.12 Access Control Options

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

On the Access Control interface to set the parameters of the control lock of the terminal and related equipment.

Access Control Terminal:



Access Control Options

Door Lock Delay(s): 5

Door Sensor Delay(s): 15

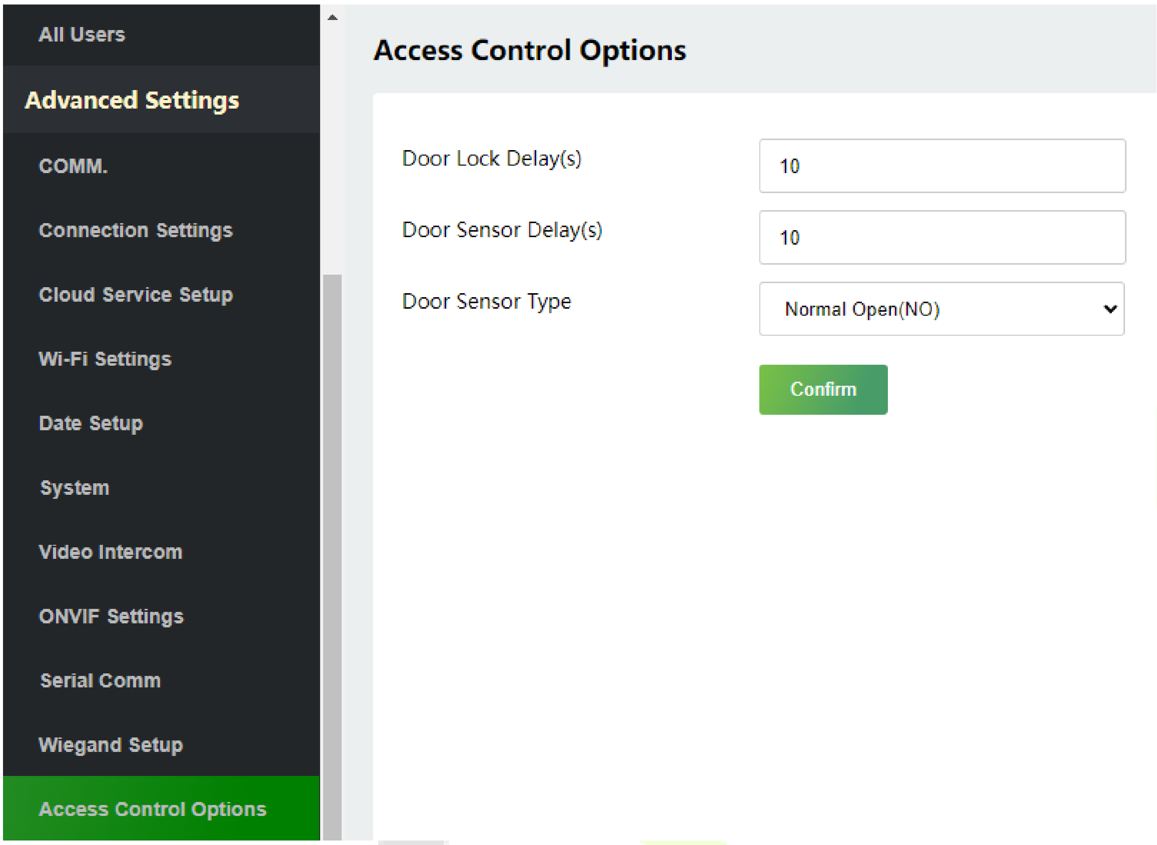
Door Sensor Type: None

Master Device: Out

Slave Device: Out

Function Name	Description
Door Lock Delay(s)	The length of time that the device controls the electric lock to be in unlock state. Valid value: 1~99 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.
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.

Attendance Terminal:



Access Control Options

Door Lock Delay(s): 10

Door Sensor Delay(s): 10

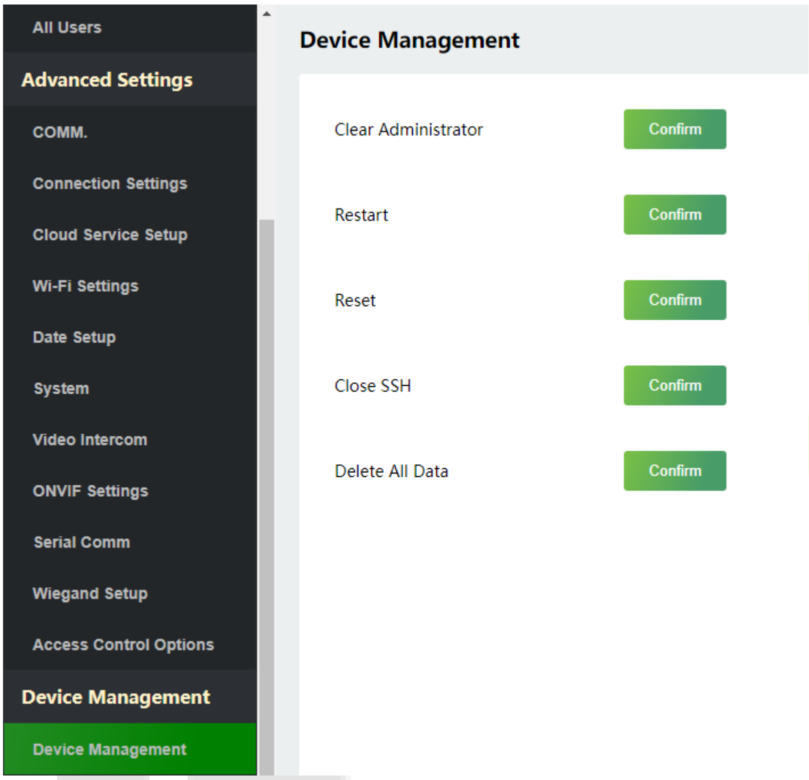
Door Sensor Type: Normal Open(NO)

Function Name	Description
Door Lock Delay(s)	The length of time that the device controls the electric lock to be in unlock state. Valid value: 1~255 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.

19.5 Device Management

19.5.1 Device Management

Click **Device Management** on the WebServer.



Device Management

Clear Administrator Confirm

Restart Confirm

Reset Confirm

Close SSH Confirm

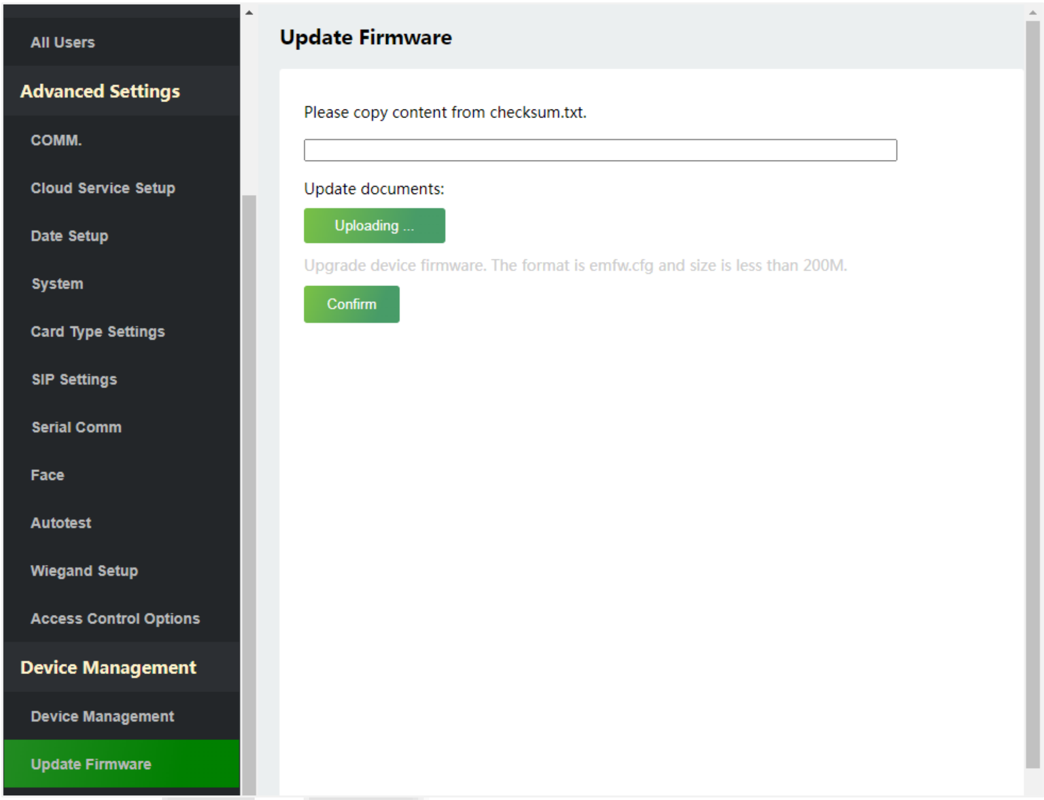
Delete All Data Confirm

Function Name	Description
Clear Administrator	Choose whether to change the super administrator into a normal user.
Restart	Choose whether to restart the device.
Reset	The Reset function restores the device settings such as communication and system settings to the default factory settings (this function does not clear registered user data). ***Note:*** After reset, the IP of the device is restored to the original 192.168.1.201, please refer to 19.4.1 Communication Settings to modify the IP.
Close SSH	SSH is used to enter the background of the device for maintenance, choose whether to close the SSH.
Delete All Data	To delete the information and attendance logs/access records of all registered users.

19.5.2 Updata Firmware

Click **Updata Firmware** on the WebServer.

Select an upgrade file and click **Confirm** to complete firmware upgrade operation.



Update Firmware

Please copy content from checksum.txt.

Update documents:

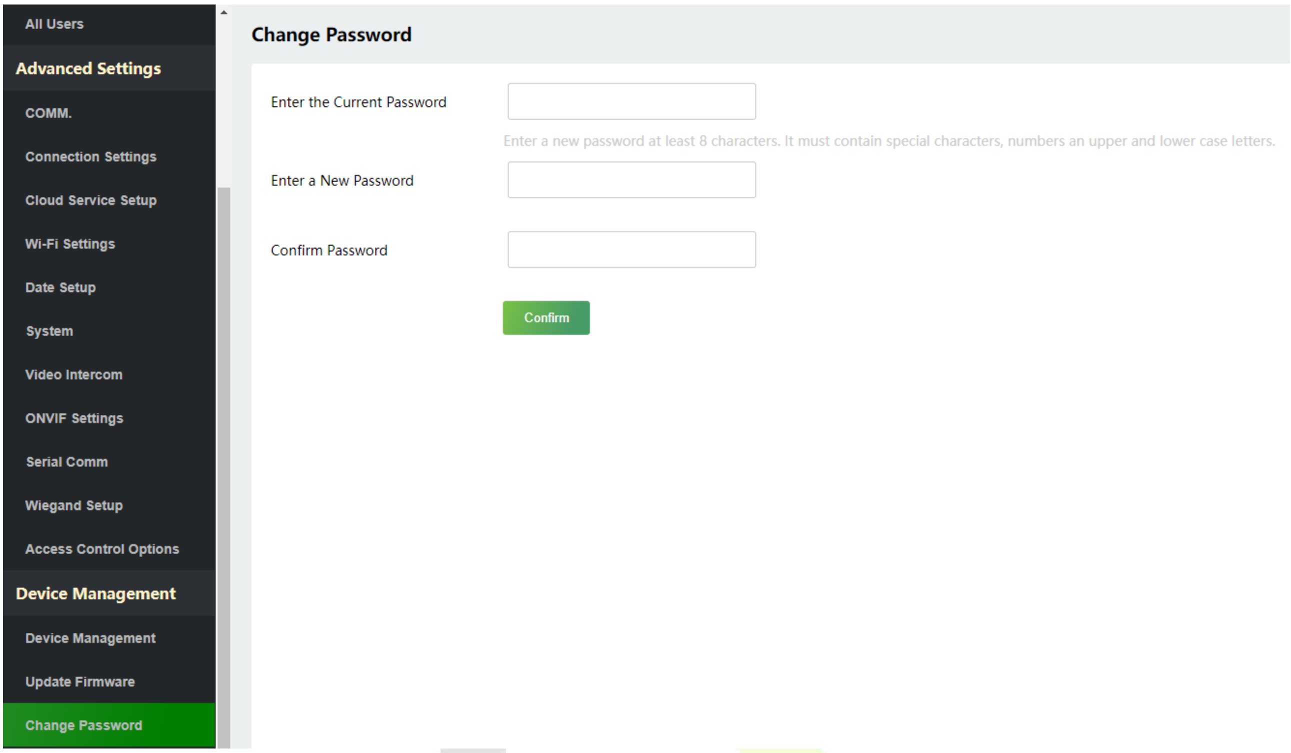
Upgrade device firmware. The format is emfw.cfg and size is less than 200M.

Note: If the upgrade file is needed, please contact our technical support. Firmware upgrade is not recommenced under normal circumstances.

19.5.3 Change Password

Click **Change Password** on the WebServer.

In this interface, you can change the password of WebServer.



Change Password

Enter the Current Password

Enter a new password at least 8 characters. It must contain special characters, numbers an upper and lower case letters.

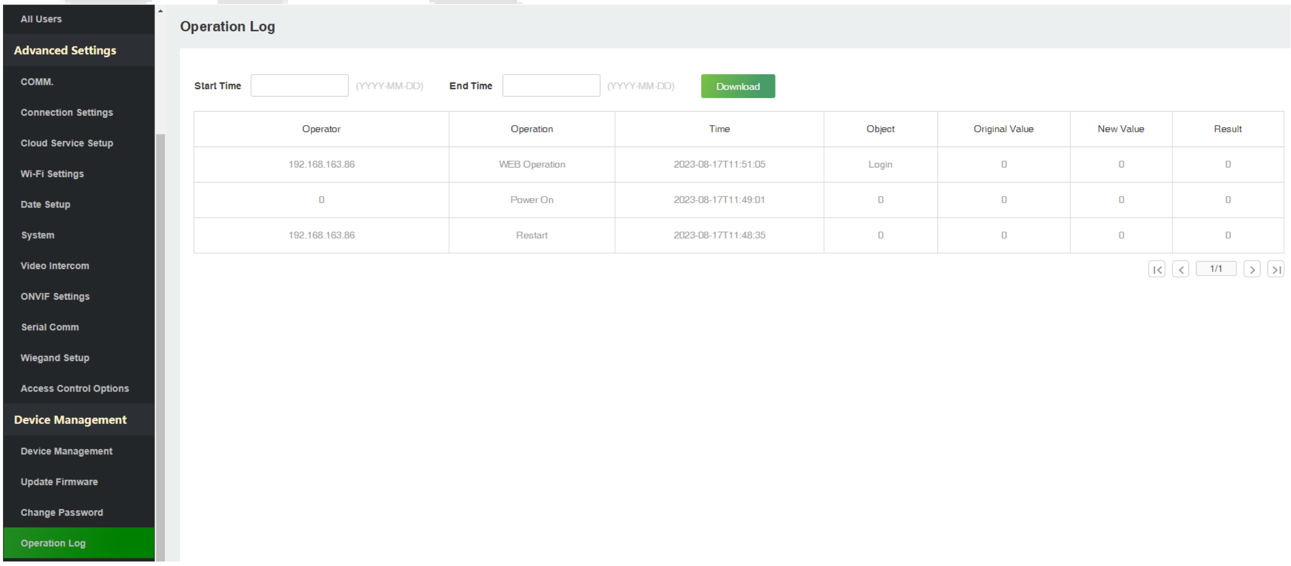
Enter a New Password

Confirm Password

19.5.4 Operation Log

Click **Operation Log** on the WebServer.

All the user's operation records on the device or WebServer are saved. Users can search and download these logs by time.



Operation Log

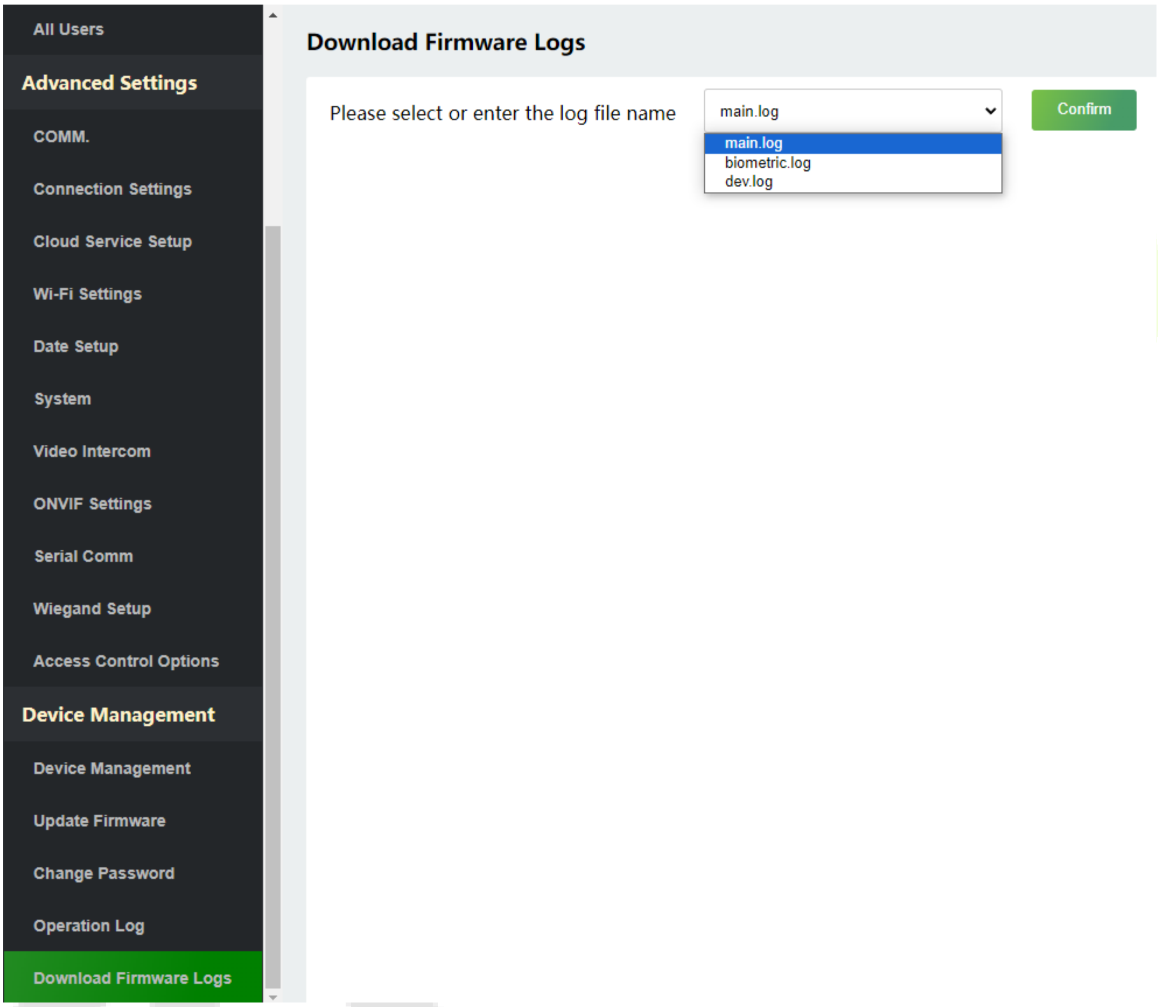
Start Time (YYYY-MM-DD) End Time (YYYY-MM-DD)

Operator	Operation	Time	Object	Original Value	New Value	Result
192.168.163.86	WEB Operation	2023-08-17T11:51:05	Login	0	0	0
0	Power On	2023-08-17T11:49:01	0	0	0	0
192.168.163.86	Restart	2023-08-17T11:48:35	0	0	0	0

19.5.5 Download Firmware Logs

Click **Download Firmware Logs** on the WebServer.

In this interface, you can select download the main, biometric, or dev.log.

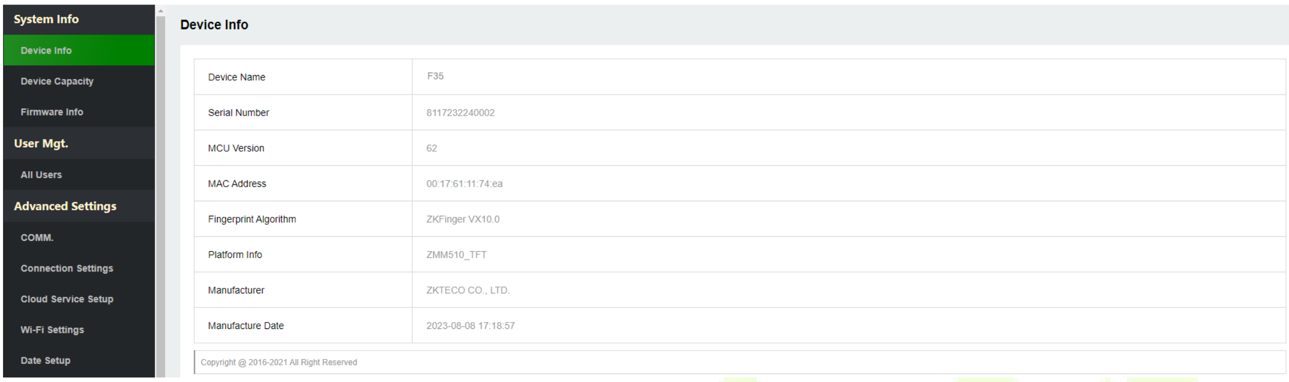


Please select or enter the log file name: main.log

19.6 System Information

Click **System Information** on the WebServer.

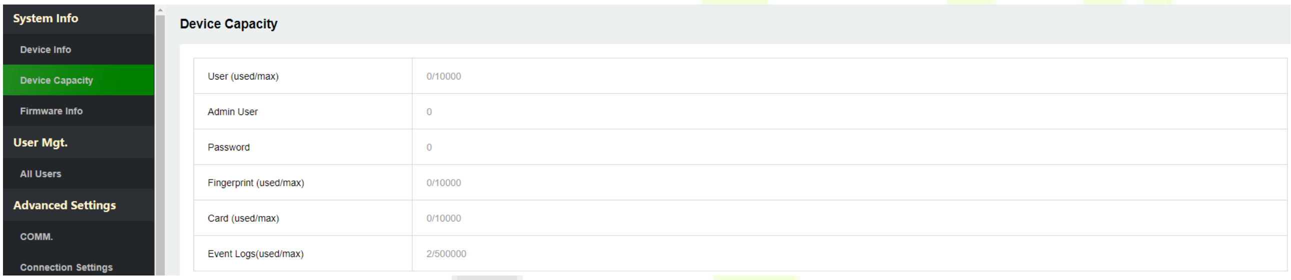
In this interface, you can view the data capacity, device and firmware information of the current device.



Device Info

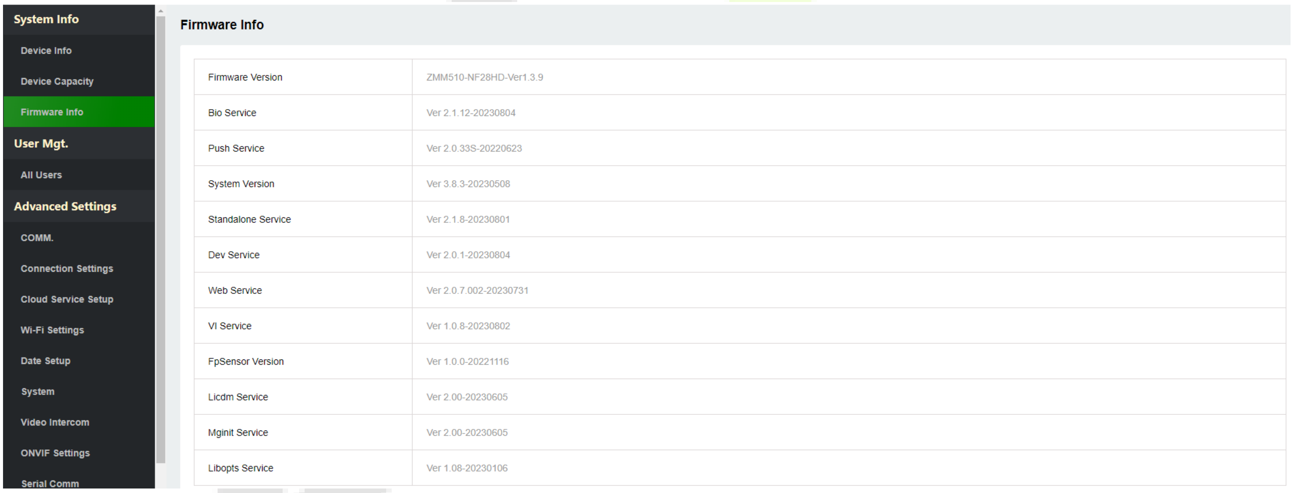
Device Name	F35
Serial Number	8117232240002
MCU Version	62
MAC Address	00:17:61:11:74:ea
Fingerprint Algorithm	ZKFinger VX10.0
Platform Info	ZMM510_TFT
Manufacturer	ZKTECO CO., LTD.
Manufacture Date	2023-08-08 17:18:57

Copyright @ 2016-2021 All Right Reserved



Device Capacity

User (used/max)	0/10000
Admin User	0
Password	0
Fingerprint (used/max)	0/10000
Card (used/max)	0/10000
Event Logs(used/max)	2/500000



Firmware Info

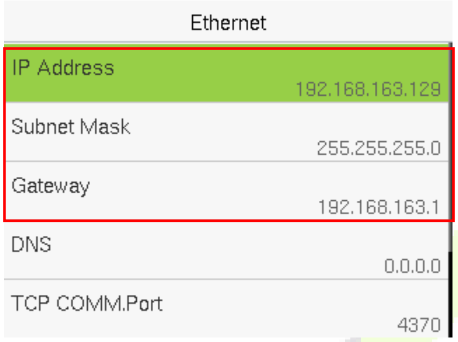
Firmware Version	ZMM510-NF28HD-Ver1.3.9
Bio Service	Ver 2.1.12-20230804
Push Service	Ver 2.0.33S-20220623
System Version	Ver 3.8.3-20230508
Standalone Service	Ver 2.1.8-20230801
Dev Service	Ver 2.0.1-20230804
Web Service	Ver 2.0.7.002-20230731
VI Service	Ver 1.0.8-20230802
FpSensor Version	Ver 1.0.0-20221116
Licdm Service	Ver 2.00-20230605
Mginit Service	Ver 2.00-20230605
Libopts Service	Ver 1.08-20230106

Function Name	Description
Device Info	Displays the device's name, serial number, MCU version, MAC address, fingerprint algorithm version information, platform and manufacturer information.
Device Capacity	Displays the current device's user storage, password, fingerprint, card storage, administrators, and event logs.
Firmware Information	Displays the firmware version and other version information of the device.

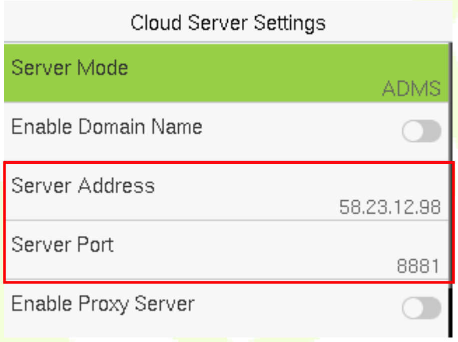
20 Connect to ZKBio CVAccess Software

20.1 Set the Communication Address

1. Tap **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 ZKBio CVAccess server)
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 ZKBio CVAccess server.
   Server port: Set the server port as of ZKBio CVAccess.


Ethernet

IP Address: 192.168.163.129
Subnet Mask: 255.255.255.0
Gateway: 192.168.163.1
DNS: 0.0.0.0
TCP COMM.Port: 4370

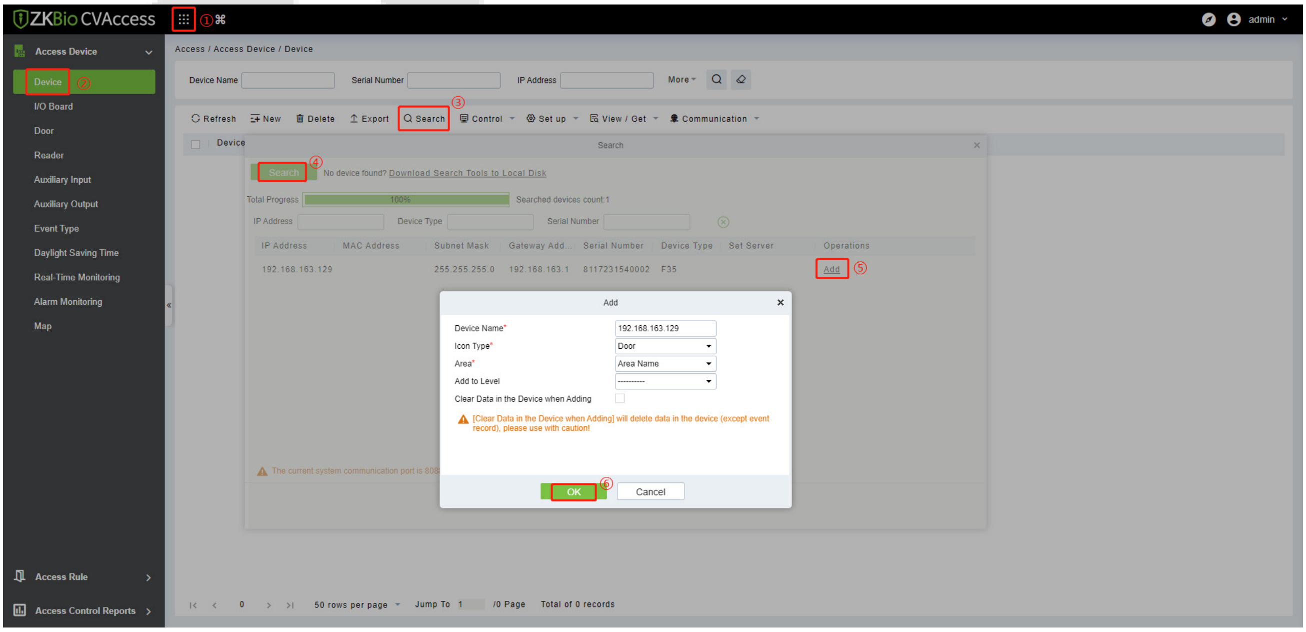

Cloud Server Settings

Server Mode: ADMS
Enable Domain Name: ○
Server Address: 58.23.12.98
Server Port: 8881
Enable Proxy Server: ○

20.2 Add Device on the Software

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

1. Click **Access** > **Device** > **Search** > **Search**, 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.



No device found? Download Search Tools to Local Disk

Total Progress 100% Searched devices count:1

IP Address	MAC Address	Subnet Mask	Gateway Add...	Serial Number	Device Type	Set Server	Operations
192.168.163.129		255.255.255.0	192.168.163.1	8117231540002	F35		Add

The current system communication port is 808

Add

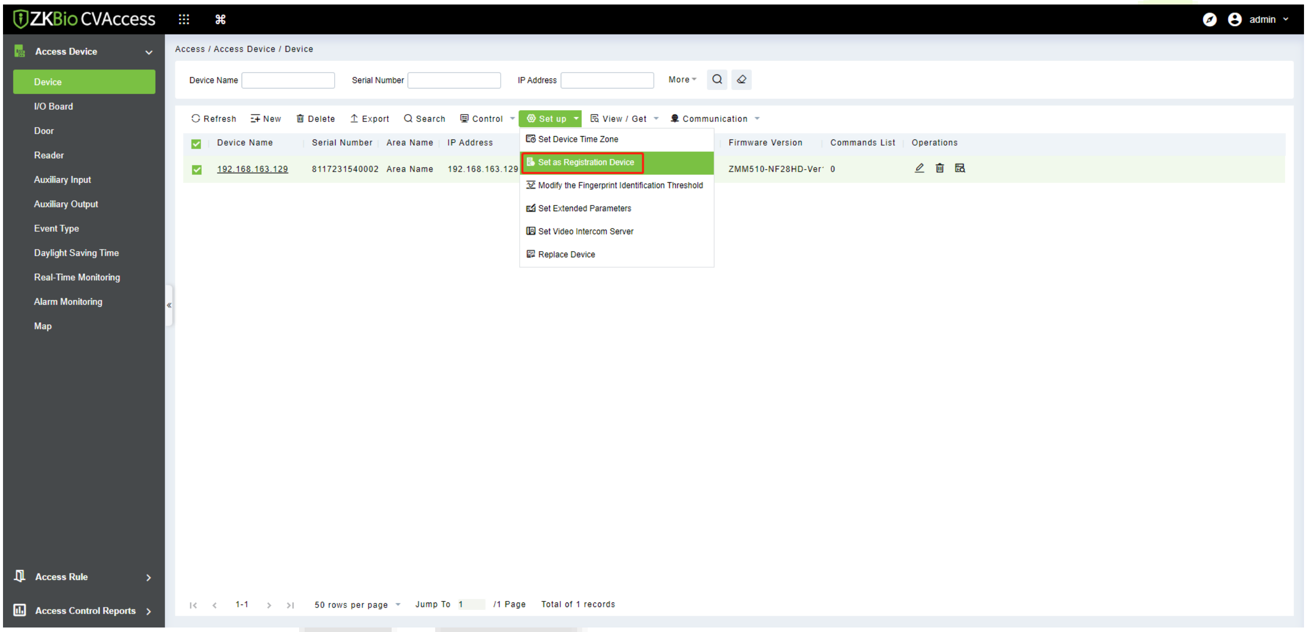
Device Name*: 192.168.163.129
Icon Type*: Door
Area*: Area Name
Add to Level: ----------
Clear Data in the Device when Adding: □

[Clear Data in the Device when Adding] will delete data in the device (except event record), please use with caution!

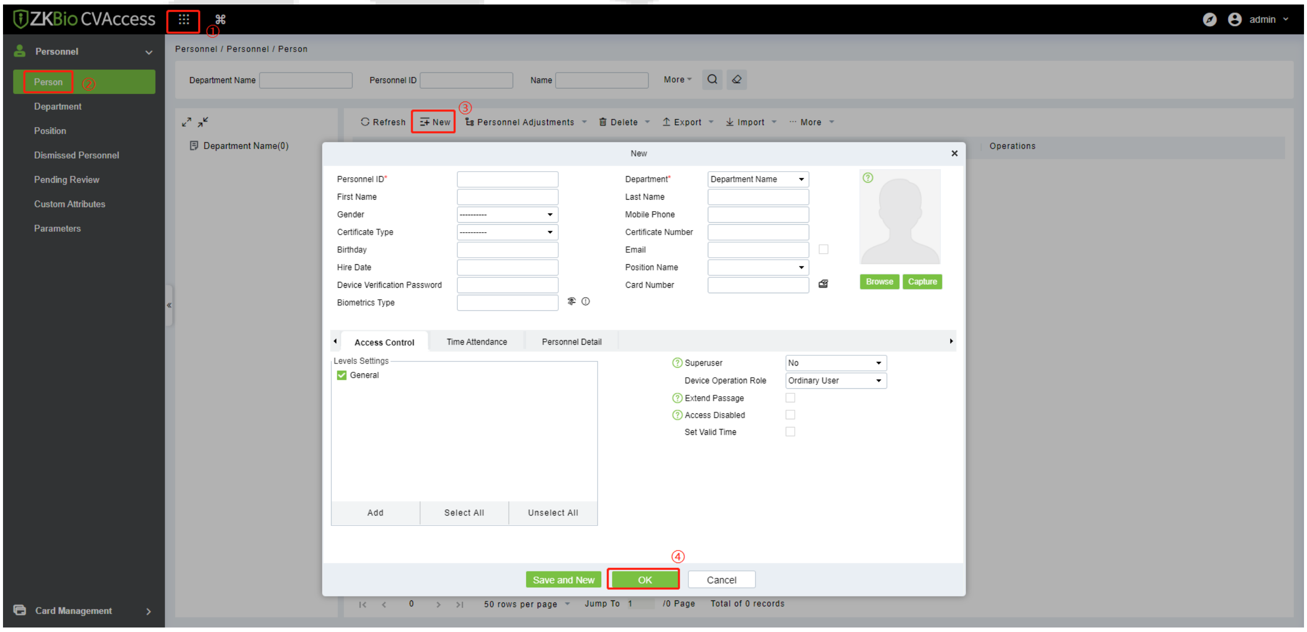
4. Click [**Add**] in operation column, a new window will pop-up. Select Icon type, Area, and Add to Level from each dropdown and click [**OK**] to add the device.
5. After the addition is successful, the device will be displayed in the device list.

20.3 Add Personnel on the Software and Online Fingerprint Registration

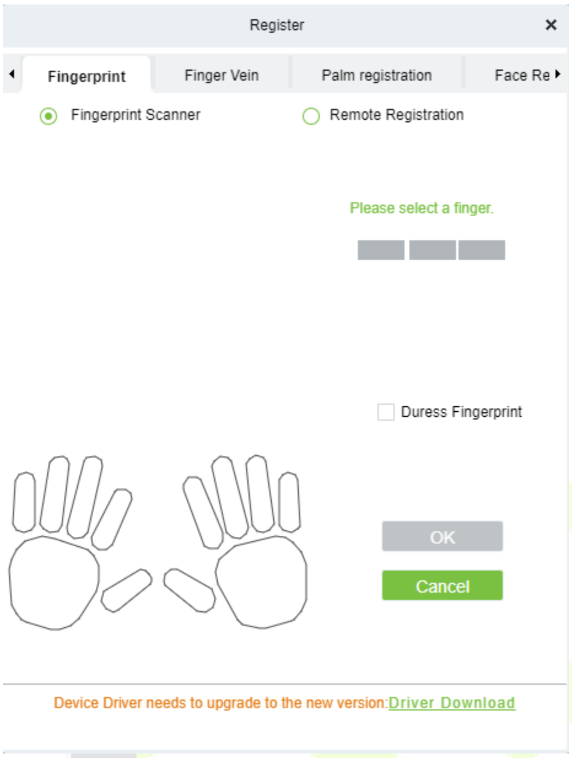
1. In the device list, select the device and click **Set up > Set as Registration Device.**



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



3. Fill in all the required fields of the user and click to enter the online fingerprint registration interface.



Register

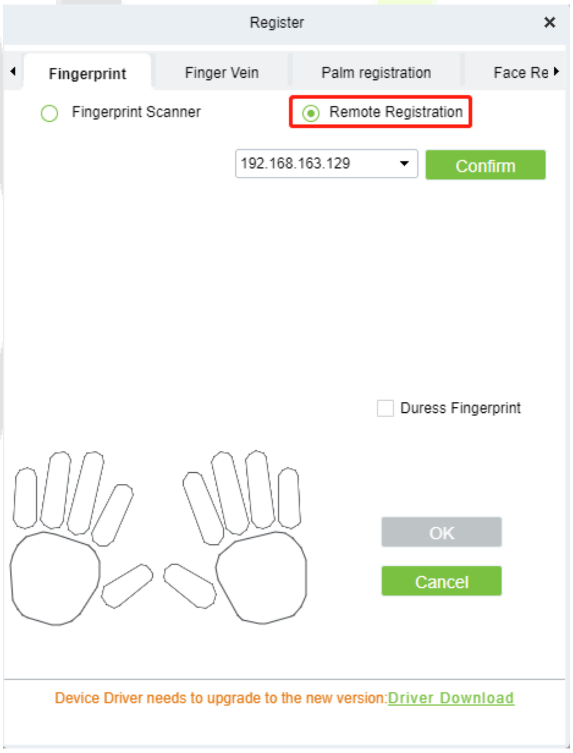
● Fingerprint Scanner ○ Remote Registration

Please select a finger.

□ Duress Fingerprint

Device Driver needs to upgrade to the new version:Driver Download

4. Click **Driver Download** to install the driver first.
5. Select **Remote Registration**, then select the IP address of the device and click **Confirm**.



Register

○ Fingerprint Scanner ● Remote Registration

192.168.163.129 Confirm

□ Duress Fingerprint

Device Driver needs to upgrade to the new version:Driver Download

6. Select the finger you want to register and press your finger on the fingerprint sensor of the device three times. If the fingerprint is successfully registered, the device will prompt "Enrolled successfully".

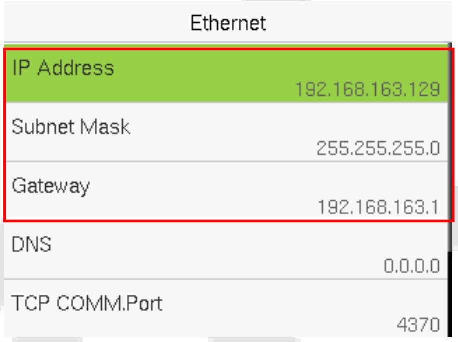
7. If you want to register a duress fingerprint, you can click **Duress Fingerprint** before registering the fingerprint.
   - **Duress fingerprint:** In any case, a duress alarm is generated when a fingerprint matches a duress fingerprint.
8. Click **OK** to save the user.
9. Click **Access** > **Device** > **Control** > **Synchronize All Data to Devices** to synchronize all the data to the device including the new users.

Note: For other specific operations, please refer the *ZKBio CVAccess User Manual*.

21 Connect to ZKBioTime 8.0 Software

21.1 Set the Communication Address

1. Tap **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 ZKBioTime 8.0 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 ZKBioTime 8.0 server.
   Server port: Set the server port as of ZKBioTime 8.0 server.


Ethernet

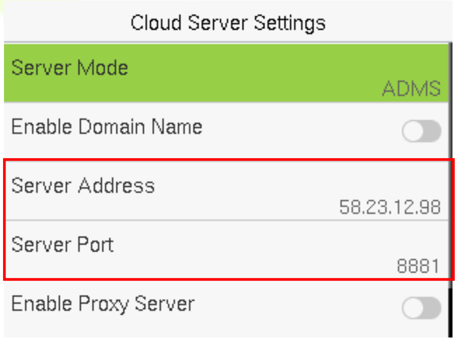
IP Address: 192.168.163.129

Subnet Mask: 255.255.255.0

Gateway: 192.168.163.1

DNS: 0.0.0.0

TCP COMM.Port: 4370


Cloud Server Settings

Server Mode: ADMS

Enable Domain Name: ○

Server Address: 58.23.12.98

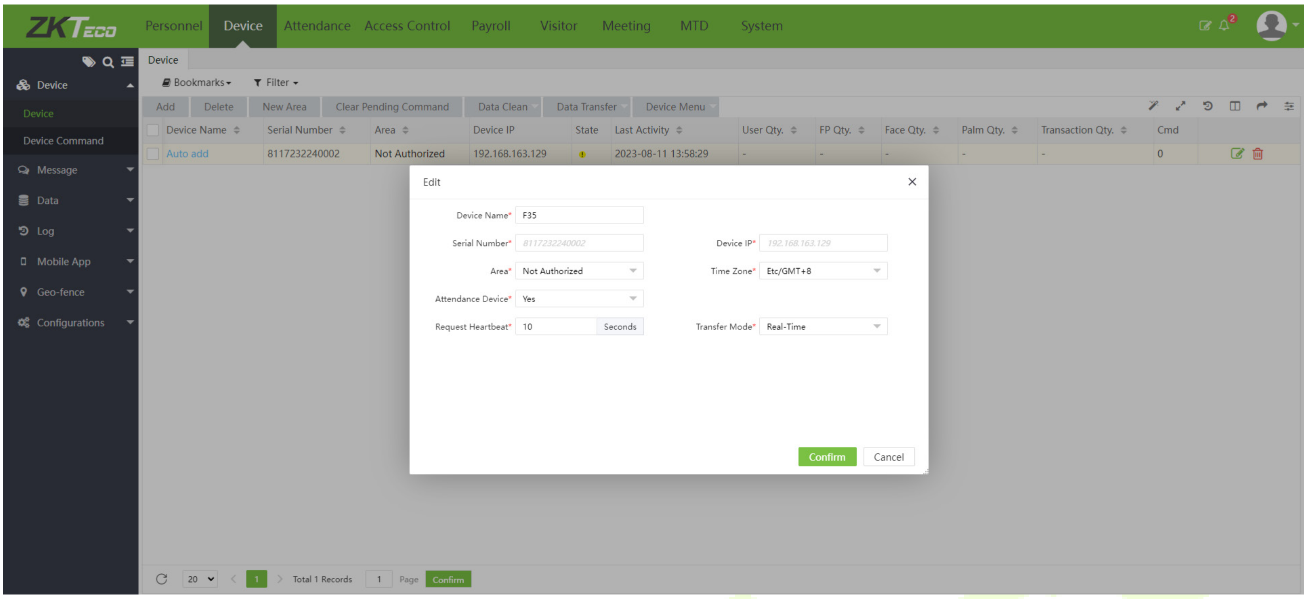
Server Port: 8881

Enable Proxy Server: ○

21.2 Add Device on the Software

After setting on the device, the device will be automatically added to the software. Open the ZKBioTime software then select [**Device Module**] > [**Device**] > [**Device**], click the device in the list, change the Device Name and Area.

Note: The devices added automatically must be assigned to custom areas to communicate with the software.



Device Name	Serial Number	Area	Device IP	State	Last Activity	User Qty.	FP Qty.	Face Qty.	Palm Qty.	Transaction Qty.	Cmd
Auto add	8117232240002	Not Authorized	192.168.163.129		2023-08-11 13:58:29	-	-	-	-	-	0

Edit

Device Name* F35

Serial Number* 8117232240002

Device IP* 192.168.163.129

Area* Not Authorized

Time Zone* Etc/GMT+8

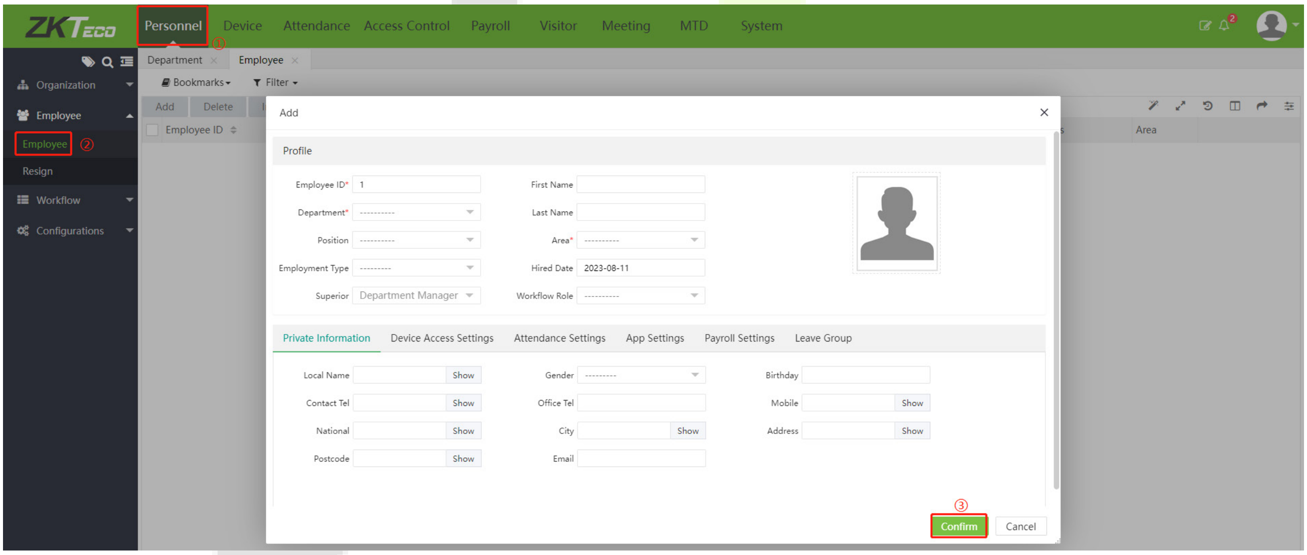
Attendance Device* Yes

Request Heartbeat* 10 Seconds

Transfer Mode* Real-Time

21.3 Add Personnel on the Software and Online Fingerprint Registration

1. Click **Personnel** > **Employee** > **Add**:



Add

Employee ID* 1

First Name

Department* ----------

Last Name

Position ----------

Area* ----------

Employment Type ----------

Hired Date 2023-08-11

Superior Department Manager

Workflow Role ----------

Local Name

Gender ---------

Birthday

Contact Tel

Office Tel

Mobile

National

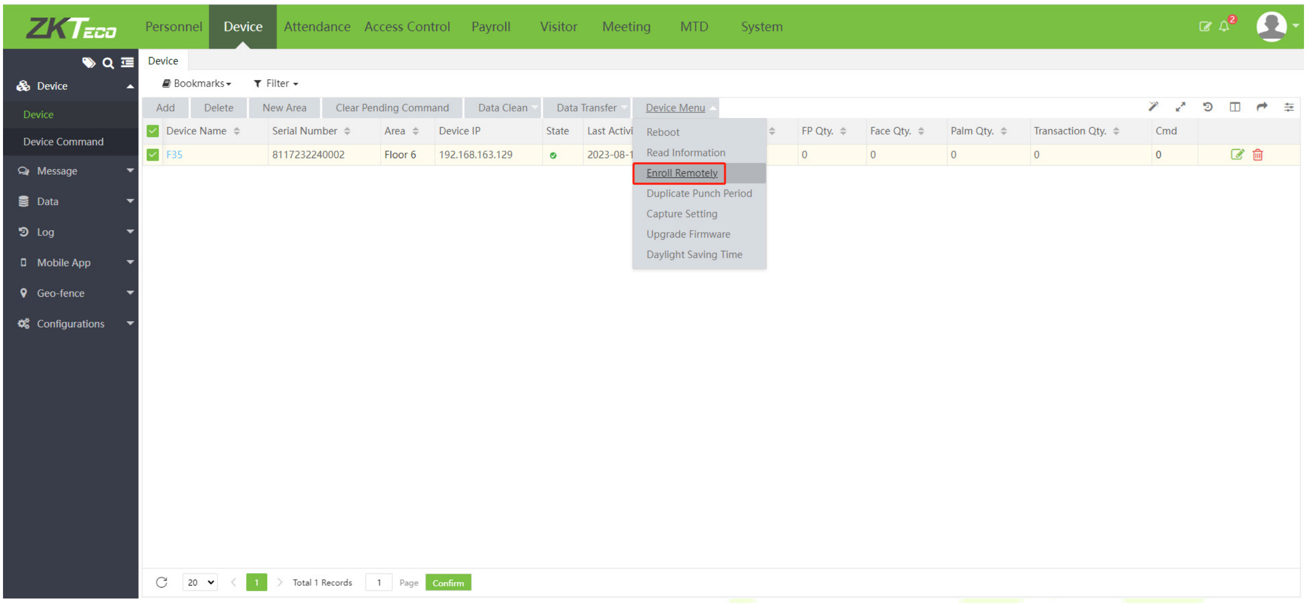
City

Address

Postcode

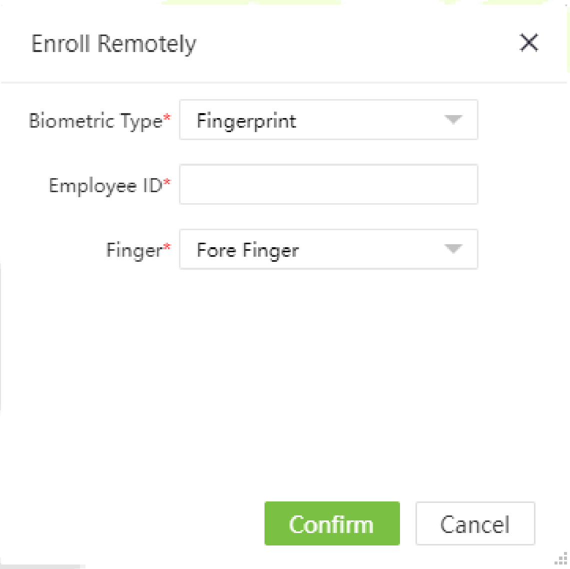
Email

2. Fill in all the required fields and click [**Confirm**] to register a new user.
3. Click **Device** > **Device**, select the device and click **Device Menu** > **Enroll Remotely**.



Device Name	Serial Number	Area	Device IP	State	Last Activi	FP Qty.	Face Qty.	Palm Qty.	Transaction Qty.	Cmd
F35	8117232240002	Floor 6	192.168.163.129	●	2023-08-1	0	0	0	0	0

4. Enter the Employee ID and select the finger you want to register and press your finger on the fingerprint sensor of the device three times. If the fingerprint is successfully registered, the device will prompt "Enrolled successfully".



Biometric Type*: Fingerprint

Employee ID*:

Finger*: Fore Finger

5. Click **Device** > **Device** > **Data Transfer** > **Sync Data to the Device** to synchronize all the data to the device including the new users.

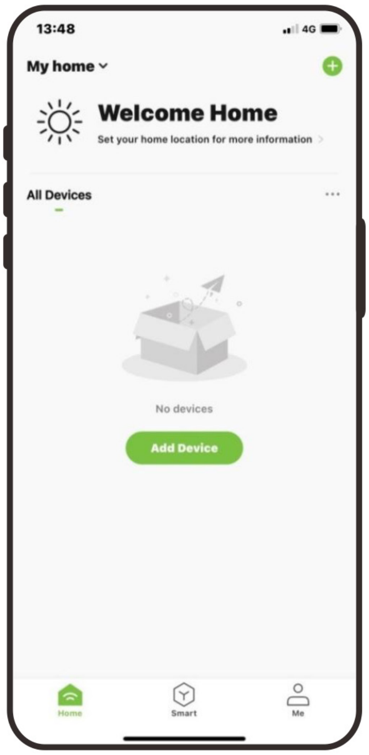
Note: For other specific operations, please refer the *ZKBioTime 8.0 User Manual*.

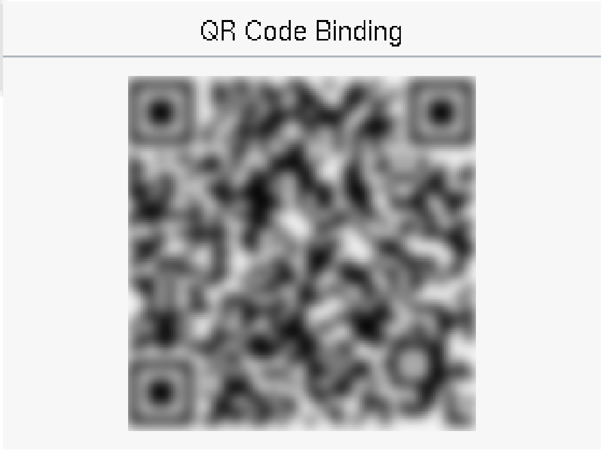
22 Connecting to ZSmart App★

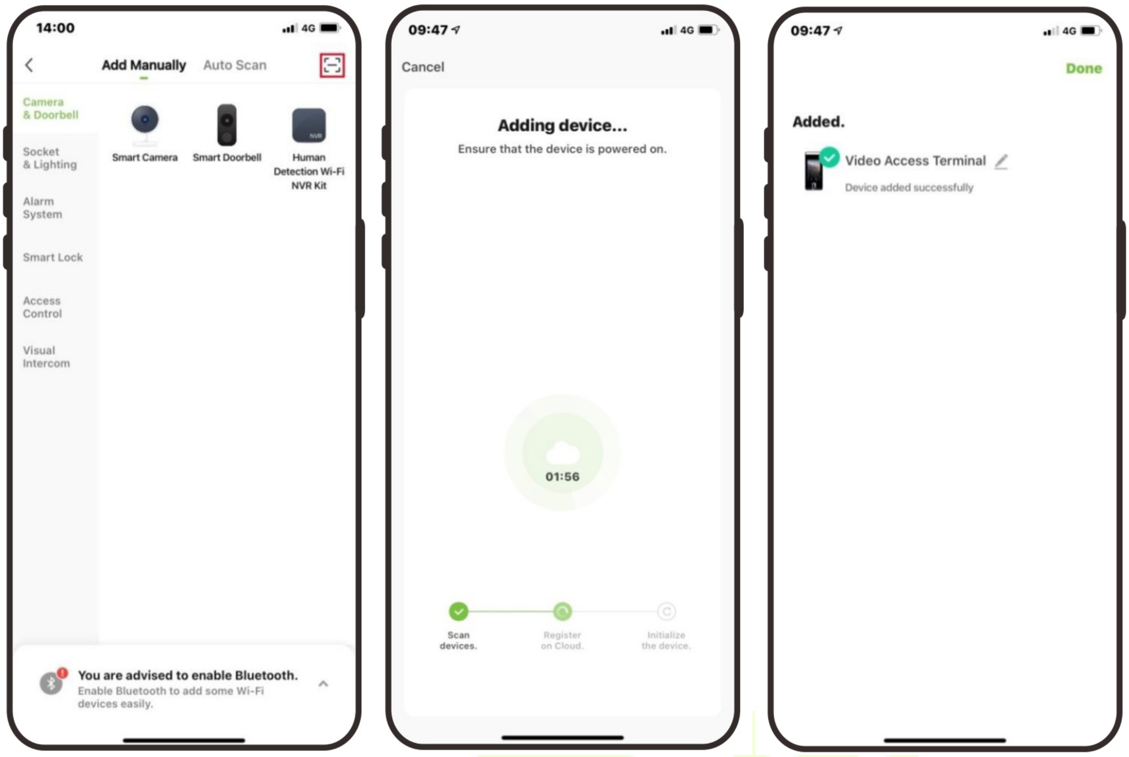
22.1 Adding Device on the ZSmart App

After downloading and installing the ZSmart App on your phone, start by setting up a user account using your Email ID. After completing the User account creation, proceed to log in to the App. Next, click either the Add Device or ⊕ icon situated at the top right corner of the screen to initiate the device addition process. The step-by-step process is as follows:

1. Click **Add Device** on the Home page.
2. On the device, tap on [**M/OK**] > **System** > **Video Intercom Parameters** > **QR Code Binding** to show the QR code of the device.
3. Click the ⛶ icon in the upper right corner.







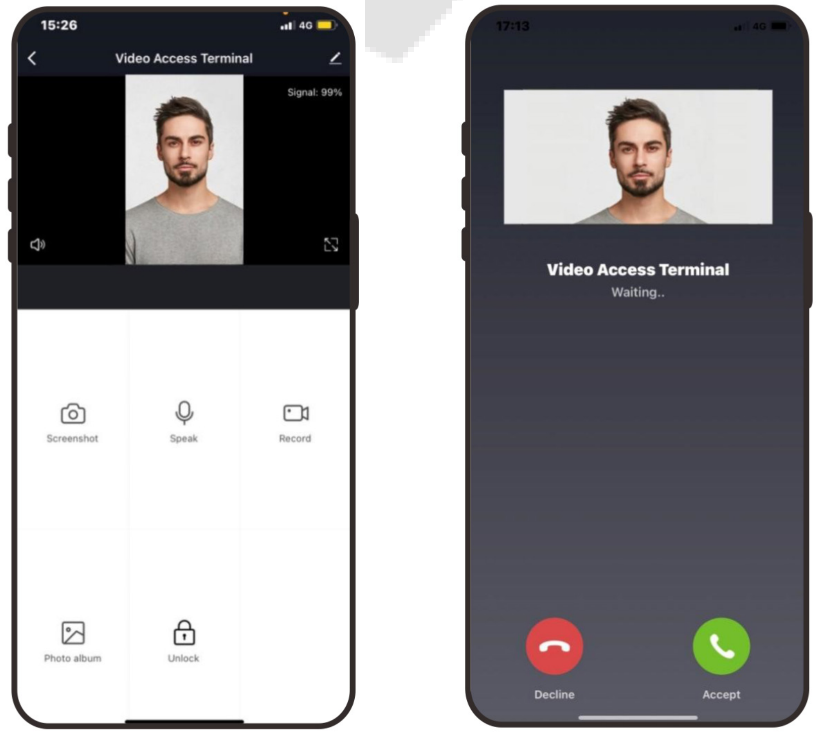
You are advised to enable Bluetooth.
Enable Bluetooth to add some Wi-Fi devices easily.

Adding device...
Ensure that the device is powered on.

Added.
Device added successfully

22.2 Video Phone Connection

Visitors click the 🔔 icon on the device to make a call and then phone will ring. The user can accept or decline the call. After the user accepts the call, it will open the video door phone interface. Enter the password to unlock the door.



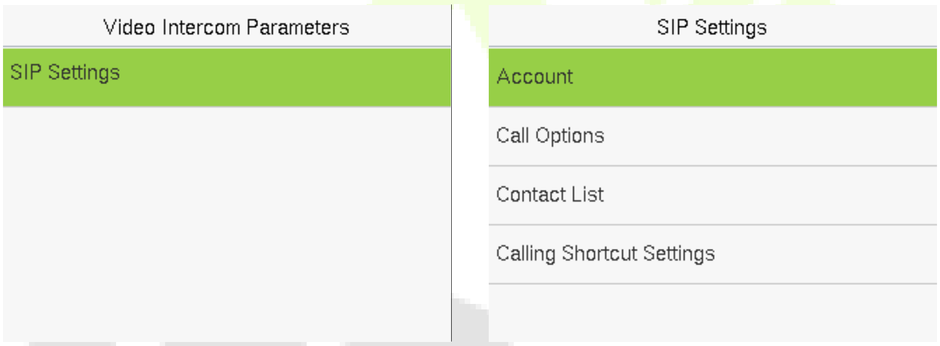
Parameter	Description
Screenshot	Click to take a screenshot.
Speak	The icon becomes blue when click it, and you can talk to the device at this time.
Record	Click to make a record video.
Photo album	View and delete screenshots and recorded videos.
Unlock	Click to open the door remotely. The unlocking record is saved in **Me** > **Message Center**.

Note: For other specific operations, please refer to the *ZSmart App User Manual*.

23 Connecting to SIP★

On the device, tap on [**M/OK**] >**System > Video Intercom Parameters** > **SIP Settings** to go to the monitoring parameter settings.

Note: This function needs to be used with the indoor station.



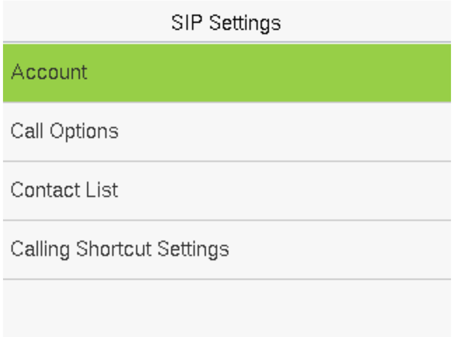
Function Description

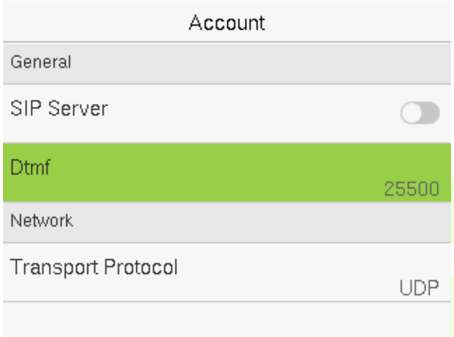
Function Name		Description
Account	SIP Server	Select whether to enable the SIP server. When it is enabled, the server address, server port, Login Name, User Name and Password need to be set. (**Note:** Each time it is switched ON/OFF, the device will restart to take effect.)
	Enable Domain Name	Select whether to enable the domain name mode.
	Server Address	Enter the server address.
	Server Port	Enter the server port.
	Login Name	Enter the login name of server.
	User Name	Enter the username of server.
	Password	Enter the password of server.
	Dtmf	The value should be set as same as the value of DTMF in the indoor station.
	Transport Protocol	Set the transport protocol between F35 and indoor station.
Call Options	Calling Delay(s)	Set the time of call, valid value 30 to 60 seconds.
	Talking Delay(s)	Set the time of intercom, valid value 60 to 120 seconds.
	Encryption	It is disabled by default.
Contact List	When the SIP server is disabled, the device number and call address of the indoor stations can be added here.	
Calling Shortcut Settings	Call Mode	When the SIP server is enabled, it is Standard Mode by default and cannot be modified; When the SIP server is disabled, it can be set as Standard Mode/ Direct Calling Mode. In Direct Calling mode, the user can call multiple indoor stations at the same time.
	There are 3 shortcut keys that can be defined in the device: **admin**, **ROOM1** and **ROOM2**. You can set a shortcut key to call the indoor station quickly without entering the IP address or room number of the indoor unit each time.	

The F35 and the indoor station to achieve video intercom there are two modes, respectively, the LAN and SIP server.

23.1 Local Area Network Use

1. Set the indoor station to the same network segment as the device.
2. On the **SIP Settings** interface, click on **Account** > **Dtmf** to set the value as same as the value of DTMF in the indoor station.



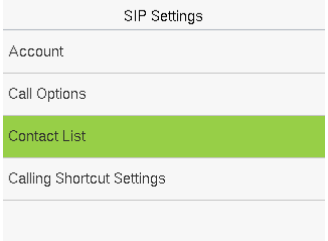


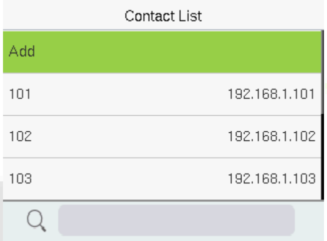
SIP Server

Dtmf 25500

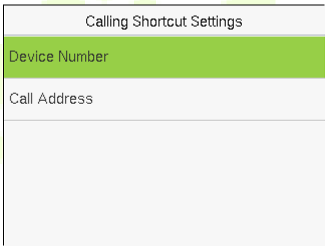
Transport Protocol UDP

3. On the **SIP Settings** interface, click on **Contact List**> **Add** to add the connected indoor station.





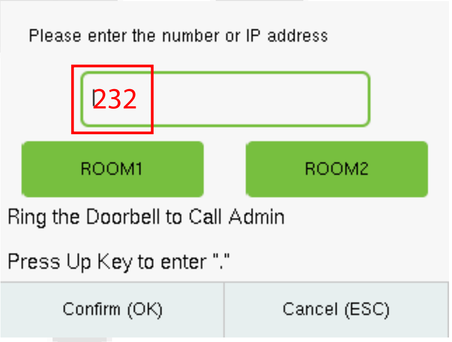
101	192.168.1.101
102	192.168.1.102
103	192.168.1.103



Device Number: Customize the number of the indoor station, you can enter this number on the device to call the indoor station quickly for video intercom.

Call Address: It is the IP Address of the indoor station.

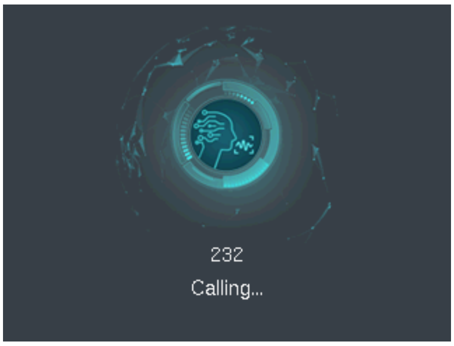
4. To enable the video intercom function, tap the 🔔 icon on the F35 and enter the IP address or device number of the indoor station in the provided interface.


Please enter the number or IP address

232

Ring the Doorbell to Call Admin

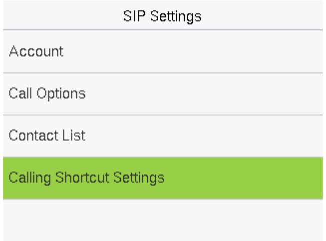
Press Up Key to enter "."


232

Calling...

Custom the Calling Shortcut Keys

1. On the **SIP Settings** interface, click on **Calling Shortcut Settings** to define the shortcut keys.



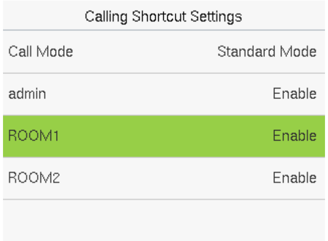
SIP Settings

Account

Call Options

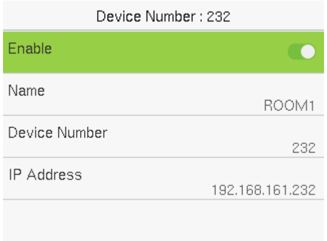
Contact List

Calling Shortcut Settings



Calling Shortcut Settings

Call Mode	Standard Mode
admin	Enable
ROOM1	Enable
ROOM2	Enable



Device Number : 232

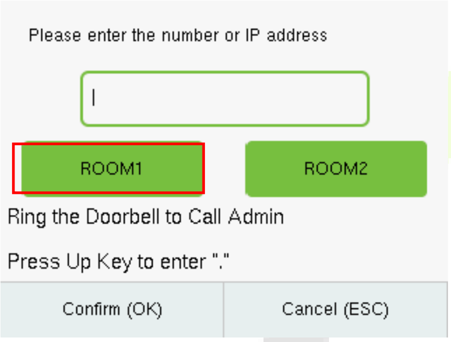
Enable	●
Name	ROOM1
Device Number	232
IP Address	192.168.161.232

Name: Customize the name of the shortcut keys.

Device Number: It is the device number that set in the **Contact List** Menu.

IP Address: Once the device number is set, it will be automatically displayed.

2. Then you can tap the 🔔 icon on the F35 and click the calling shortcut keys to call the indoor station.



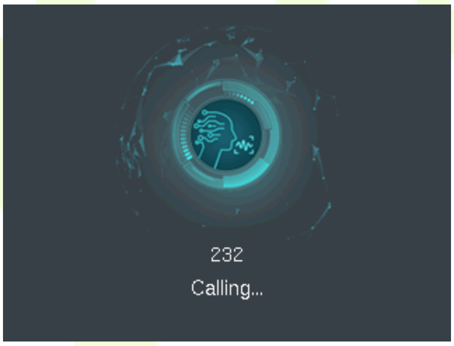
Please enter the number or IP address

ROOM1 ROOM2

Ring the Doorbell to Call Admin

Press Up Key to enter "."

Confirm (OK) Cancel (ESC)

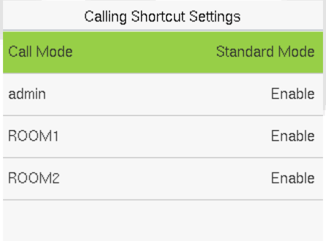


232

Calling...

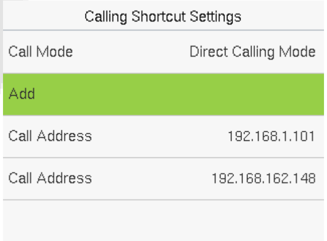
Direct Calling

1. On the **SIP Settings** interface, click on **Calling Shortcut Settings** > **Call Mode** > **Direct Calling Mode** > **Add**. Select the IP addresses of the indoor stations that you want to call, then the indoor stations will be displayed in the list.



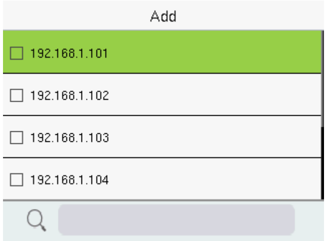
Calling Shortcut Settings

Call Mode	Standard Mode
admin	Enable
ROOM1	Enable
ROOM2	Enable



Calling Shortcut Settings

Call Mode	Direct Calling Mode
Add	
Call Address	192.168.1.101
Call Address	192.168.162.148



Add

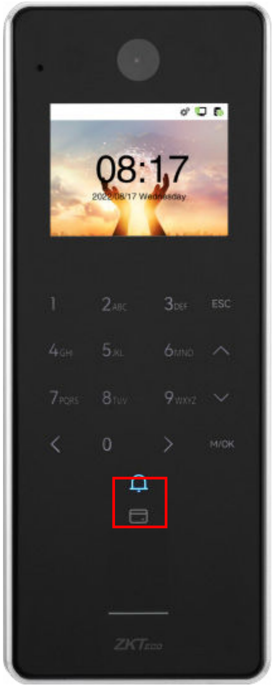
□ 192.168.1.101

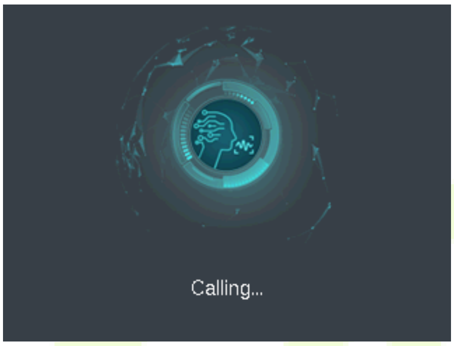
□ 192.168.1.102

□ 192.168.1.103

□ 192.168.1.104

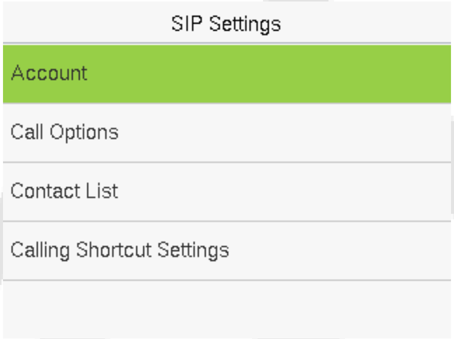
2. Then you can tap the 🔔 icon on the F35 to call the indoor stations at the same time.

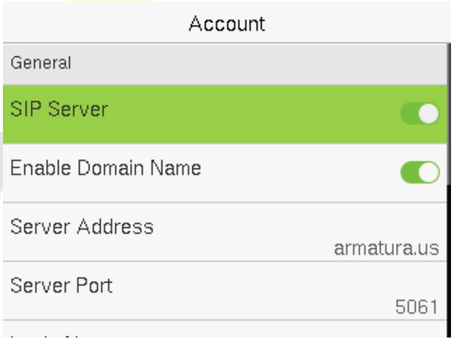




23.2 SIP Server

1. On the **SIP Settings** interface, click on **Account** > **SIP Server** to enable it, enter the server-related parameters, as shown below:





SIP Server ●

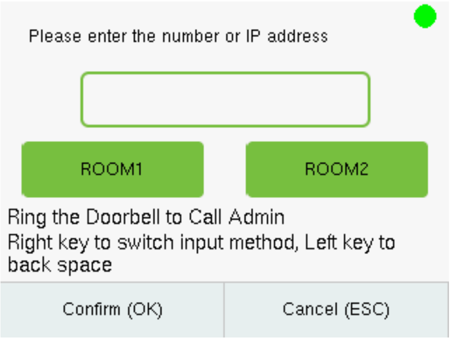
Enable Domain Name ●

Server Address armatura.us

Server Port 5061

2. After correctly setting up the SIP, a green dot will appear in the upper right corner of the call page, indicating that the F35 is connected to the server. You can then initiate a call to the account name of the indoor station."

   Note: Customers create their own SIP server.

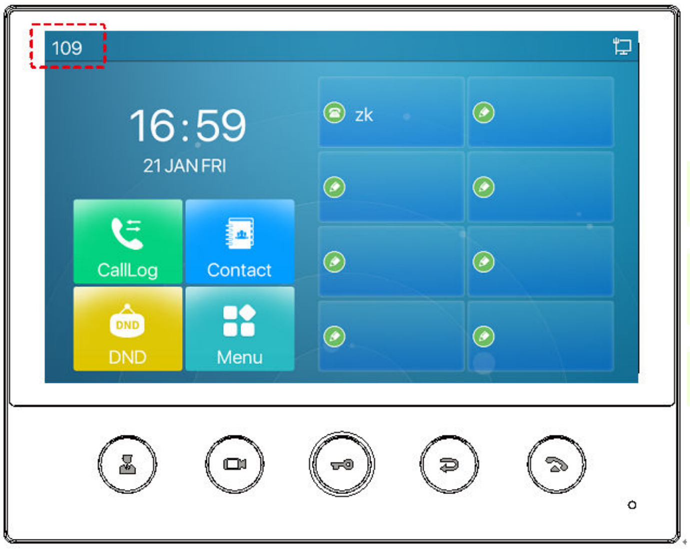


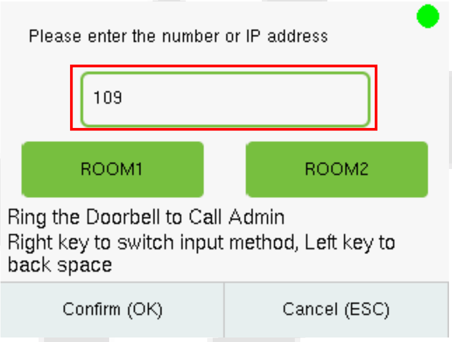
Please enter the number or IP address

ROOM1 ROOM2

Ring the Doorbell to Call Admin
Right key to switch input method, Left key to back space

Confirm (OK) Cancel (ESC)





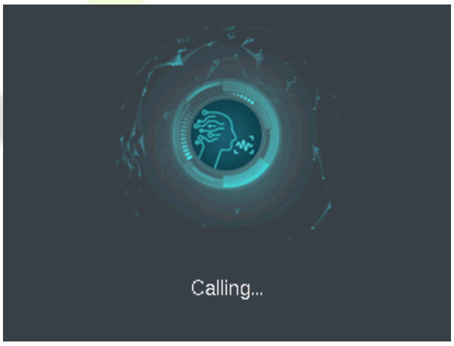
Please enter the number or IP address

109

ROOM1 ROOM2

Ring the Doorbell to Call Admin
Right key to switch input method, Left key to back space

Confirm (OK) Cancel (ESC)



Calling...

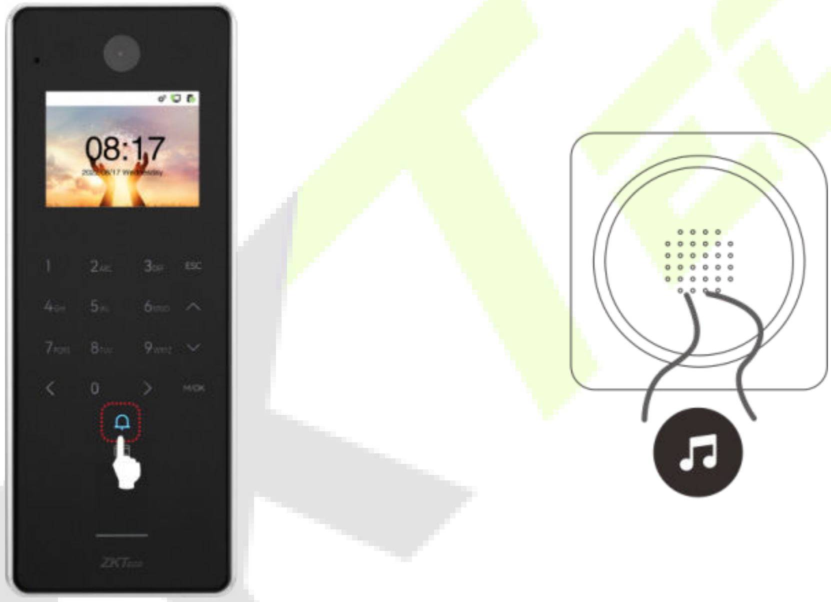
For details on the operation and use of the indoor station, please refer to the *Indoor Station User Manual*.

24 Connecting to Wireless Doorbell★

Note: This function needs to be used with the wireless doorbell.

24.1 Connect the Wireless Doorbell

1. First, power on the wireless doorbell. Then, press and hold the music button ♫ for 1.5 seconds until you see the indicator start flashing. The flashing indicator shows that the doorbell is now in pairing mode. If the wireless doorbell rings and the indicator flashes, the connection has been successful, and you can then click on the device icon 🔔 to finish the process.



2. After a successful pairing, click the device icon 🔔 will ring the wireless doorbell.

Note:

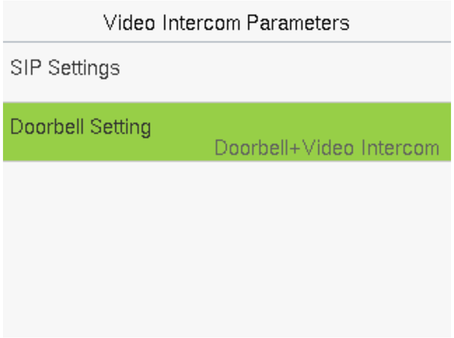
1) Each F35 only supports one wireless doorbell.
2) Wireless doorbell needs to be purchased by the customers themselves.

24.2 Unbinding the Wireless Doorbell

Power off the wireless doorbell first, then re-installing the batteries while pressing and holding the music button ♫ until the indicator is on, indicating that the unbinding is successful.

24.3 Settings

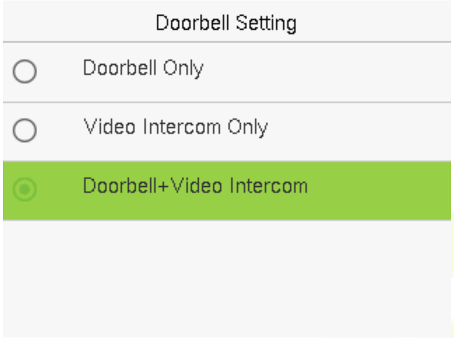
On the device, tap on [**M/OK**] >**System > Video Intercom Parameters** > **Doorbell Setting** to set the doorbell.



Video Intercom Parameters

SIP Settings

Doorbell Setting
Doorbell+Video Intercom



Doorbell Setting

○ Doorbell Only

○ Video Intercom Only

● Doorbell+Video Intercom

Function Description:

Function Name	Description
Doorbell Setting	**Doorbell Only:** When the user clicks on the doorbell button, only the doorbell rings. **Video Intercom Only:** When the user clicks on the doorbell button, only the device makes a call. **Doorbell+Video Intercom:** When the user clicks on the doorbell button, the doorbell rings and the device makes a call at the same time.

Appendix 1

Privacy Policy

Notice:

To help you better use the products and services of ZKTeco and its affiliates, hereinafter referred as "we", "our", or "us", the smart service provider, we consistently collect your personal information. Since we understand the importance of your personal information, we took your privacy sincerely and we have formulated this privacy policy to protect your personal information. We have listed the privacy policies below to precisely understand the data and privacy protection measures related to our smart products and services.

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.

IV. Others

You can visit https://www.zkteco.com/cn/index/Index/privacy_protection.html to learn more about how we collect, use, and securely store your personal information. To keep pace with the rapid development of technology, adjustment of business operations, and to cope with customer needs, we will constantly deliberate and optimize our privacy protection measures and policies. Welcome to visit our official website at any time to learn our latest privacy policy.

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.

ZKTeco Industrial Park, No. 32, Industrial Road,
Tangxia Town, Dongguan, China.

Phone : +86 769 - 82109991

Fax : +86 755 - 89602394

www.zkteco.com