User Manual

SC800

Date: November 2022

Doc Version: 1.1

English

Table of Contents

1 SAFETY MEASURES 5

2 ELECTRICAL SAFETY 6

3 OPERATION SAFETY 7

4 INSTRUCTIONS FOR USE 9

4.1 INSTALLATION 9

4.1.1 INSTALLATION ENVIRONMENT 9

4.1.2 DEVICE INSTALLATION 9

4.2 STANDBY INTERFACE 10

4.3 VERIFICATION MODE 12

4.3.1 CARD VERIFICATION 12

4.3.2 PASSWORD VERIFICATION 13

4.3.3 COMBINED VERIFICATION 14

4.4 APPEARANCE 16

4.5 TERMINAL DESCRIPTION 16

4.6 WIRING DESCRIPTION 18

4.6.1 POWER CONNECTION 18

4.6.2 ETHERNET CONNECTION 18

4.6.3 DOOR SENSOR, EXIT BUTTON, ALARM AND AUXILIARY CONNECTION 19

4.6.4 LOCK RELAY CONNECTION 19

4.6.5 WIEGAND READER CONNECTION 20

4.6.6 RS485 CONNECTION 20

4.6.7 RS232 CONNECTION 20

5 MAIN MENU 21

6 USER MANAGEMENT 23

6.1 NEW USER REGISTRATION 23

6.1.1 REGISTER A USER ID 23

6.1.2 USER ROLE 24

6.1.3 CARD NUMBER 24

6.1.4 PASSWORD 25
6.1.5 ACCESS CONTROL ROLE 25
6.2 ALL USERS 26
6.2.1 EDIT USER 27
6.2.2 DELETE USER 27
6.3 DISPLAY STYLE 28
7 USER ROLE 29
8 COMMUNICATION 31
8.1 ETHERNET 31
8.2 SERIAL COMM 32
8.3 PC CONNECTION 33
8.4 WI-FI SETTINGS 34
8.5 CLOUD SERVER SETTINGS 36
8.6 WIEGAND SETUP 37
8.6.1 WIEGAND INPUT 38
8.6.2 WIEGAND OUTPUT 41
8.7 NETWORK DIAGNOSIS 42
9 SYSTEM SETTINGS 43
9.1 DATE AND TIME 43
9.2 ACCESS LOGS SETTINGS AND ATTENDANCE 45
9.3 CARD MANAGEMENT 47
9.4 DEVICE TYPE SETTINGS 48
9.5 SECURITY SETTINGS 48
9.6 FACTORY RESET 49
10 PERSONALIZE SETTINGS 51
10.1 USER INTERFACE 51
10.2 VOICE 53
10.3 BELL SCHEDULES 53
10.4 PUNCH STATES OPTIONS 55
10.5 SHORTCUT KEY MAPPINGS 57

11 DATA MANAGEMENT 59
11.1 DELETE DATA 59
11.2 BACKUP DATA 60
11.3 RESTORE DATE 61
12 ACCESS CONTROL 63
12.1 ACCESS CONTROL OPTIONS 64
12.2 TIME RULE SETTINGS AND TIME SCHEDULE 69
12.3 HOLIDAYS 70
12.4 ACCESS GROUPS 72
12.5 COMBINED VERIFICATION 73
12.6 ANTI-PASSBACK SETUP 75
12.7 DURESS OPTIONS SETTINGS 76
13 ATTENDANCE SEARCH 79
14 WORK CODE 80
14.1 NEW WORK CODE 80
14.2 ALL WORK CODES 81
14.3 WORK CODE OPTIONS 81
15 AUTOTEST 83
16 SYSTEM INFORMATION 85
17 CONNECT TO ZKBIO ACCESS IVS SOFTWARE 86
17.1 SET THE COMMUNICATION ADDRESS 86
17.2 ADD DEVICE ON THE SOFTWARE 87
17.3 ADD PERSONNEL ON THE SOFTWARE 88
18 CONNECT TO BIOTIME 8.0 SOFTWARE 89
18.1 SET THE COMMUNICATION ADDRESS 89
18.2 ADD DEVICE ON THE SOFTWARE 89
18.3 ADD PERSONNEL ON THE SOFTWARE 90
19 CONNECT TO WEBSERVER 91
19.1 LOGIN WEBSERVER 91
19.2 FORGOT PASSWORD 93

19.3 USER REGISTRATION 96
19.4 SEARCH FOR USERS.....98
19.5 EDIT USER.....98
19.6 DELETE USER.....99
19.7 COMM. 100
19.8 CLOUD SERVER SETTINGS 101
19.9 DATE SETUP 102
19.10 SYSTEM 103
19.11 SERIAL COMM..... 105
19.12 WIEGAND SETUP..... 106
19.13 ACCESS CONTROL OPTIONS..... 107
19.14 DEVICE MANAGEMENT 109
19.15 UPDATE FIRMWARE..... 110
19.16 CHANGE PASSWORD 111
19.17 OPERATION LOG..... 112
19.18 DOWNLOAD FIRMWARE LOGS 113
19.19 SYSTEM INFORMATION 113
ECO-FRIENDLY OPERATION 116

1 Safety Measures

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

Just change controls defined in operating instructions. Improper adjustment of the controls may result in damage and involve a qualified technician to return the device to normal operation.

And do not connect multiple devices to one power adapter, as adapter overload can cause over-heat or fire hazard.

7. **Replacement parts** - When replacement parts are needed, service technicians must only use replacement parts provided by the supplier. Unauthorized substitutes can result in a burn, shock, or other hazards.
8. **Safety check** - On completion of servicing or repair work on the unit, ask the service technician to perform safety checks to make sure that the 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, contact your dealer.
10. **Lightning** - External lightning conductors can be installed to provide protection against electrical storms. It prevents power-ups from destroying the system.

    It is recommended that the devices are installed 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.
- Make sure 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 in your country or region is used. If you are not sure about the recommended standard voltage, please consult your local electric power company. A mismatch in power might result in a short circuit or device damage.
- Return the device to professional technical personnel or your dealer if the power supply is damaged.
- To avoid interference, keep the device away from high electromagnetic radiation devices, such as generators (including electric generators), radios, televisions, (especially CRT) monitors, or speakers.

3 Operation Safety

- If smoke, smell, or noise rise from the device, immediately turn off the power and unplug the power cable, and then please contact the service center.
- Transportation and other unpredictable factors may cause damage the device hardware. Before installation, check to see whether the device has any severe damage.
- If the device has major defects that you cannot solve, contact your dealer as soon as possible.
- Dust, moisture, and sudden temperature changes all 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 vibrating surfaces. 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 incorrect operation, and damage due to independent installation or repair of the product by the user.

4 Instructions for Use

4.1 Installation

4.1.1 Installation Environment

Please refer to the following recommendations for installation

KEEP DISTANCE

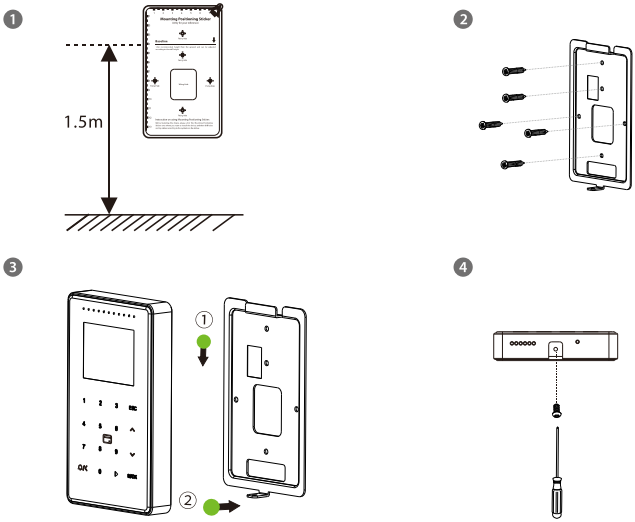
AVOID GLASS REFRACTION

AVOID DIRECT SUNLIGHT AND EXPOSURE

AVOID USE OF ANY HEAT SOURCE NEAR THE DEVICE

4.1.2 Device Installation

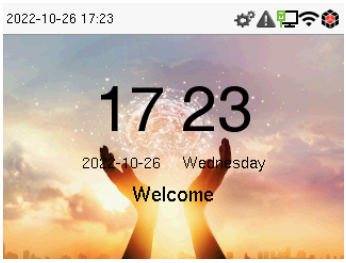
1. Stick the mounting template sticker to the wall, and drill holes according to the mounting template sticker.
2. Fix the backplate on the wall using wall mounting screws.
3. Place the device to the backplate.
4. Mount the device to the backplate with the security screws.



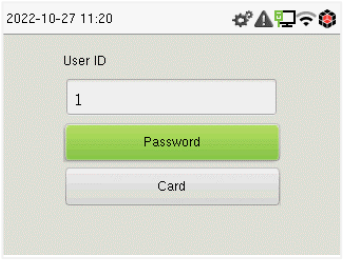
4.2 Standby Interface

The device uses a 2.4-inch color screen, which all operations are performed through hidden touch keypad. (***Note:*** The device only supports the input of numbers, other characters such as English and symbols can be synchronized by the software down.) Before getting into the device features and functions, it is recommended to be familiar with the below fundamentals.

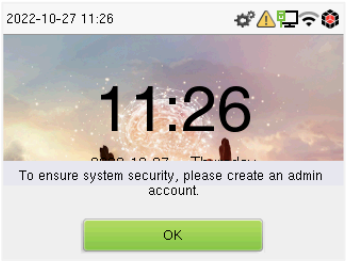
After connecting the power supply, the following standby interface is displayed:

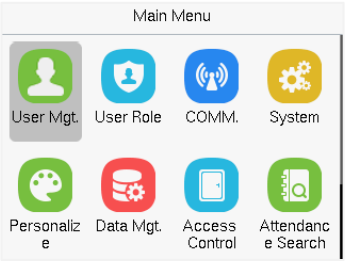


- Enter any number to access the User ID input interface.

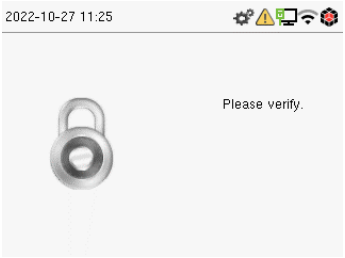


- When there is no Super Administrator set in the device, tap **M/OK** to go to the menu.



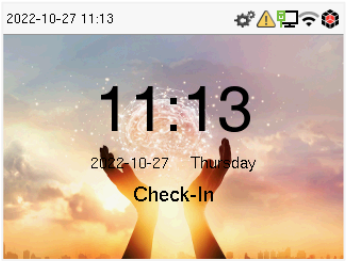


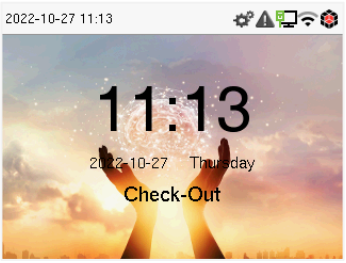
- After adding a Super Administrator on the device, it requires the Super Administrator's verification before opening the menu functions.



Note: 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."





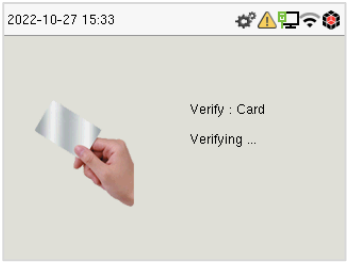
Note: The punch state options are disabled by default, and you must select other mode options in the "Punch States Options" section to see them on the standby screen.

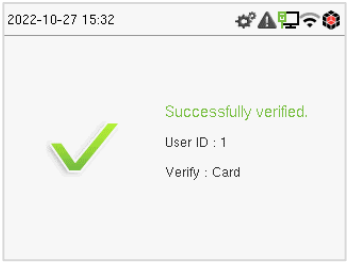
4.3 Verification Mode

4.3.1 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 is the card verification screen:

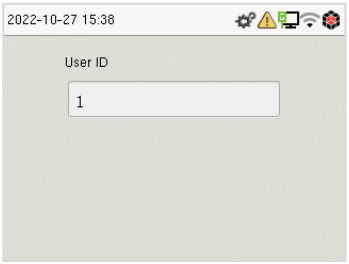


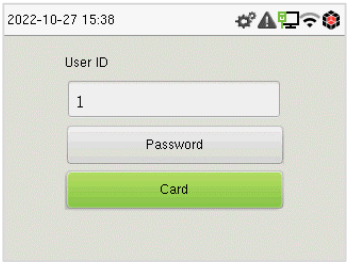


- **1:1 Card Verification Mode:**

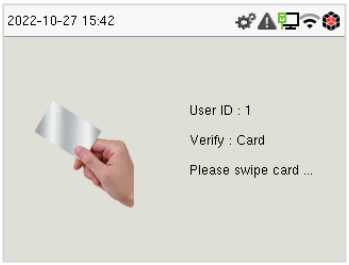
The 1:1 Card Verification mode compares the card number in the card induction area with the number associated with the employee's User ID registered in the device.

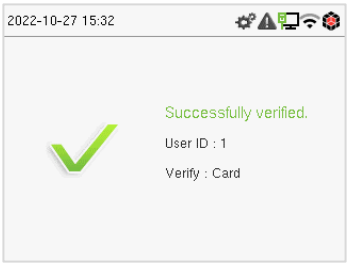
Enter the user ID and tap **M/OK** to enter the 1:1 card verification mode.





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

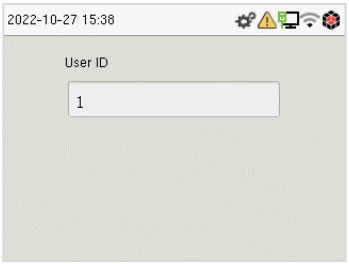


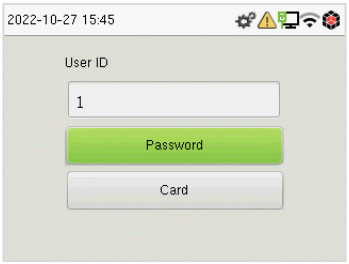


4.3.2 Password Verification

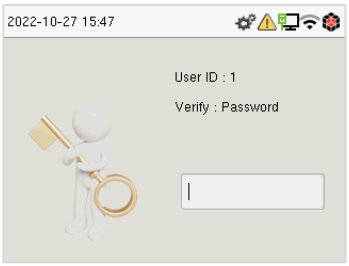
The device compares the entered password with the registered password of the given User ID.

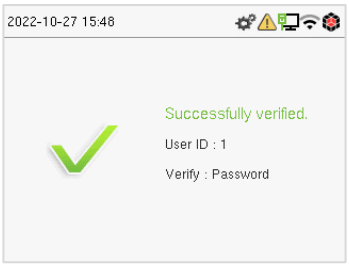
Enter the user ID and tap **M/OK** to enter the 1:1 password verification mode. Then, input the user ID and tap **M/OK**.





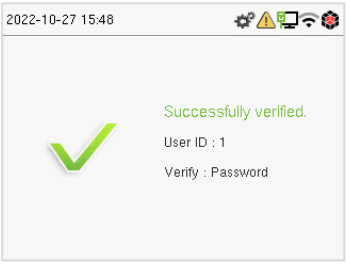
If an employee registers a card in addition to the password, the following screen will appear. Select the password to enter card verification mode.



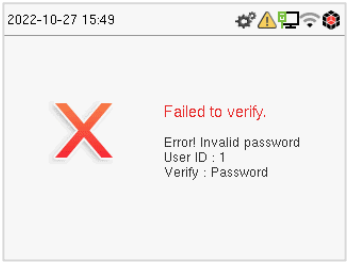


Below are the display screens after entering a correct password and a wrong password, respectively.

Verification is successful:



Verification is failed:



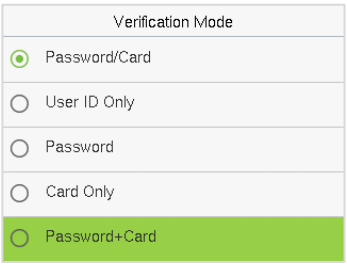
4.3.3 Combined Verification

This device allows you to use a different types of verification methods to increase security. There are a total of 5 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.



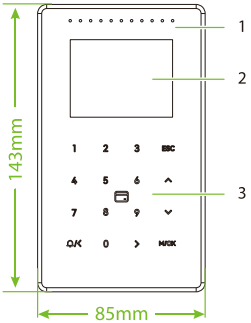
Combined Verification Mode set up procedure:

- 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.

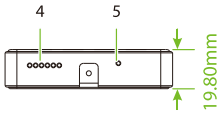
Reason:

- 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 "Verification Failed."

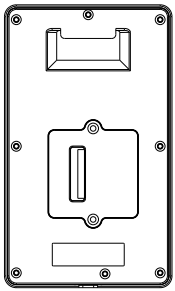
4.4 Appearance



Front



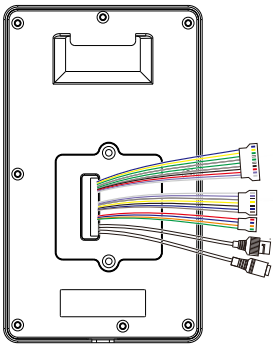
Bottom



Rear

No.	Description
1	Breathing Light
2	2.4-inch Color Screen
3	Hidden Touch Keypad
4	Speaker
5	Reset

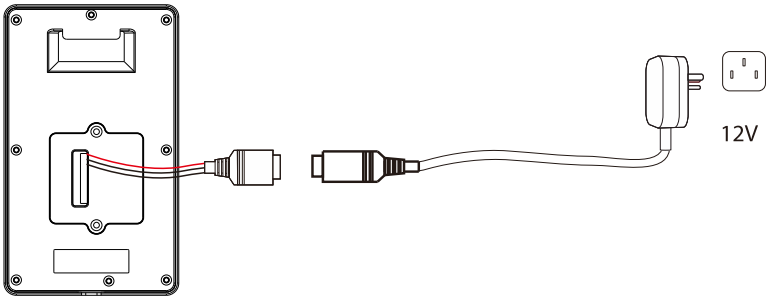
4.5 Terminal Description



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

4.6 Wiring Description

4.6.1 Power Connection

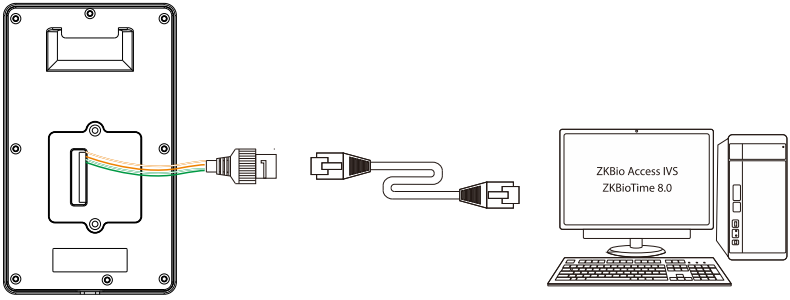


Recommended AC Adapter

1. 12V ± 10%, at least 3A.
2. To share the power with other devices, use an AC Adapter with higher current ratings.

4.6.2 Ethernet Connection

Connect the device and computer via an Ethernet cable, as shown in the example below:

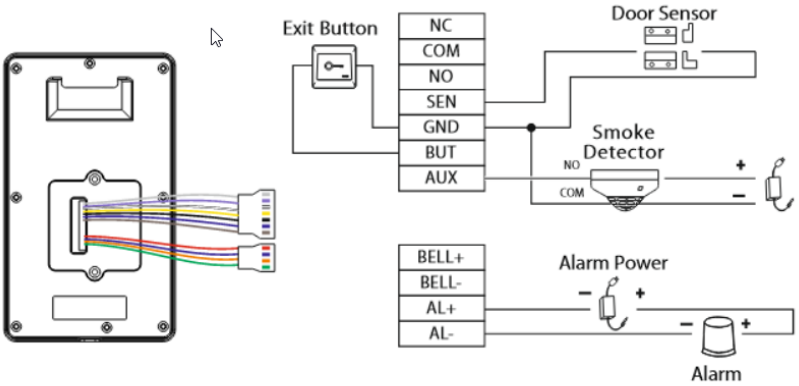


Default IP address: 192.168.1.201
Subnet mask: 255.255.255.0

IP address: 192.168.1.130
Subnet mask: 255.255.255.0

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

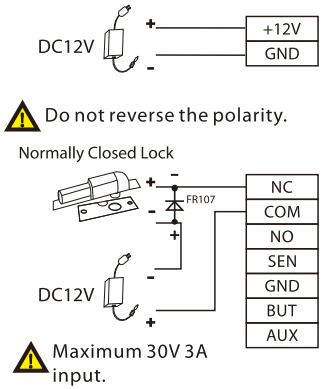
4.6.3 Door Sensor, Exit Button, Alarm and Auxiliary Connection



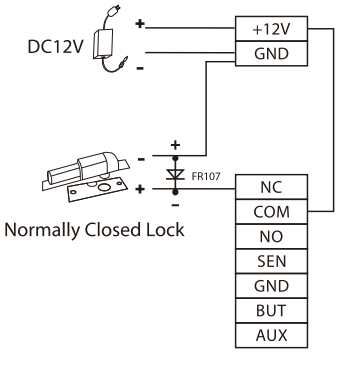
4.6.4 Lock Relay Connection

The system supports Normally Opened Lock and Normally Closed Lock. The NO LOCK (normally unlocked when power-ON) is connected with 'NO' and 'COM' terminals, and the NC LOCK (normally locked when power-ON) is connected with 'NC' and 'COM' terminals. Take NC Lock as an example below:

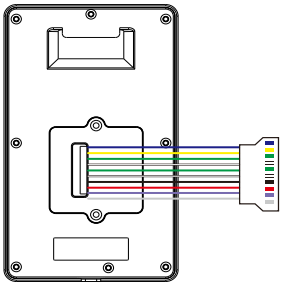
1) Device not sharing power with the lock

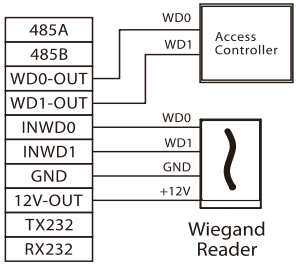


2) Device sharing power with the lock



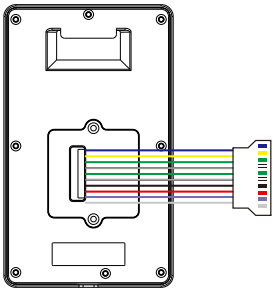
4.6.5 Wiegand Reader Connection

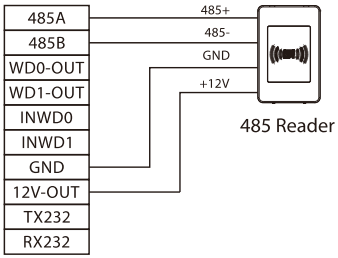




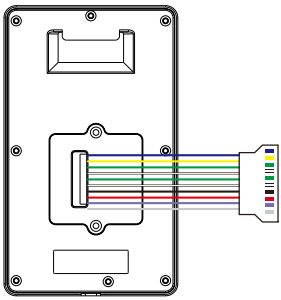
Note: 485A and 485B can be connected to the Barrier gate or the 485 Reader, separately, but cannot be connected to the gate and reader at the same time.

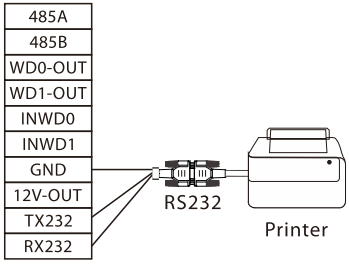
4.6.6 RS485 Connection





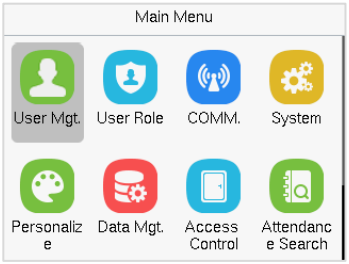
4.6.7 RS232 Connection

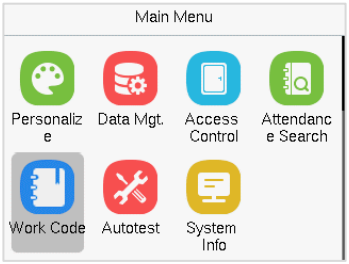




5 Main Menu

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





Function Description

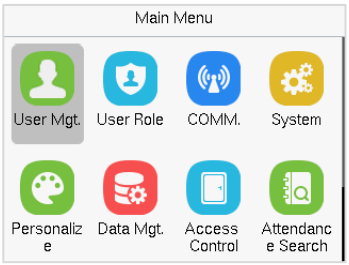
Menu	Description
User Mgt.	To Add, Edit, View, and Delete information of a User.
User Role	To set the permission scope of the custom role and enroller for the users, for example the system's operating rights.
COMM.	To set the relevant parameters of Network, Serial Comm., PC Connection, Wi-Fi, Cloud Server, Wiegand and Network Diagnosis.
System	To set parameters related to the system, including Date Time, attendance/Access Logs Settings, Card management, 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, backup or restore the data.

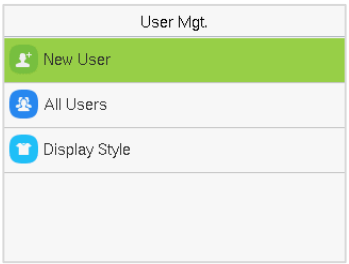
Access Control	To set the parameters of the lock and the relevant access control device including options like Time schedule, Holiday Settings, Combine verification, Anti-Passback Setup, and Duress Option Settings.
Attendance Search	To query the specified Event logs.
Work Code	Set different type of work.
Autotest	To automatically test whether each module functions properly, including the LCD Screen, Audio, Keyboard and Real-Time Clock.
System Info	To view Privacy Policy, Data Capacity and Device and Firmware information of the current device.

6 User Management

6.1 New User Registration

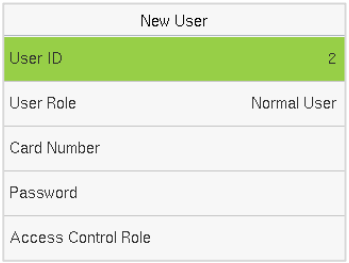
Tap **User Mgt.** on the main menu.

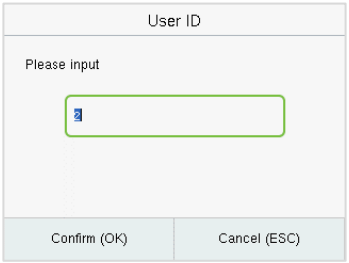




6.1.1 Register a User ID

Tap **New User** and enter the **User ID**.





Note:

1. By default, the user ID can have 1 to 14 digits.
2. During the initial registration, you can modify your ID but not after the registration.
3. If the message "**Duplicated!**" appears, you must choose a different User ID because the one you entered already exists.

4. The device only supports the input of numbers, other characters such as English and symbols can be synchronized by the software.

6.1.2 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.

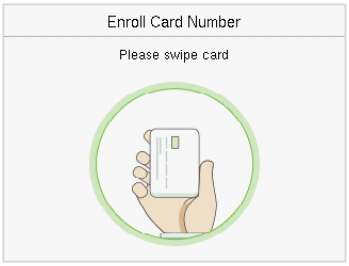
Note: If the selected user role is the Super Admin, then the user must pass the identity authentication to access the main menu. The authentication is based on the authentication method(s) that the super administrator has registered.

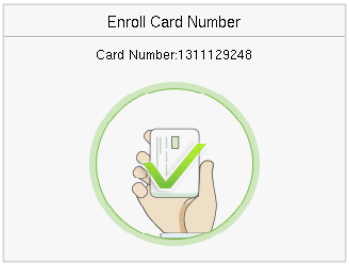
6.1.3 Card Number

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

- Swipe the card underneath the card reading area on the Card interface. 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 looks like this:

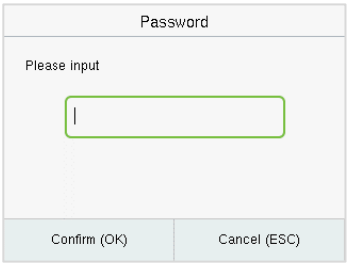


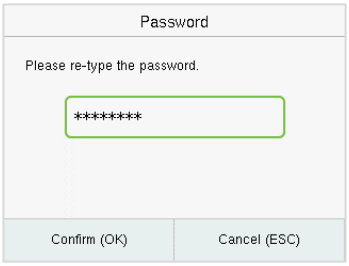


6.1.4 Password

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.

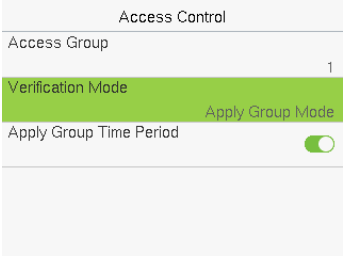




6.1.5 Access Control Role

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

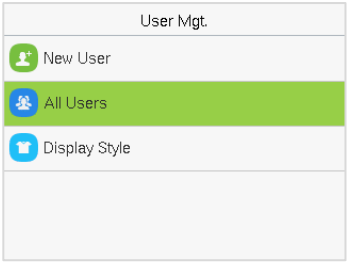
- Tap **Access Control Role** > **Access Group** to assign the registered users to different groups for better management. New users belong to Group 1 by default and can be reassigned to other groups. The device supports up to 99 Access Control groups.
- Tap **Verification Mode**, to select the verification mode.
- Tap **Apply Group Time Period**, to select the time to use.

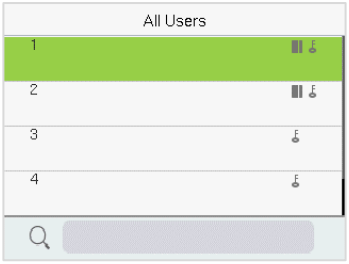


6.2 All Users

On the **Main Menu**, tap **User Mgt.**, and then tap **All Users** to search a User.

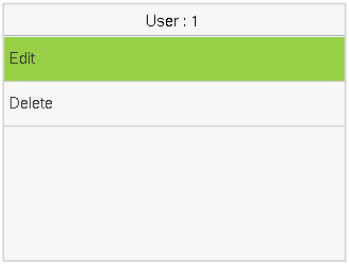
- On the **All-Users** interface, tap on the search bar on the user's list to enter the user ID and the system will search for the related user information.

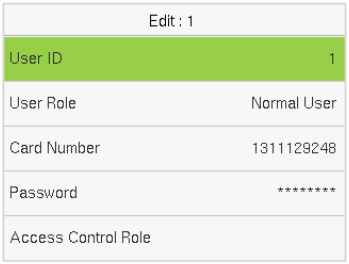




6.2.1 Edit User

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





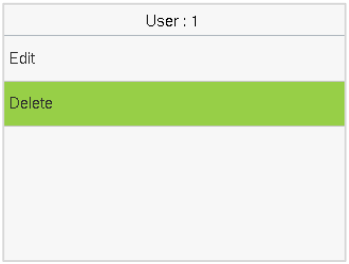
Note: The process of editing the user information is the same as adding a new user, except that the User ID cannot be modified while editing a user. The process in detail refers to "User Registration".

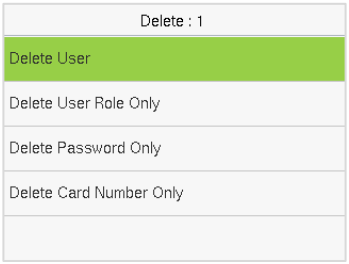
6.2.2 Delete User

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:

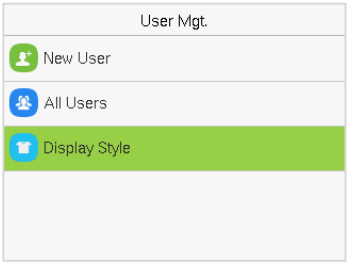
- **Delete User:** Deletes all the user information (deletes the selected User as a whole) from the Device.
- **Delete User Role Only:** Deletes the user's administrator privileges and make the user a normal user.
- **Delete Password Only:** Deletes the password information of the selected user.
- **Delete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





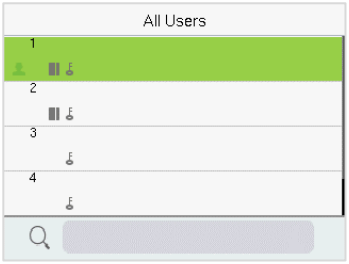
6.3 Display Style

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

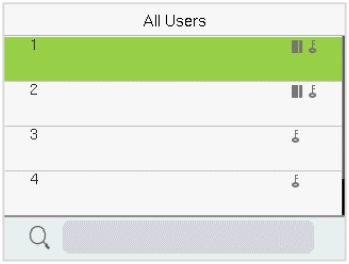


All the Display Styles are shown as below:

Multiple Line:



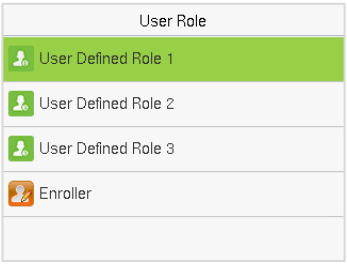
Mixed Line:



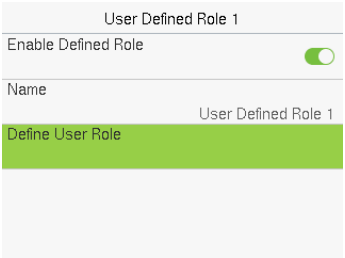
7 User Role

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

- On the **Main** menu, tap **User Role**, and then tap on the **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.

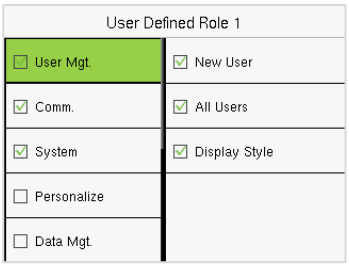


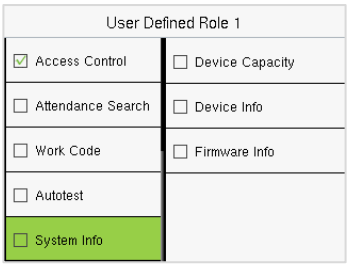
- On the **User Defined Role** interface, toggle **Enable Defined Role** to enable or disable the user defined role.



- 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.



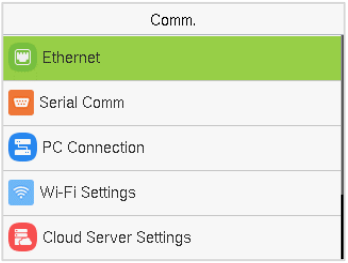


Note: If the User Role is enabled for the Device, tap on **User Mgt. > New User > User Role** to assign the created roles to the required users. But if there is no super administrator registered in the Device, then the device will prompt "**Please enroll super admin first!**" when enabling the User Role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

8 Communication

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

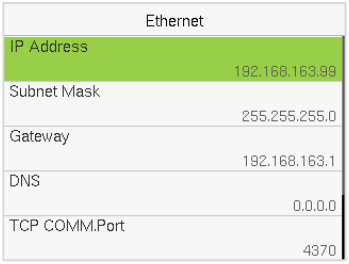
Tap **COMM.** on the main menu.

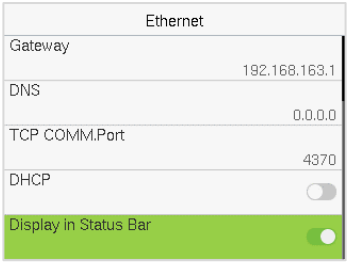


8.1 Ethernet

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

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





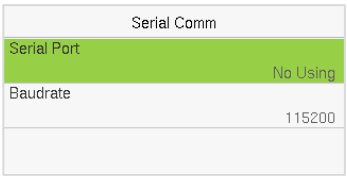
Function Description:

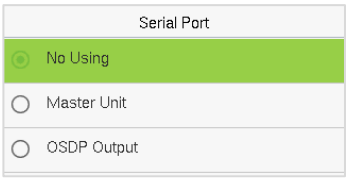
Function Name	Description
IP Address	The default IP address is 192.168.1.201. It can be modified according to the network availability.
Subnet Mask	The default Subnet Mask is 255.255.255.0. It can be modified according to the network availability.
Gateway	The Default Gateway address is 0.0.0.0. It can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

8.2 Serial Comm

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

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





Function Description

Function Name	Description
Serial Port	**No Using:** No communication with the device through the serial port. **Master Unit:** When OSDP is used as the function of "**Master unit**", it can be connected to a card reader. **OSDP Output:** Communicate with the device through the OSDP serial port.
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.

8.3 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.

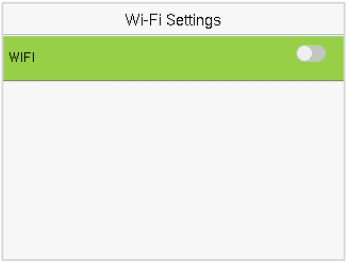
Baudrate	It is the identification number of the device, which ranges between 1 and 254. If the communication method is RS485, you need to input this device ID in the software communication interface.

8.4 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.

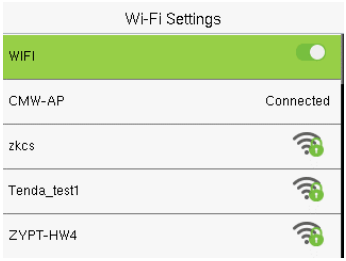
Tap **Wi-Fi Settings** on the **Comm.** Settings interface to configure the Wi-Fi settings.



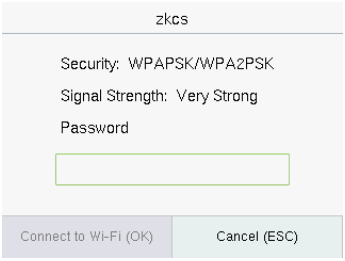
➢ **Searching the Wi-Fi Network**

- WIFI is enabled in the device by default. Toggle the button to enable or disable WIFI.
- 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**.



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



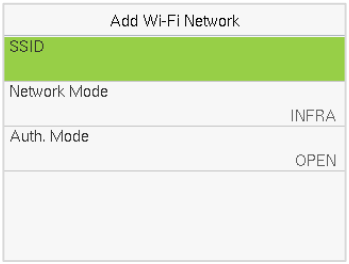
Tap on the password field to enter the password and tap **M/OK.**

- When the WIFI 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.

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

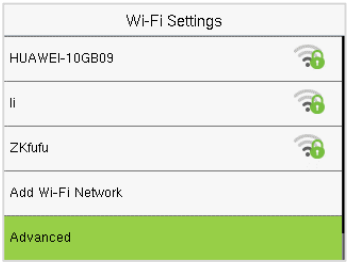


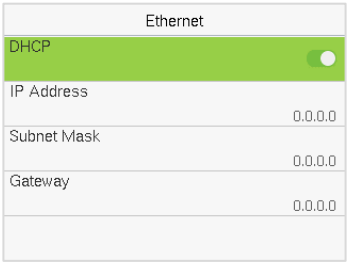
On this interface, enter the Wi-Fi network parameters. (The added network must exist.)

Note: After successfully adding the WIFI 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.



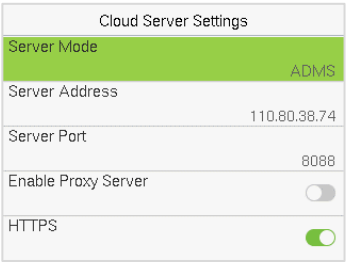


Function Description

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.

8.5 Cloud Server Settings

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



Function Description

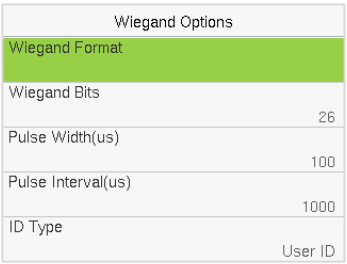
Function Name	Description
Server Address	The IP address of the ADMS server.
Server Port	Port used by the ADMS server.
Enable Proxy Server	The IP address and the port number of the proxy server is set manually when the proxy is enabled.
HTTPS	Based on HTTP, transmission encryption and identity authentication make sure that the security of the transmission process.

8.6 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.

8.6.1 Wiegand Input



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.

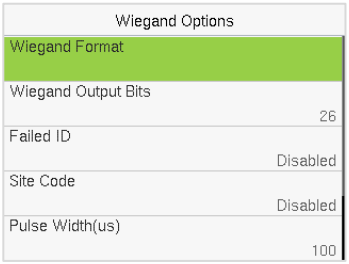
Various Common Wiegand Format Description:

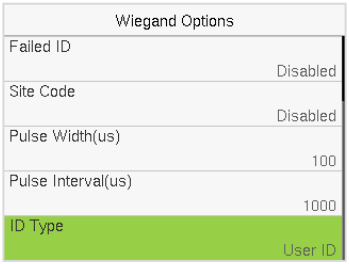
Wiegand Format	Description
Wiegand26	ECCCCCCCCCCCCCCCCCCCCCCCCO It consists of 26 bits of binary code. The 1st bit is the even parity bit of the 2nd to 13th bits, while the 26th bit is the odd parity bit of the 14th to 25th bits. The 2nd to 25th bits are the card numbers.
Wiegand26a	ESSSSSSSSCCCCCCCCCCCCCCCCO 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 are 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	OFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCMME It consists of 36 bits of binary code. The 1st bit is the odd parity bit of the 2nd to 18th bits, while the 36th bit is the even parity bit of the 19th to 35th bits. The 2nd to 17th bits is the device codes. The 18th to 33rd bits is the card numbers, and the 34th to 35th bits are the manufacturer codes.
Wiegand36a	EFFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCO It consists of 36 bits of binary code. The 1st bit is the even parity bit of the 2nd to 18th bits, while the 36th bit is the odd parity bit of the 19th to 35th bits. The 2nd to 19th bits is the device codes, and the 20th to 35th bits are the card numbers.
Wiegand37	OMMMMSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCE It consists of 37 bits of binary code. The 1st bit is the odd parity bit of the 2nd to 18th bits, while the 37th bit is the even parity bit of the 19th to 36th bits. The 2nd to 4th bits is the manufacturer codes. The 5th to 16th bits is the site codes, and the 21st to 36th bits are the card numbers.
Wiegand37a	EMMMFFFFFFFFFSSSSSSCCCCCCCCCCCCCCCCO It consists of 37 bits of binary code. The 1st bit is the even parity bit of the 2nd to 18th bits, while the 37th bit is the odd parity bit of the 19th to 36th bits. The 2nd to 4th bits is the manufacturer codes. The 5th to 14th bits is the device codes, and15th to 20th bits are the site codes, and the 21st to 36th bits are the card numbers.

Wiegand50	ESSSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO 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.	

8.6.2 Wiegand Output





Function Description

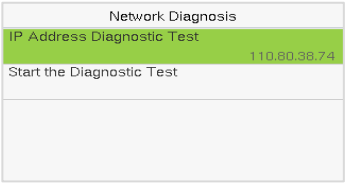
Function Name	Description
Wiegand Format	Its value can be 26 bits, 34 bits, 36 bits, 37 bits, and 50 bits.
Wiegand Output Bits	After selecting the required Wiegand format, select the corresponding output bit digits from the Wiegand format.

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.

8.7 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.

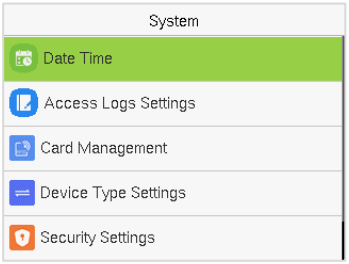


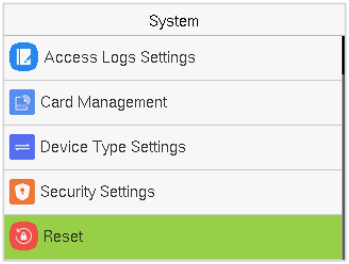
9 System Settings

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

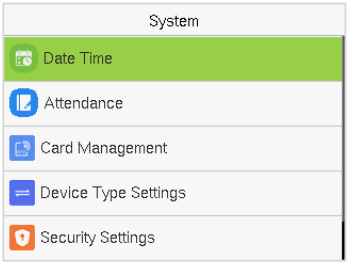
Tap **System** on the **Main Menu** interface to get into its menu options.

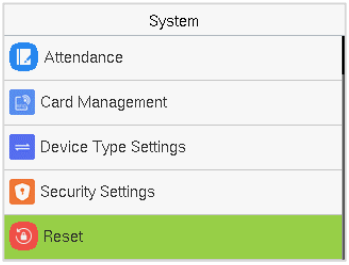
Access Control Terminal:





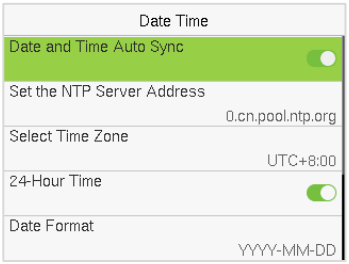
Time Attendance Terminal:



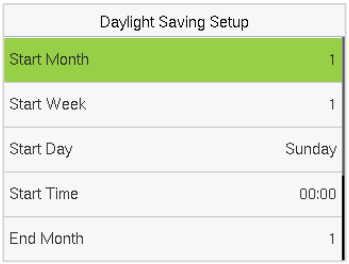


9.1 Date and Time

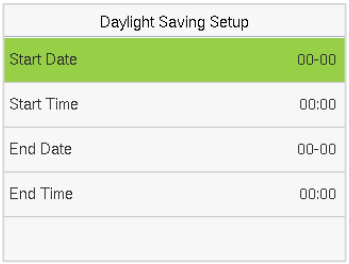
Tap **Date Time** on the **System** interface to set the date and time.



- Tap **Date and Time Auto Sync** to enable automatic time synchronization based on the service address you enter.
- Tap **Set the NTP Server Address** to manually set the date and time and then tap to **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.



Week Mode



Date Mode

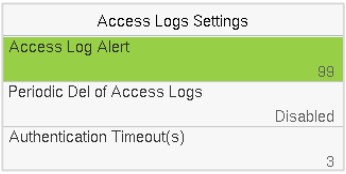
- When restoring the factory settings, the time (24-hour) and date format (YYYY-MM-DD) can be restored, but the device date and time cannot be restored.

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.

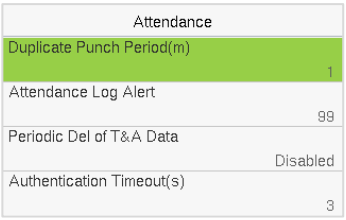
9.2 Access Logs Settings and Attendance

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

Access Control Terminal:



Time Attendance Terminal:



Function Description of Access Control Terminal:

Function Name	Description
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.

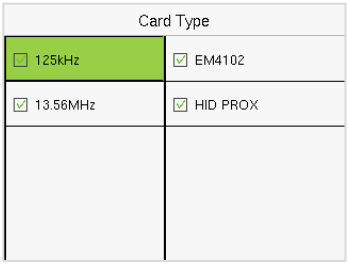
Function Description of Time Attendance Terminal:

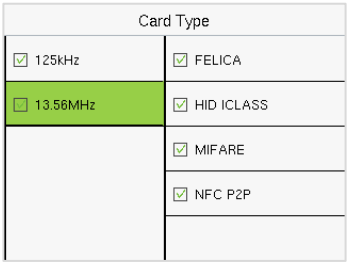
Function Name	Description
Duplicate Punch Period(m)	Within a set time period (unit: minutes), the duplicated attendance record will not be reserved (value ranges from 1 to 999999 minutes).
Attendance Log Alert	When the record space of the attendance reaches the maximum threshold value, the device automatically 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.

9.3 Card Management

Tap **Card Management** on the **System** interface.

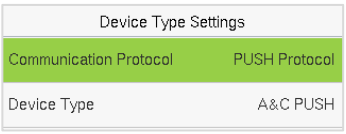




- During card management, the main menu card type will be displayed on the left and its sub-menus will be listed on the right.
- First tap on the required card type, and then select its required sub-menus from the list.

9.4 Device Type Settings

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

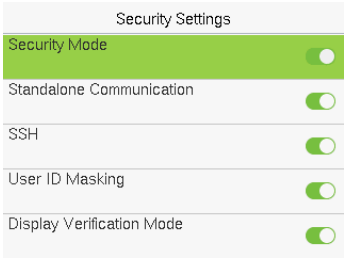


Function Name	Description
Communication Protocol	Set the PUSH protocol.
Device Type	Set the device as an access control terminal or attendance terminal.

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

9.5 Security Settings

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



Function Description

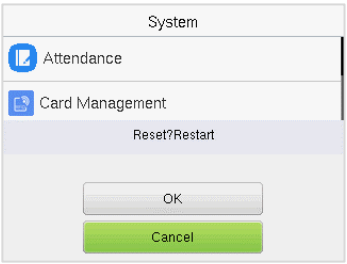
Function Name	Description
Security Mode	Select whether to enable the security mode to protect the device and the user's personal information. You can set the device to work offline and hide the user's personal information to prevent leakage during user verification.
Standalone Communication	To avoid 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 Mode	Set whether to display the verification mode in the verification result interface.

9.6 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).

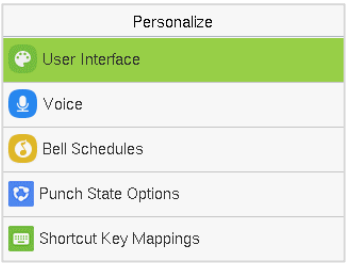
Tap **Reset** on the **System** interface and then tap **OK** to restore the default

factory settings.



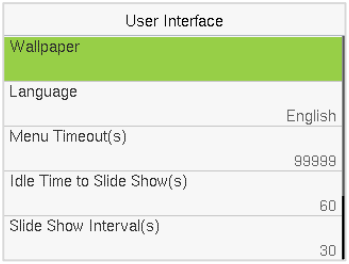
10 Personalize Settings

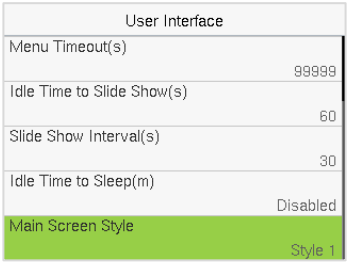
Tap **Personalize** the **Main Menu** interface to customize interface settings, voice, bell, punch state options, and shortcut key mappings.



10.1 User Interface

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





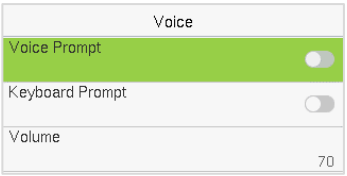
Function Description

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.

10.2 Voice

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

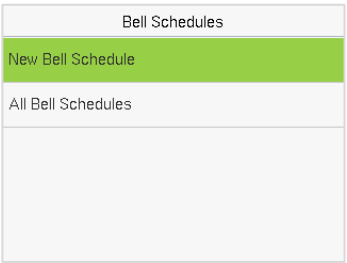


Function Description

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.

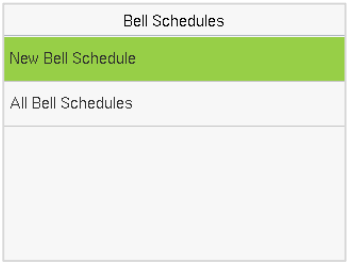
10.3 Bell Schedules

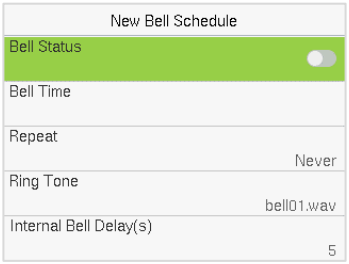
Tap **Bell Schedules** on the **Personalize** interface to configure the Bell settings.



➢ **New Bell Schedule:**

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





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:**

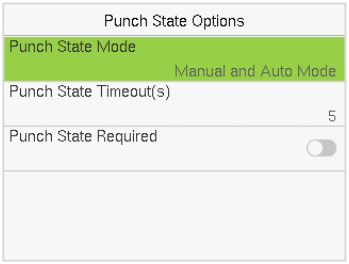
  On the **All Bell Schedules** interface, tap on the required bell schedule, and tap **Edit** to edit the selected bell schedule. The editing method is the same as the operations of adding a new bell schedule.

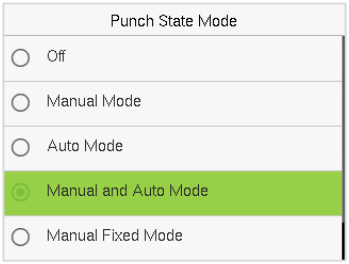
- **Delete a Bell Schedules:**

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

10.4 Punch States Options

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





Function Description

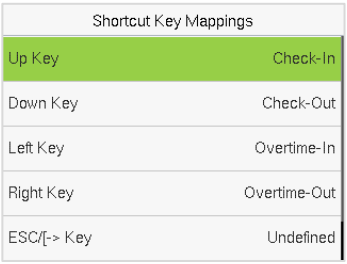
Function Name	Description
Punch State Mode	**Off:** Disable the punch state function. Therefore, the punch state key set under Shortcut Key Mappings menu will become invalid. **Manual Mode:** Switch the punch state key manually, and the punch state key will disappear after Punch State Timeout. **Auto 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.

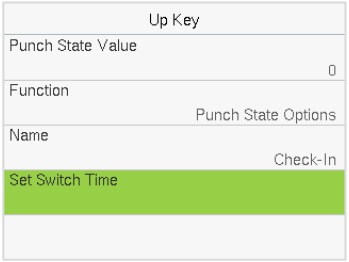
10.5 Shortcut Key Mappings

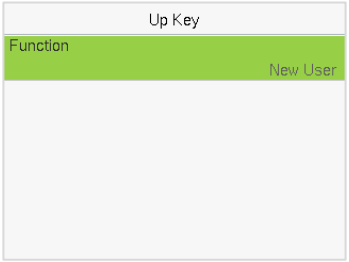
Users may define shortcut keys for attendance status and functional keys which will be defined on the main interface. So, on the main interface, when the shortcut keys are tapped, the corresponding attendance status or the function interface will be displayed directly.

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



- 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.

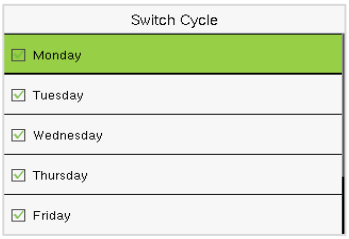


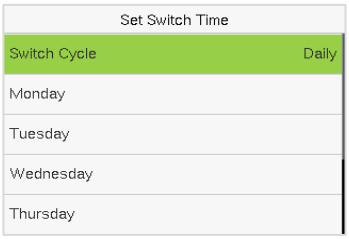


- If the Shortcut key is set as a punch state key (such as check in, check out, etc.), then it is required to set the punch state value (valid value 0 to 250), name.

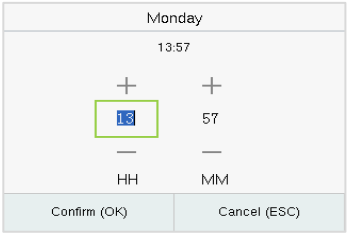
➢ **Set the Switch Time**

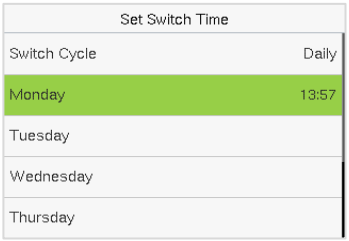
- The switch time is set in accordance with the punch state options.
- When the **Punch State Mode** is set to **Auto Mode**, the switch time should be set.
- On the **Shortcut Key** interface, tap **Set Switch Time** to set the switch time.
- On the **Switch Cycle** interface, select the switch cycle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





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

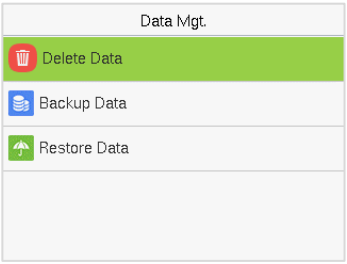




Note: When the function is set to Undefined, the device will not enable the punch state key.

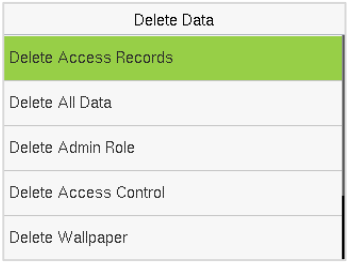
11 Data Management

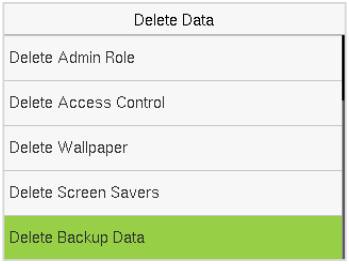
On the **Main Menu**, tap **Data Mgt.** to delete the relevant data in the device.



11.1 Delete Data

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



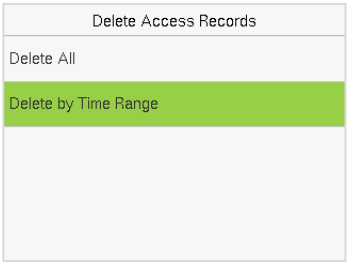


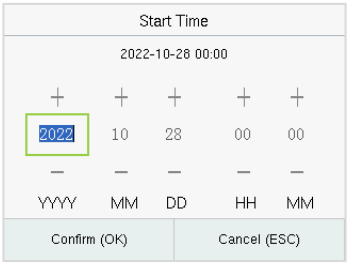
Function Description

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 & attend date, to **Delete by Time Range**, you need to set a specific time range to delete all data within a specific period.

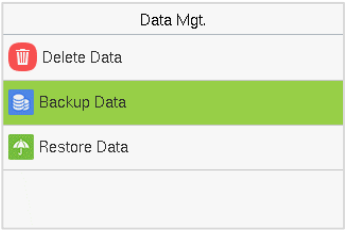




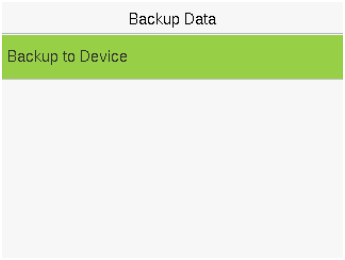
11.2 Backup Data

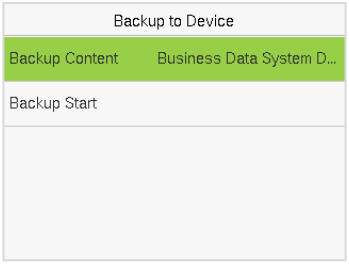
Back up the configuration data of the device to the device.

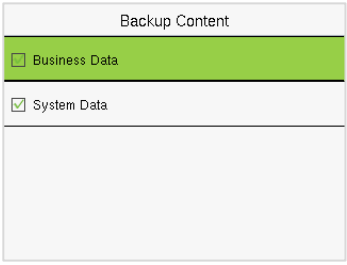
Select the **Backup Data** option on the **Data Mgt.** interface.



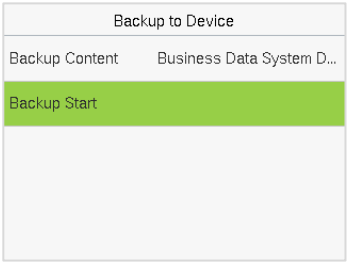
- Select the local configuration items to be back up to the device and save the selected items.

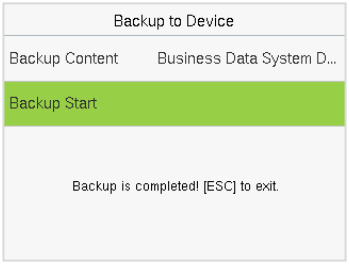






- Select **Backup Start** and tap **M/OK**.

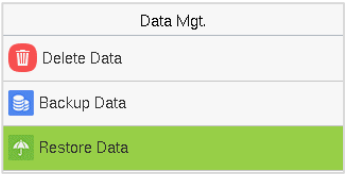




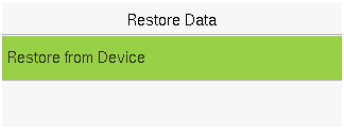
11.3 Restore Date

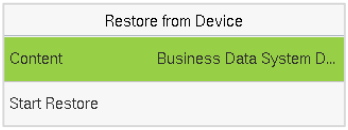
Restore the data stored on the device to the device.

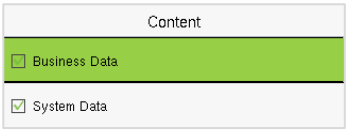
Select the **Restore Data** option on the **Data Mgt.** interface.



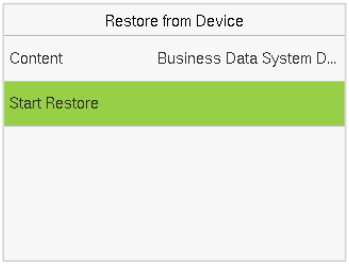
- Select the local configuration items to be restore to the device and save the selected items.

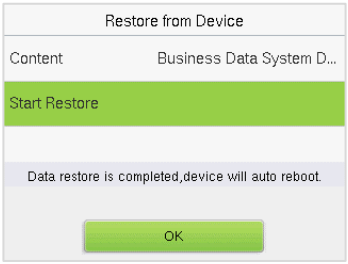






- Select **Backup Start** and tap **M/OK**.

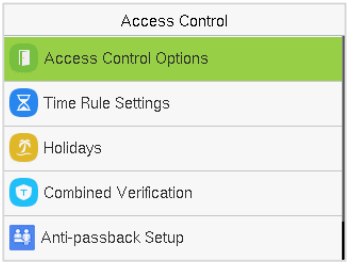


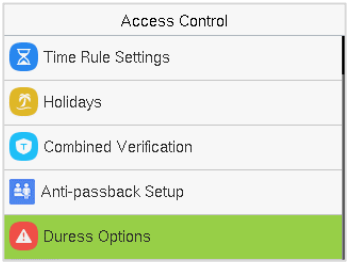


12 Access Control

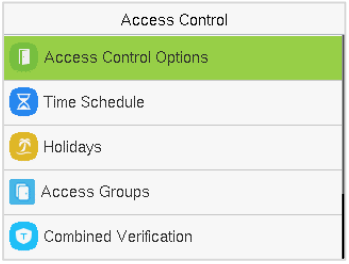
On the **Main Menu**, tap **Access Control** to set the schedule of the door opening, locks control and to configure other parameters settings related to access control.

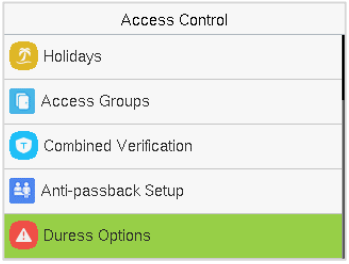
Access Control Terminal:





Time Attendance Terminal:





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

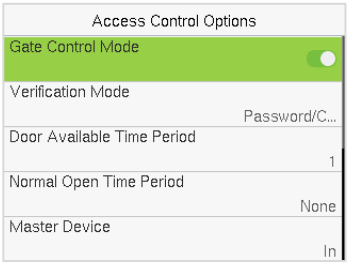
1. The relevant door's current unlock time should be within any valid time zone of the user's time period.
2. The corresponding user's group must be already set in the door unlock combination (and if there are other groups, being set in the same access combo, then the verification of those group's members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

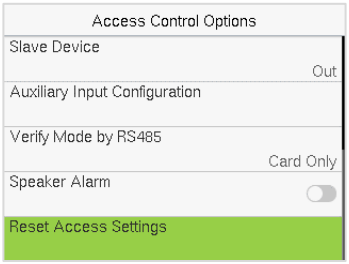
3. In default settings, new users are allocated into the first group with the default group time zone, where the access combo is "1" and is set in unlock state by default.

12.1 Access Control Options

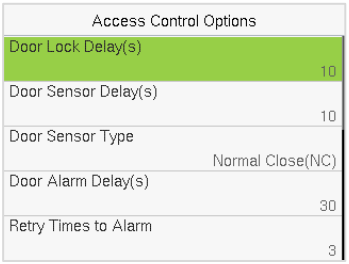
Tap **Access Control Options** on the **Access Control** interface to set the parameters of the control lock of the terminal and related equipment.

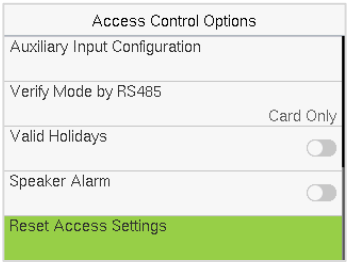
Access Control Terminal:





Time Attendance Terminal:





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.
Verification Mode	The supported verification mode includes Password/Card, User ID Only, Password, Card Only, Password + Card.
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).

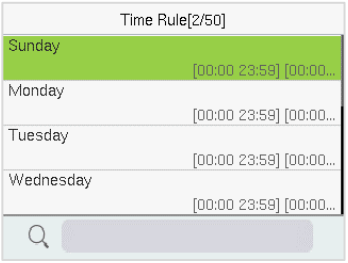
Retry Times to Alarm	When the number of failed verification reaches the set value (value ranges from 1 to 9 times), the alarm will be triggered. If the set value is None, the alarm will not be triggered after failed verification.
Auxiliary Input Configuration	Sets the door unlock time period and auxiliary 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, verification mode, door available time period, normal open time period, master device, and alarm. However, erased access control data in Data Mgt. is excluded.

12.2 Time Rule Settings and Time Schedule

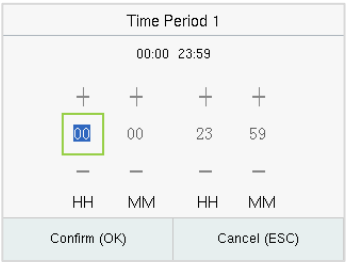
Tap **Time Rule Settings and Time Schedule** on the **Access Control** interface to configure the time settings.

- 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 H**H 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).



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**.

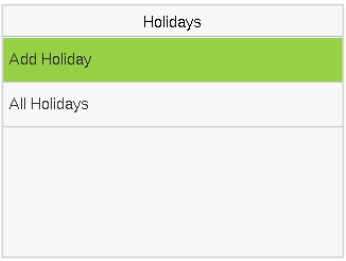
Note:

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.

12.3 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.

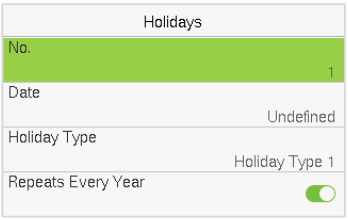
Tap **Holidays** on the **Access Control** interface to set the holiday access.



➢ **Add a New Holiday:**

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

Access Control Terminal:



Time Attendance Terminal:

➢ **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**.

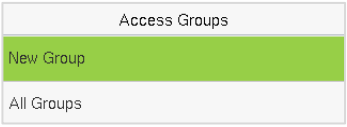
Tap **M/OK** to confirm the deletion. After deletion, this holiday does not display on the **All Holidays** interface.

12.4 Access Groups

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

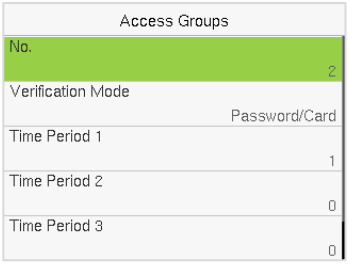
The default time zone for group members is the group time zone, while users can set their personal time zone. When the group verification mode and the user verification mode overlap, the user verification mode takes priority. Each group can set a maximum of 3 time zones; as long as one of them is valid, 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.

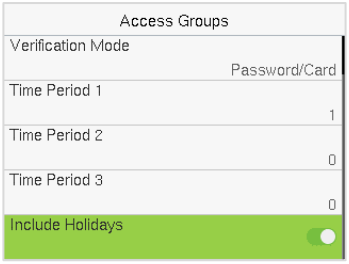
Tap **Access Groups** on the **Access Control** interface.



➢ **Add a New Holiday:**

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





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:**

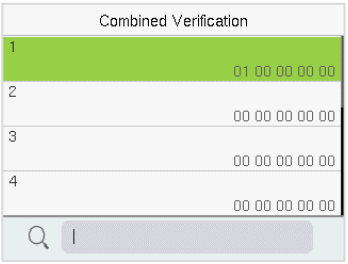
On the **All Group** interface, select a access group item to be deleted and tap **Delete**. Tap **M/OK** to confirm the deletion. After deletion, this group does not display on the **All Group** interface.

12.5 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.



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.

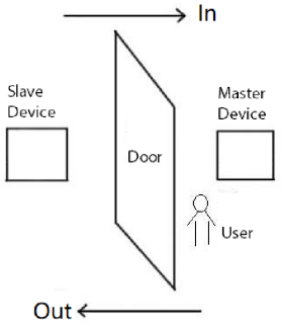
Note: To delete the door-unlock combination, set all Door-unlock combinations to 0.

12.6 Anti-passback Setup

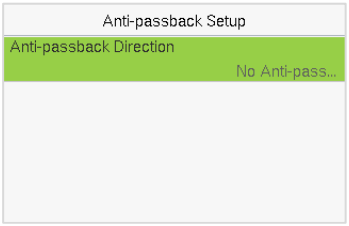
A user may be followed by some person(s) to enter the door without verification, resulting in a security breach. So, to avoid such situations, the Anti-Passback option was developed. Once it is enabled, the check-in and check-out record must occur alternatively to open the door to represent a consistent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

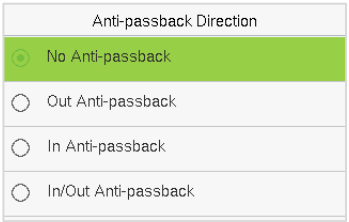
This function requires two devices to work together:

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.





Function Description:

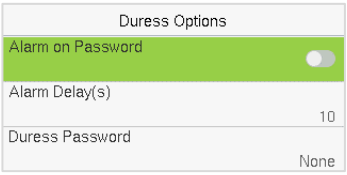
Function Name	Description
Anti-passback Direction	**No Anti-passback:** The Anti-Passback function is disabled, which means successful verification through either the master device or slave device can unlock the door. The attendance state is not saved in this option. **Out Anti-passback:** The user can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

12.7 Duress Options Settings

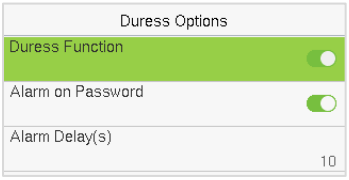
Once a user activates the duress verification function with a specific authentication method(s), and when he/she is under coercion and authenticates using duress verification, the device unlocks the door as usual. At the same time, a signal is sent to activate the alarm as well.

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

Access Control Terminal:



Time Attendance Terminal:



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 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.

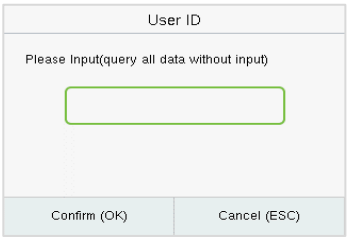
Function Description of Time Attendance Terminal:

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 Delay (s)	Alarm signal will not be transmitted until the alarm delay time is elapsed. The value ranges from 1 to 999 seconds.

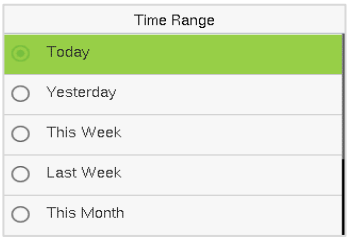
13 Attendance Search

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

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

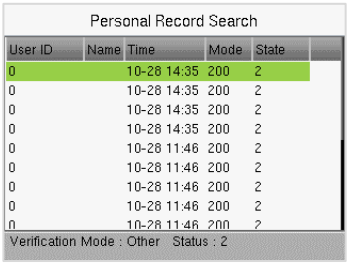


1. Enter the user ID to be searched and tap **M/OK**. If you want to search for records of all users, tap **M/OK** without entering any user ID.



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

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

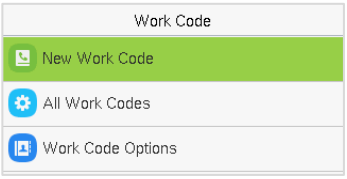


4. The figure shows the details of the selected record.

14 Work Code

Employees' salaries are subject to their attendance records. An employee can be engaged in more than one type of work which may vary with time. As the pay varies according to the work types, the FFR terminal provides a parameter to indicate the corresponding work type for every attendance record to facilitate rapid understanding of different attendance situations during the handling of attendance data.

On the **Main Menu**, tap **Work Code** to set the work code.



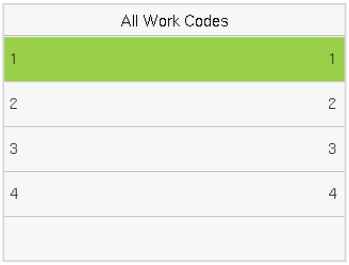
14.1 New Work Code

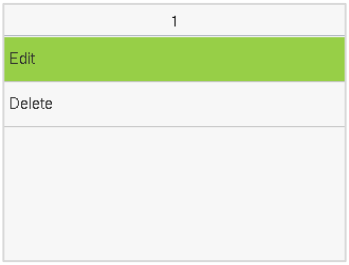
Function Description

Function Name	Description
ID	It is the digital code of the work code. Users may set a valid value between 1 and 99999999.
Name	It is the naming of the work code. Only supports input the numbers.

14.2 All Work Codes

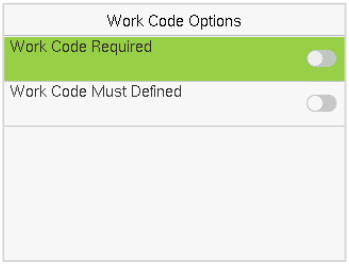
You can view, edit and delete work codes in All Work Codes. The process of editing a work code is the same as adding a work code, except that the ID is not allowed to be modified.

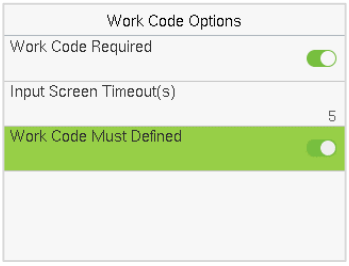




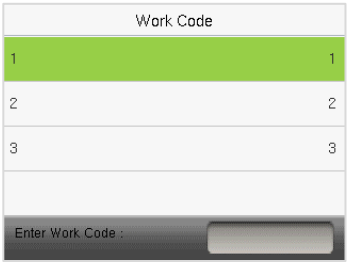
14.3 Work Code Options

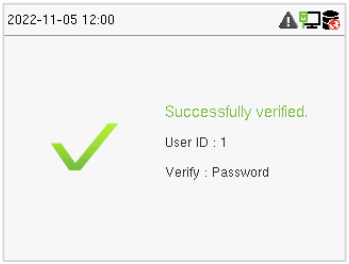
To set whether entering the work code is a must and whether the entered work code must exist during authentication.





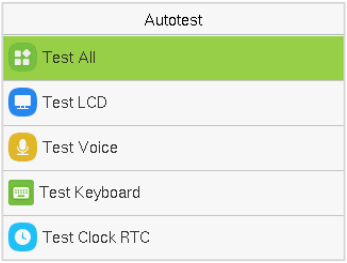
In **1: N** or **1:1** verification, the system will automatically pop up the following window. Select the corresponding Word Code manually to verify successfully.


Work Code
1
1
2
2
3
3
Enter Work Code :


2022-11-05 12:00
Successfully verified.
User ID : 1
Verify : Password

15 Autotest

Select **Main Menu**, tap on **Autotest**, it enables the system to automatically test whether the functions of various modules are working normally, including the LCD, Voice, Microphone, Fingerprint, Camera and Real-Time Clock (RTC).



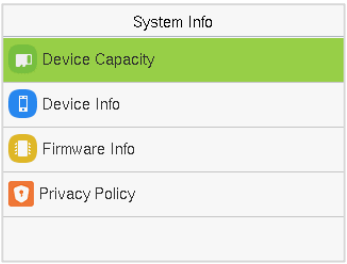
Function Description

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.
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 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.

16 System Information

On the **Main Menu**, tap **System Info** to view the storage status, the version information of the device, firmware information and the privacy policy.



Function Description

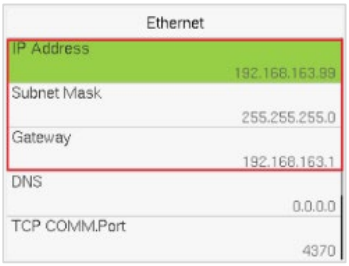
Function Name	Description
Device Capacity	Displays the current device's user storage, card and password storage, administrators and records.
Device Info	Displays the device's name, serial number, MAC address, Platform information, MCU Version, Manufacturer, and manufacture date.
Firmware Info	Displays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

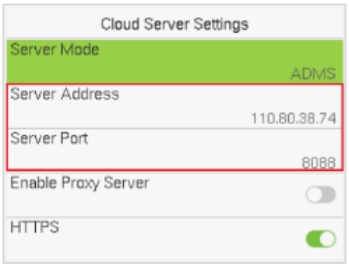
17 Connect to ZKBio Access IVS Software

17.1 Set the Communication Address

➢ **Device side:**

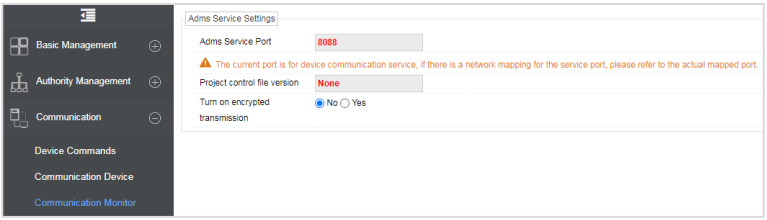
1. Tap **COMM.** > **Ethernet** in the main menu to set the IP address and gateway of the device.
   (***Note:*** The IP address should be able to communicate with the ZKBio Access IVS server, preferably in the same network segment with the server address).
2. In the main menu, click **COMM.** > **Cloud Server Setting** to set the server address and server port.
   Server address: Set the IP address as of ZKBio Access IVS server.
   Server port: Set the server port as of ZKBio Access IVS (The default is 8088).





➢ **Software side:**

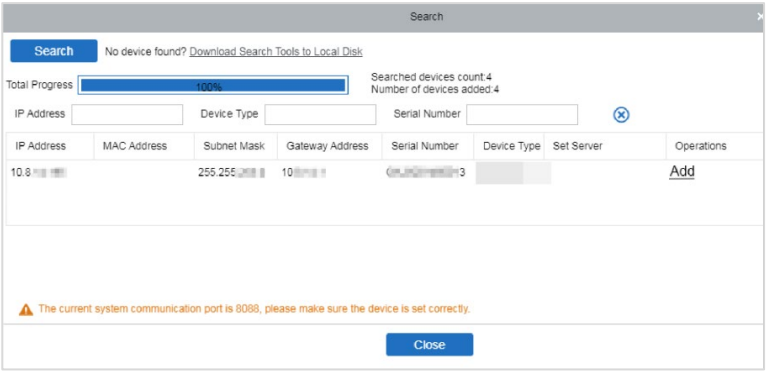
Login to ZKBio Access IVS software, click **System** > **Communication** > **Communication Monitor** to set the ADMS service port, as shown in the figure below:



17.2 Add Device on the Software

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

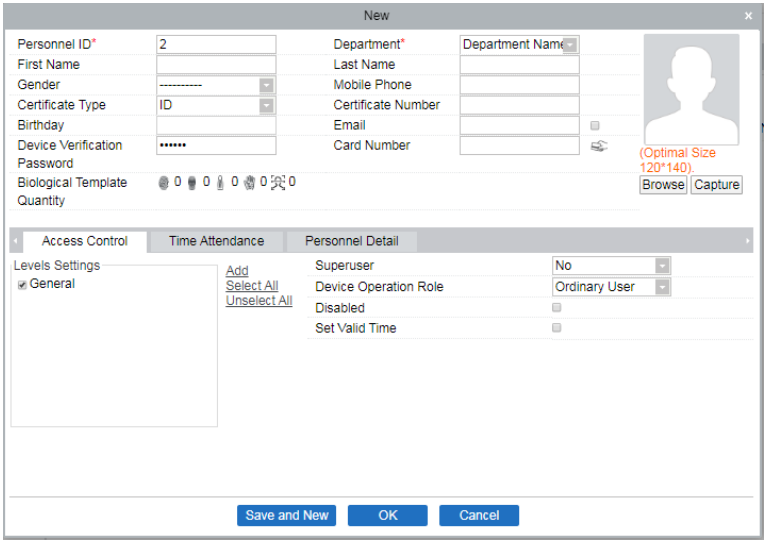
1. Click **Access Control** > **Device** > **Search Device**, to open the Search interface in the software.
2. Click Search, and it will prompt [**Searching……**].
3. After searching, the list and total number of access controllers will be displayed.



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

17.3 Add Personnel on the Software

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

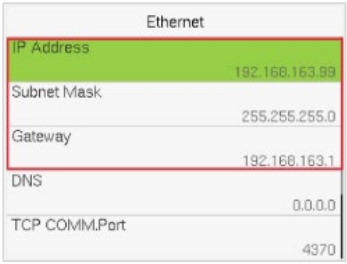


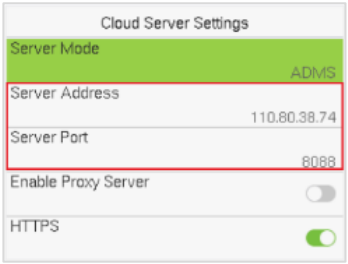
2. Fill in all the required fields and click [**OK**] **to register a new user.**
3. Click **Access** > **Device** > **Device Control** > **Synchronize All Data to Devices** to synchronize all the data to the device including the new users.

18 Connect to BioTime 8.0 Software

18.1 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.

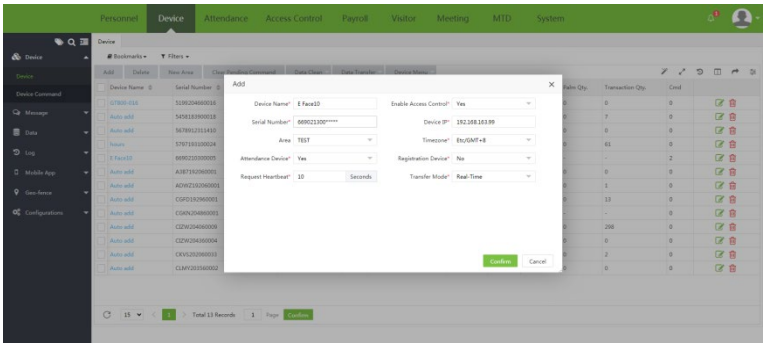




18.2 Add Device on the Software

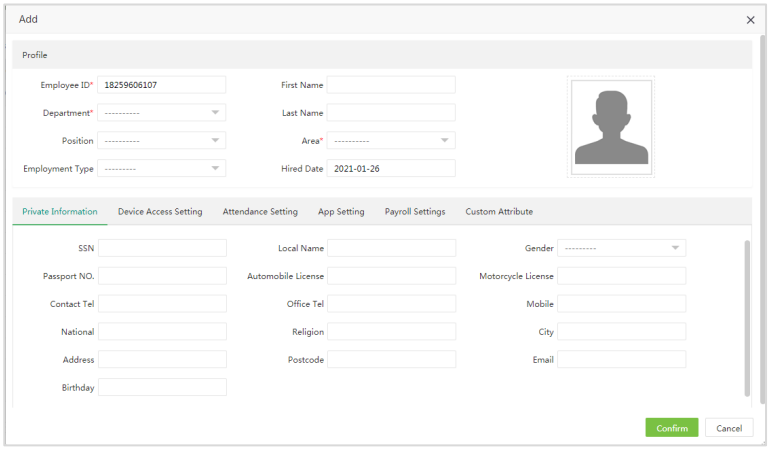
Add the device by searching. The process is as follows:

1. Click **Device** > **Device** > **Add**, to add the device on the software.
2. A new window pops-up on clicking [**Add**]. Enter the required information about the device and click [**Confirm**], then the added devices are displayed automatically.



18.3 Add Personnel on the Software

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

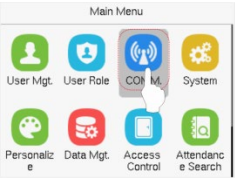


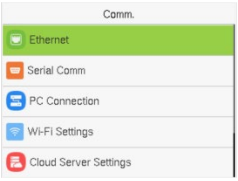
2. Fill in all the required fields and click [**Confirm**] to register a new user.
3. Click **Device** > **Device** > **Data Transfer** > **Sync Data to Device** to synchronize all the data to the device including the new users.

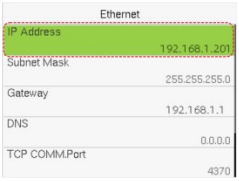
19 Connect to WebServer

19.1 Login WebServer

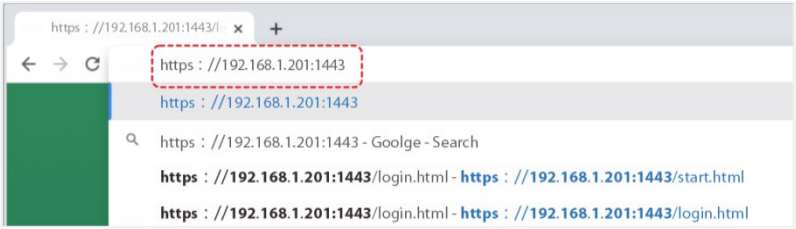
According to the configured network login, allows the Webserver to remotely view the information of the device (hardware, software, capacity and data, etc.), set up the system (communication, access control and system functions, etc.), add users and upgrade the system.

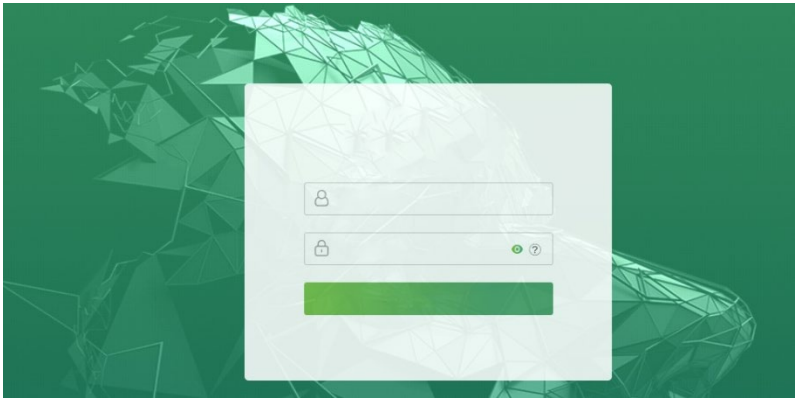




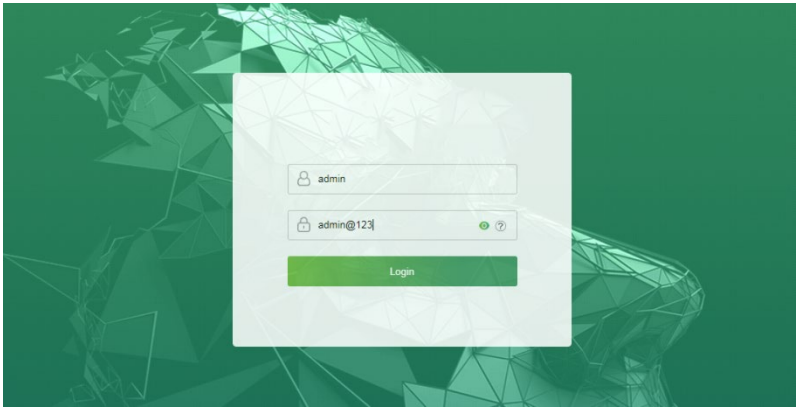


1. Open a browser and enter the address to log in to the WebServer; the address is https:// **Serial IP Address:1443**. For example: **https://192.168.1.201:1443**.





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



Note:

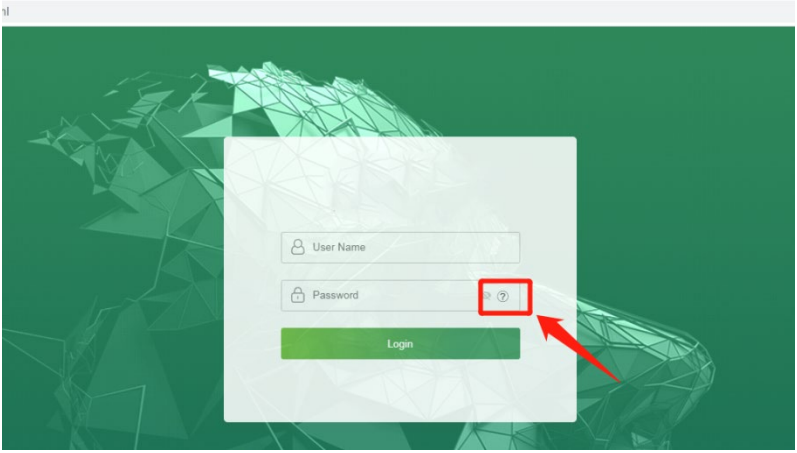
1. After logging in for the first time, users must need to change their default password and log in again before they can use it, please refer to Change Password.
2. To retrieve the password easily, please register a super admin first, please refer to User Registration.

19.2 Forgot Password

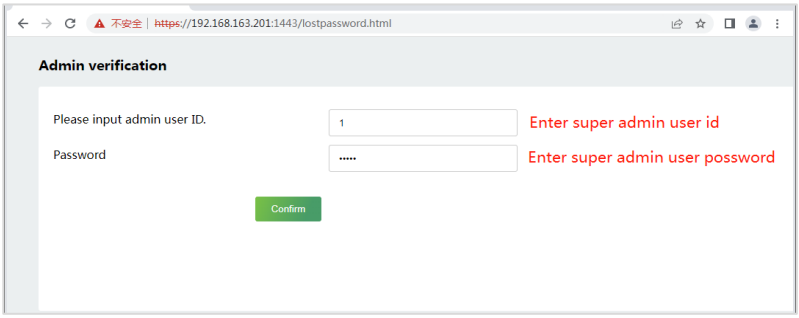
➢ **Method 1 (When there is a super admin):**

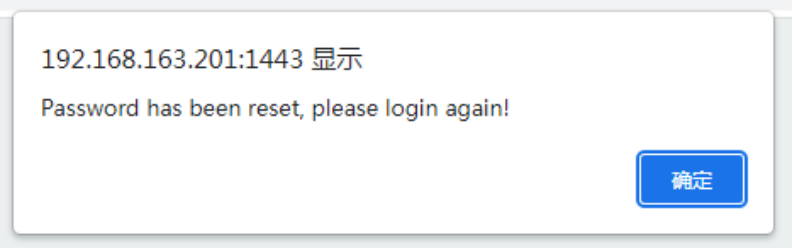
If you forget your WebServer password, the registered super admin can reset it for you. The detailed steps are as follows:

1. Click the icon on the login interface.

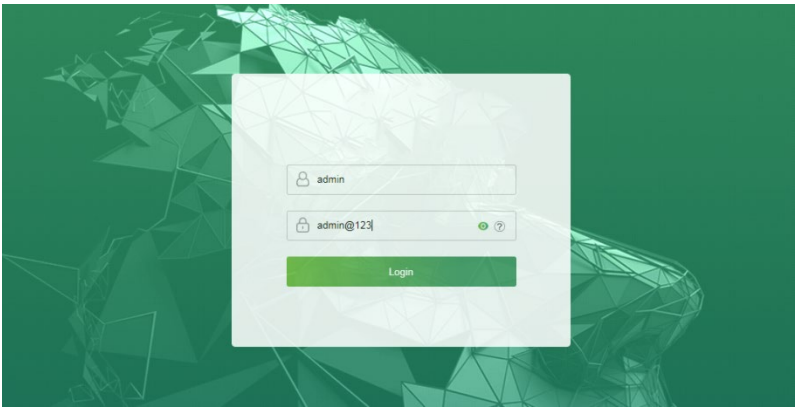


2. On the pop-up page, enter the relevant information of the super admin user as prompted.

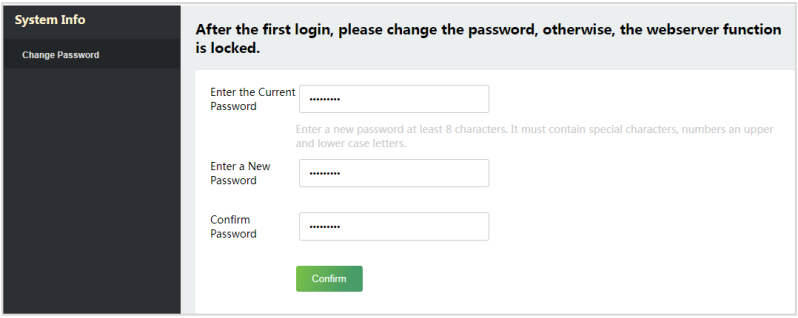




3. After a successful reset, enter the default user name and password (user name: **admin** and password: **admin@123**) on the login interface to log in.



4. After successfully logging in, please change your password for security reasons.

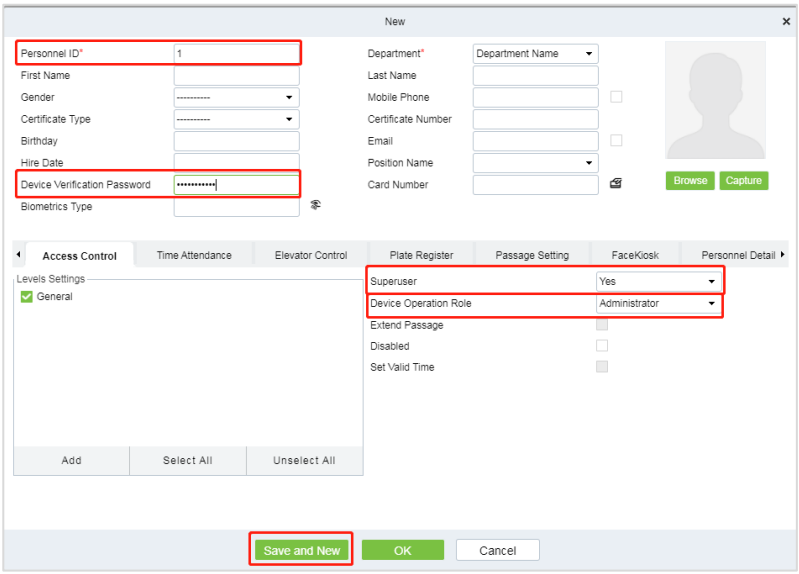


Note: The super admin must exist.

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

If the network of the device is normal and ZKBio Access IVS / 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 Access IVS / ZKBioTime 8.0 Server; register the super admin information and set the super admin role on the new interface as required.



2. After registering the information of the super admin, click **Save and New**.
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 Access IVS 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.

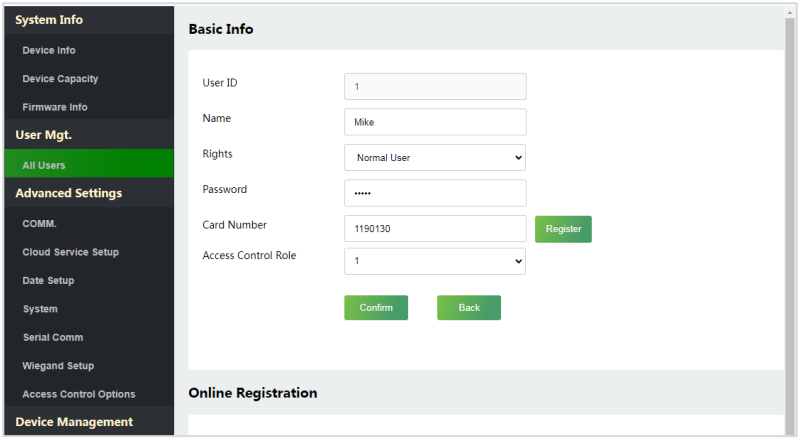
➢ **Method 3:**

If the device has not registered a super admin and is unable to connect to the server, please contact our after-sales personnel for assistance in resetting the password.

19.3 User Registration

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

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



Function Name	Description
User ID	The default user ID can have 1 to 14 digits.
Name	A name can be up to 63 characters. The device only supports the input of numbers, you can add a user name by this method.

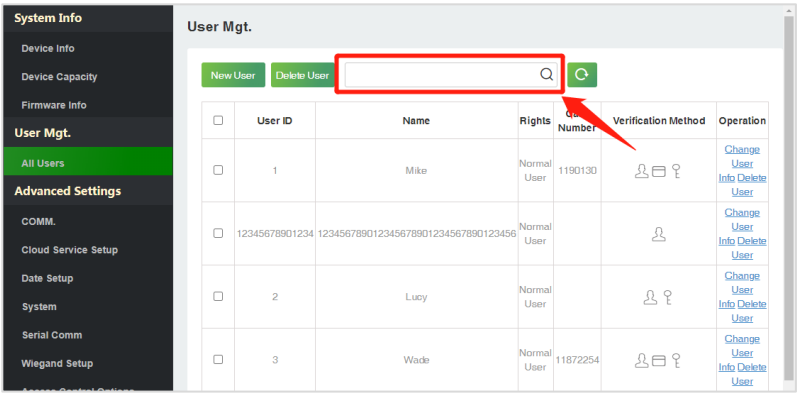
Rights	Set the role for the user as either Normal User or Super Admin. • **Super Admin:** The Super Admin owns all management privileges in the WebServer. • **Normal User:** If the Super Admin is already registered in the WebServer, then the Normal Users will not have the privileges to manage the system and can only access authentication verifications.
Password	Set the user's registration password.
Card Number	Enter the card number manually, after registering the user's card number, the user can swipe the card for verification. Also can click **Register**, and the device will display the card registration interface in real time, swipe the card underneath the card reading area. The registration of the card will be successful.
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 "**Setup failed!**" pops up, you must choose a different User ID because the one you entered already exists.

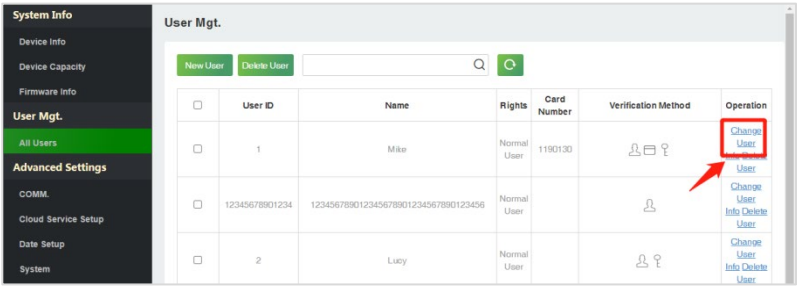
19.4 Search for Users

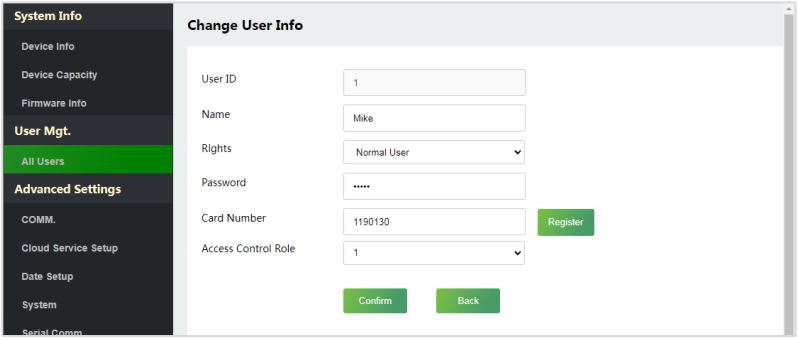
Click **All Users** on the WebServer, click the **Search Bar** to enter the required retrieval keyword (which the keyword can be the user ID, surname or full name) and the system will search for the related user information.



19.5 Edit User

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

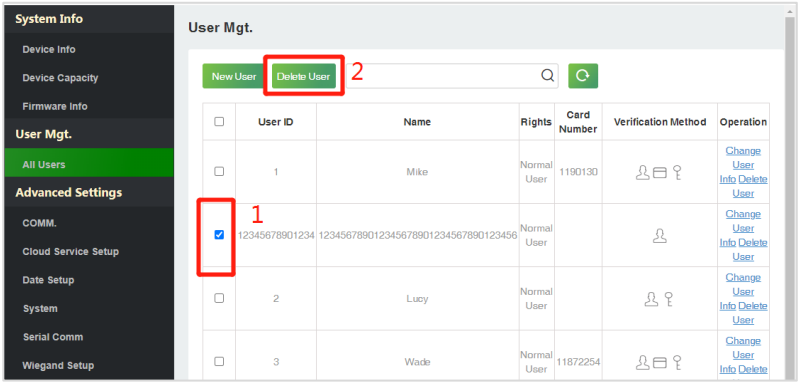




Note: The process of editing the user information is the same as that of adding a new user, except that the User ID cannot be modified. The process in detail refers to User Registration.

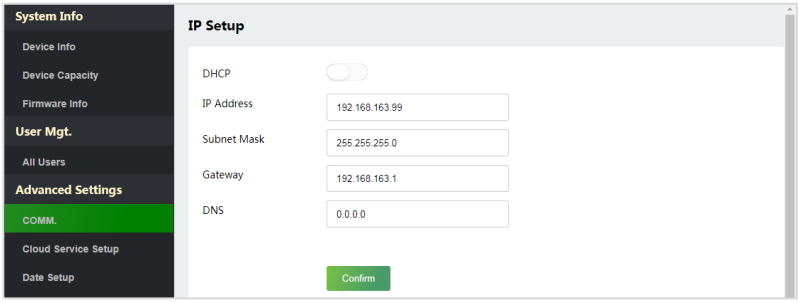
19.6 Delete User

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.



19.7 COMM.

Click **COMM.** on the WebServer, then change the IP address of the device as needed, click **Confirm** to save, and the device will automatically synchronize the IP information.



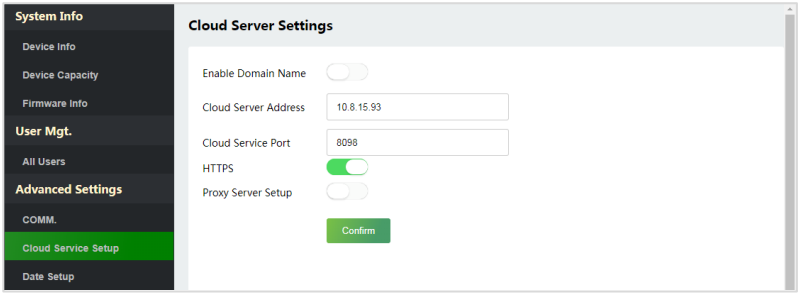
Function Name	Description
DHCP	Dynamic Host Configuration Protocol dynamically allocates IP addresses for clients via server.
IP Address	The default IP address is 192.168.1.201. It can be modified according to network availability.
Subnet Mask	The default Subnet Mask is 255.255.255.0. It can be modified 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 successfully changing the device's IP address, you must log out of the existing WebServer and log back into the IP address you just changed to connect to the device. For WebServer login details, please refer to Login WebServer.

19.8 Cloud Server Settings

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

Cloud Server Setup was used to connect to the ZKBio Access IVS and ZKBioTime8.0, please refer to set the communication address.



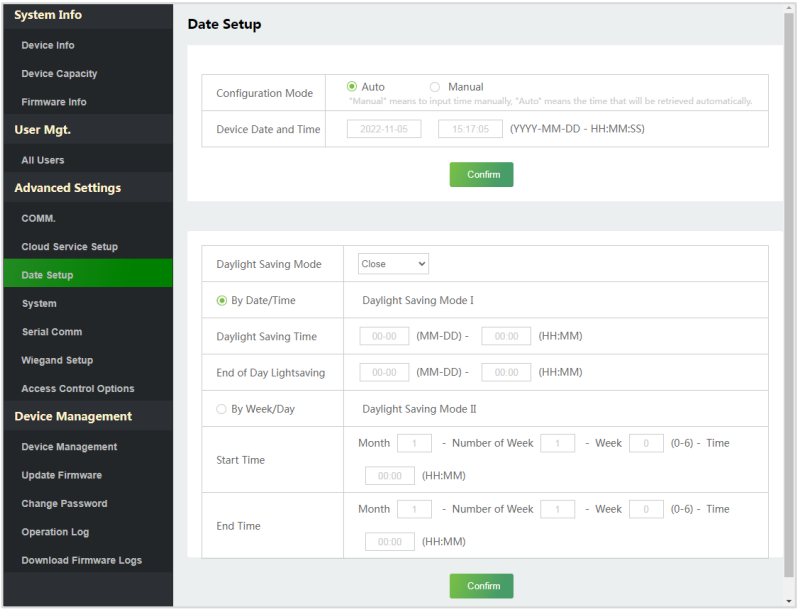
Function Name	Description	
Enable Domain Name	**Server Address**	Once this function is enabled, the domain name mode "http://..." will be used, such as http://www.XYZ.com, while "XYZ" denotes the domain name (when this mode is turned ON).
Disable Domain Name	**Cloud Server Address**	IP address of the ADMS server.

	Cloud Server Port	Port used by the ADMS server.
HTTPS	Based on HTTP, transmission encryption and identity authentication ensure the security of the transmission process.	
Proxy Server Setup	When you choose to enable the proxy, you need to set the IP address and port number of the proxy server.	

19.9 Date Setup

Click **Date Setup** on the WebServer.

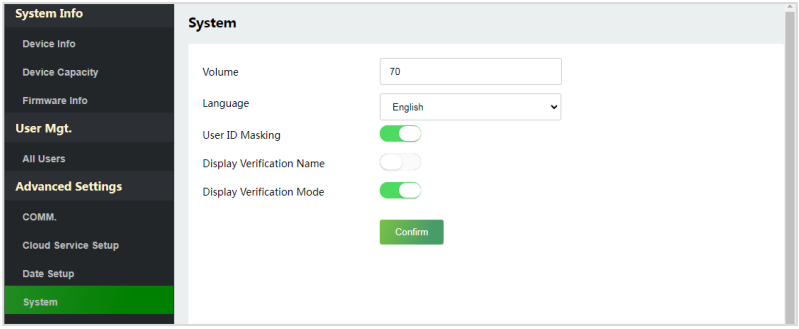
- Click **Manual** to manually set the date and time and click **Confirm** to save.
- Select Open or Close the **Daylight Saving Mode** function. If opened, set the **Daylight Saving Time** and **End of Daylight Saving**.



19.10 System

Click **System** on the WebServer.

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



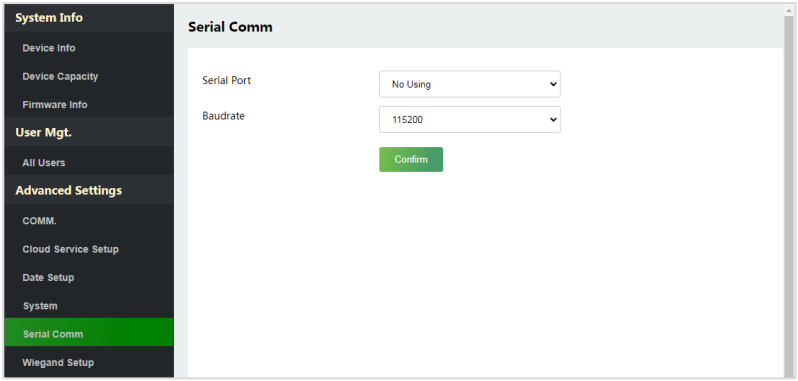
Function Name	Description
Volume	Adjust the volume of the device which can be set between 0 and 100.
Language	Select the language of the WebServer and device.
User ID Masking	When enabled, and then the user is successfully compared and verified, the User ID in the displayed verification result will be 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.

Note:

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

19.11 Serial Comm

Click **Serial Comm** on the WebServer.



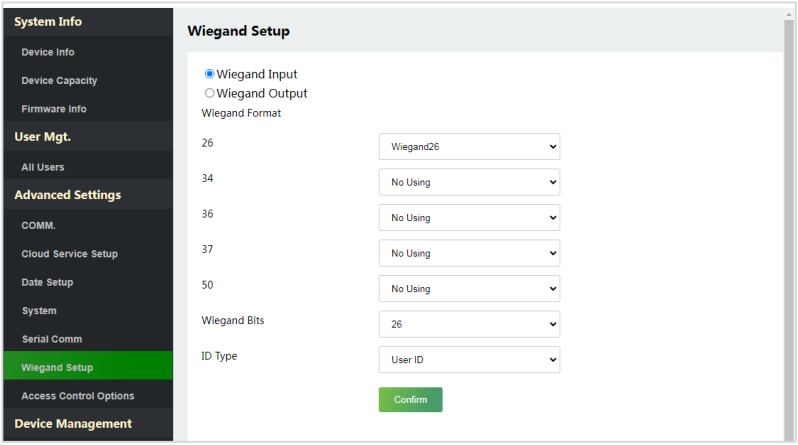
Function Name	Description
Serial Port	**No Using:** No communication with the device through the serial port. **Master Unit:** When OSDP is used as the function of "**Master unit**", it can be connected to a card reader. **OSDP Output:** Communicate with the device through the OSDP serial port.
Baudrate	There are 5 baudrate options at which the data communicates with the PC. They are: 115200 (default), 57600, 38400, 19200 and 9600. 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.

19.12 Wiegand Setup

Click **Wiegand Setup** on the WebServer.

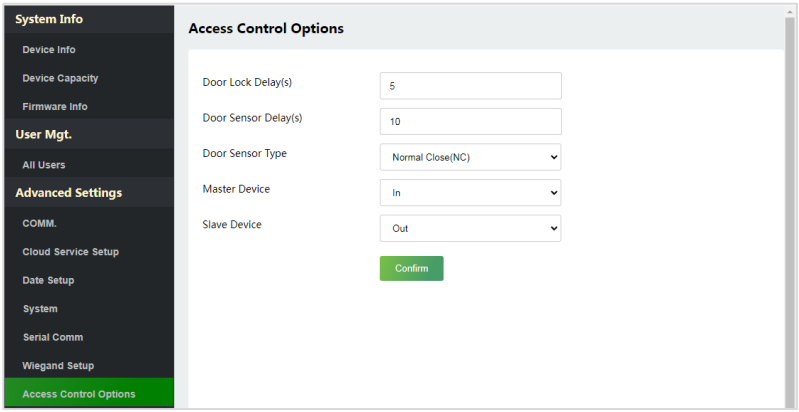
It is used to set the Wiegand input and output parameters.



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.

19.13 Access Control Options

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

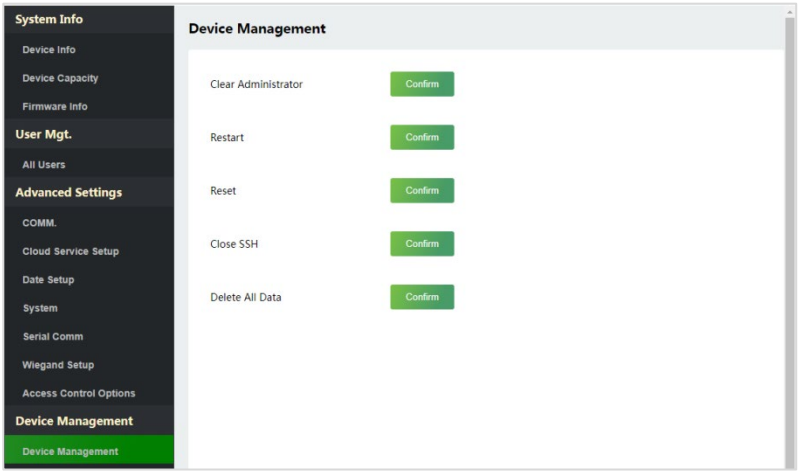


Function Name	Description
Door Lock Delay (s)	The length of time that the device controls the electric lock to be in unlock state. Valid value: 1 to 99 seconds.
Door Sensor Delay (s)	If the door is not locked and is left open for a certain duration (Door Sensor Delay), an alarm will be triggered. The 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.
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.

19.14 Device Management

Click **Device Management** on the WebServer.



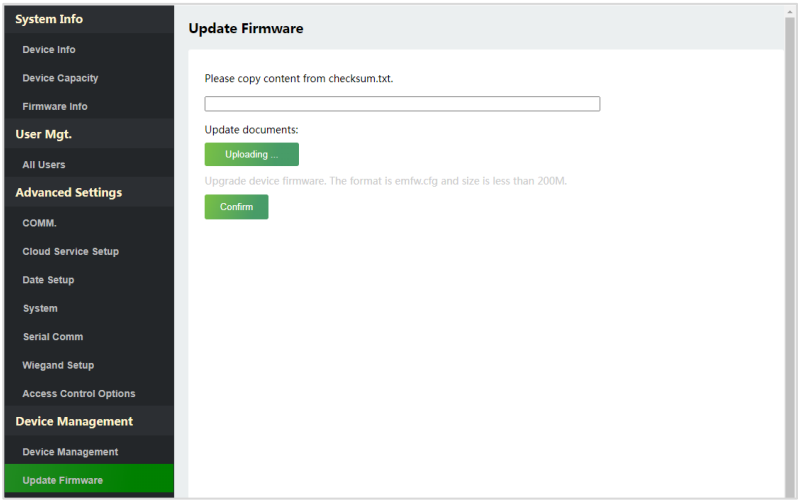
Function Name	Description
Clear Administrator	Choose whether to change the super administrator into a normal user.
Restart	Choose whether to restart the device.
Reset	The Reset function restores the device settings such as communication and system settings to the default factory settings (this function 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 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.

19.15 Update Firmware

Click **Update Firmware** on the WebServer.

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

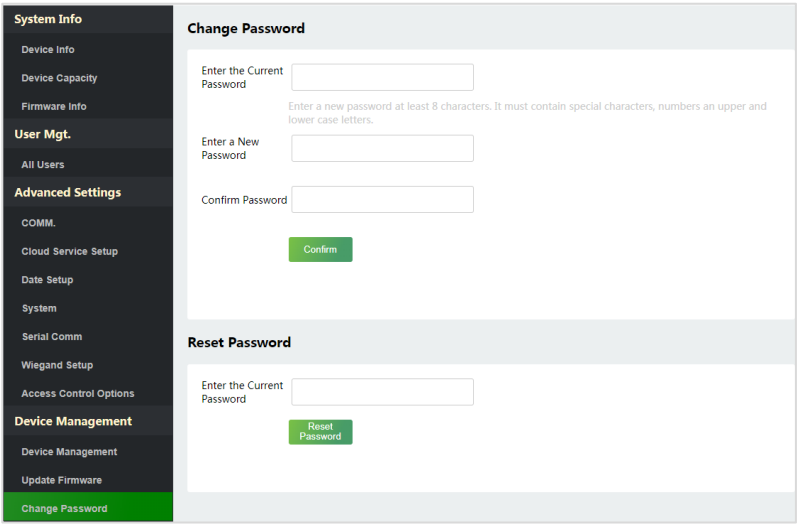


Note: If the upgrade file is needed, please contact our technical support. Firmware upgrade is not recommenced under normal circumstances.

19.16 Change Password

Click **Change Password** on the WebServer.

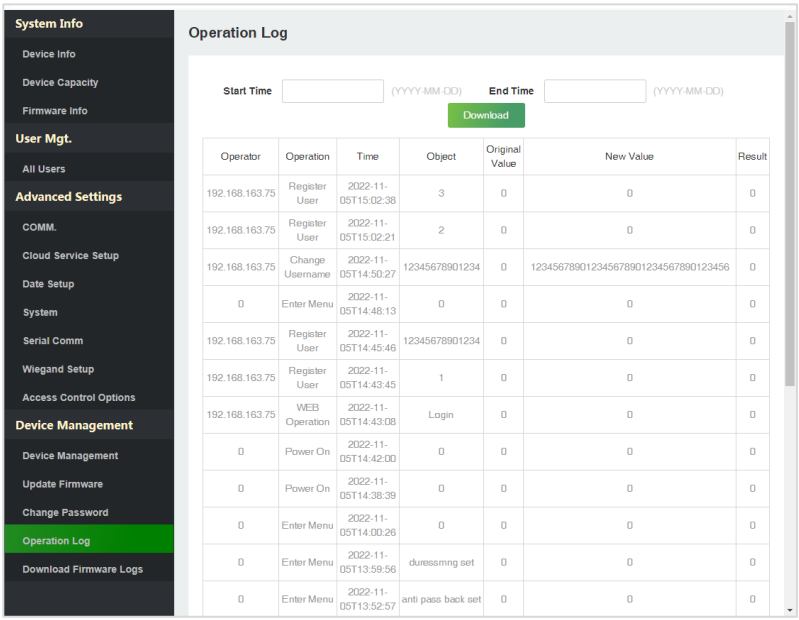
In this interface, you can change the password and reset the password of WebServer.



19.17 Operation Log

Click **Operation Log** on the WebServer.

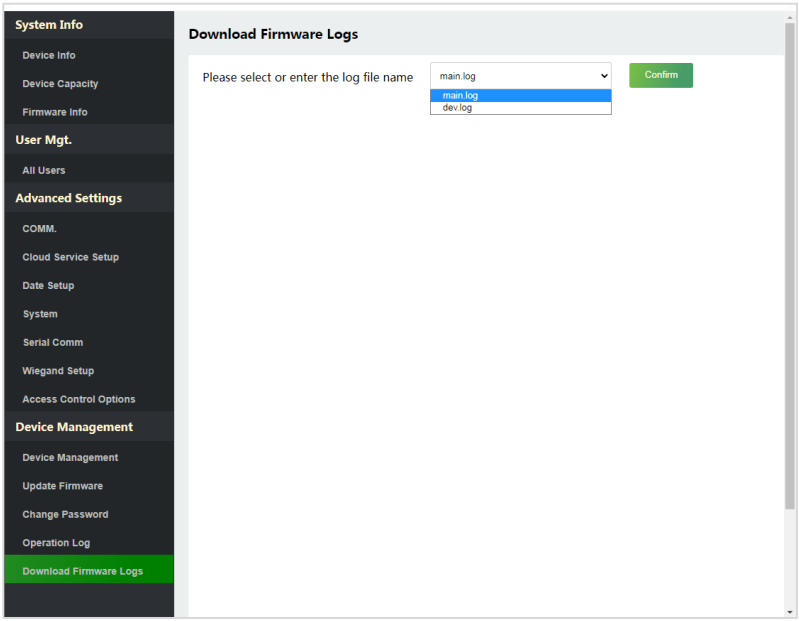
All the user's operation records on the device or WebServer are saved. Users can search and download these logs by time.



19.18 Download Firmware Logs

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

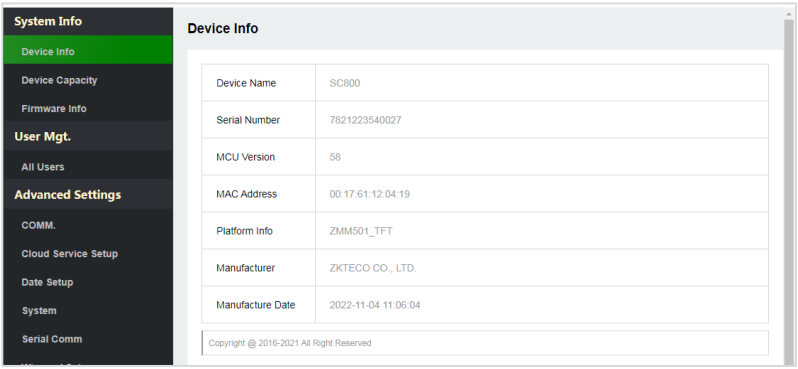
In this interface, you can select download the main, biometric, or dev.log.

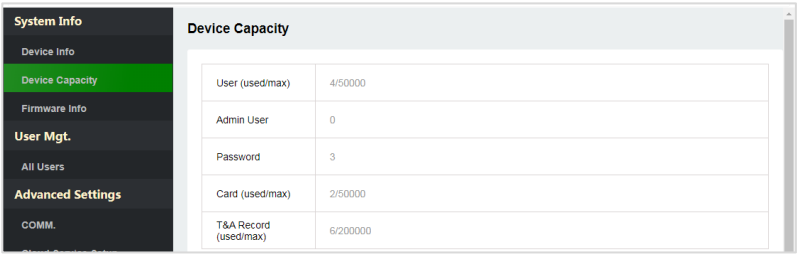


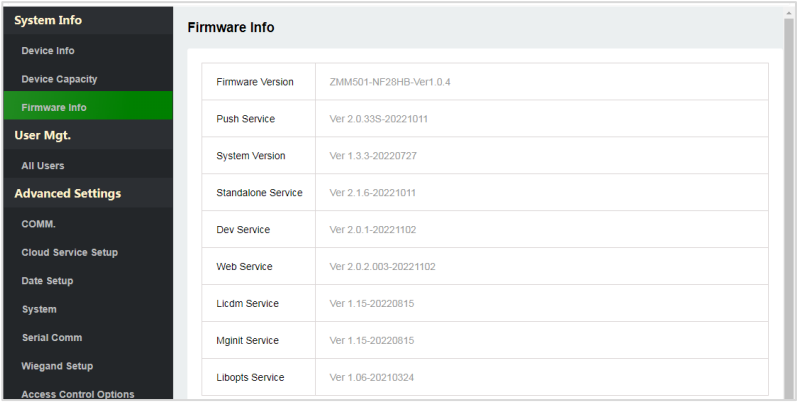
19.19 System Information

Click **System Information** on the WebServer.

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


System Info
Device Info
Device Capacity
Firmware Info
User Mgt.
All Users
Advanced Settings
COMM.
Cloud Service Setup
Date Setup
System
Serial Comm
Device Info
Device Name SC800
Serial Number 7821223540027
MCU Version 58
MAC Address 00:17:61:12:04:19
Platform Info ZMM501_TFT
Manufacturer ZKTECO CO., LTD.
Manufacture Date 2022-11-04 11:06:04
Copyright @ 2016-2021 All Right Reserved


System Info
Device Info
Device Capacity
Firmware Info
User Mgt.
All Users
Advanced Settings
COMM.
Device Capacity
User (used/max) 4/50000
Admin User 0
Password 3
Card (used/max) 2/50000
T&A Record (used/max) 6/200000


System Info
Device Info
Device Capacity
Firmware Info
User Mgt.
All Users
Advanced Settings
COMM.
Cloud Service Setup
Date Setup
System
Serial Comm
Wiegand Setup
Access Control Options
Firmware Info
Firmware Version ZMM501-NF28HB-Ver1.0.4
Push Service Ver 2.0.33S-20221011
System Version Ver 1.3.3-20220727
Standalone Service Ver 2.1.6-20221011
Dev Service Ver 2.0.1-20221102
Web Service Ver 2.0.2.003-20221102
Licdm Service Ver 1.15-20220815
Mginit Service Ver 1.15-20220815
Libopts Service Ver 1.06-20210324

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

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

FCC Warning:
Any Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
-Reorient or relocate the receiving antenna.
-Increase the separation between the equipment and receiver.
-Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
-Consult the dealer or an experienced radio/TV technician for help.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator

No.32,Pingshan Industrial Avenue,Tangxia Town,
Dongguan City,Guangdong Province,China 523728

Phone : +86 769 - 82109991

Fax : +86 755 - 89602394

www.zkteco.com

Copyright © 2022 ZKTECO CO., LTD. All Rights Reserved.