USER MANUAL

Facial Access Control Terminal

Version: 1.0
Date: July, 2015

About This Document

This document introduces the interfaces and menu function operations of the facial access control terminal product.

About This Manual

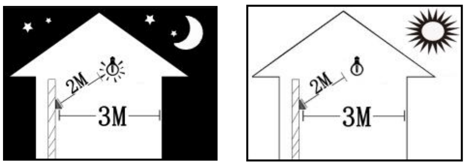
- This manual introduces the operation of user interfaces and menu functions.
- The pictures in this manual may not be exactly consistent with those of your product; the actual product's display shall prevail.

Contents

1 Use Instructions

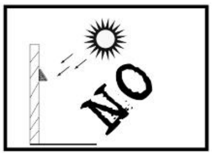
1.1 Operating Environment of the Device

Recommended Installation Position

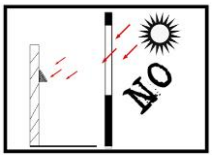


√ Recommended installation position (as shown in the left figure):
Install the device in an indoor position which is three meters far from the window and door and two meters far from the lamp source, with illuminance of ambient light source being 0-800 LUX.

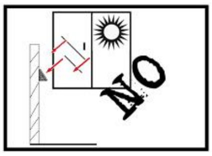
2) Several Installation Positions Affecting Application Effect



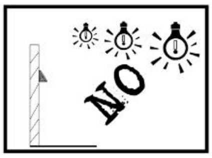
Direct sunlight
(Outdoor)



Direct sunlight through
the window
(Indoor)

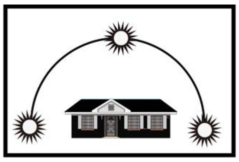


Oblique sunlight
through the window
(Indoor)



Exposure to close
range lamp light
(Indoor)

10Lux



Lager than 1200 Lux

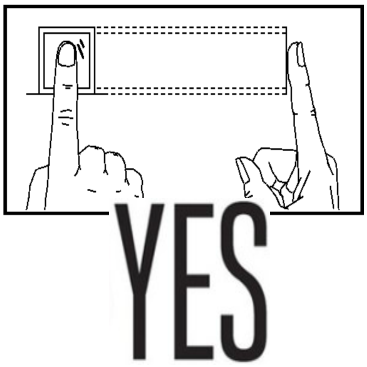
50-800Lux

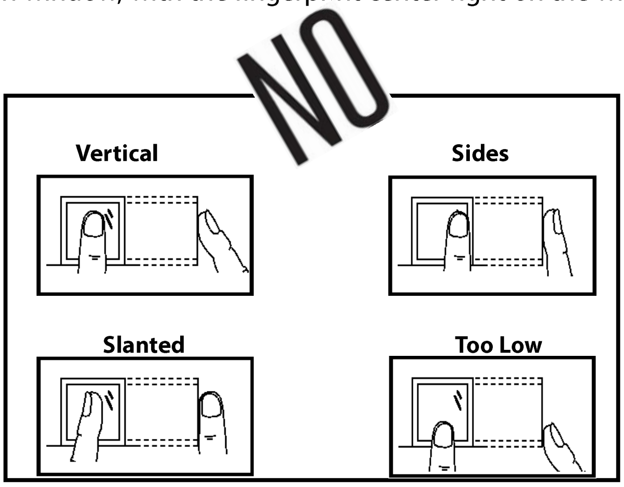
Note: reference illuminance value of the ambient light source:

1.2 Method of Pressing Fingerprint

It is recommended to use the index finger, middle finger or ring finger; avoid using the thumb or little finger.

Press a figure flatly against the fingerprint collection window, with the fingerprint center right on the window center.

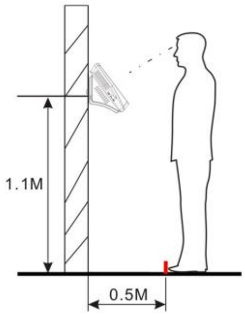




1.3 Standing Position, Facial Expression and Stance

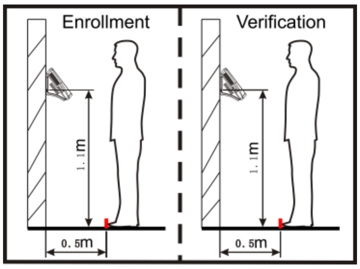
1. Recommended Standing Position

√ The distance between a person and the device is recommended to be 0.5 meters (applicable height range from 1.5–1.8 meters). The distance can be adjusted based on the effect of facial image captured by the device.

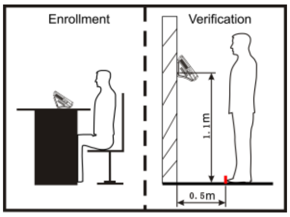


Recommended Application Position

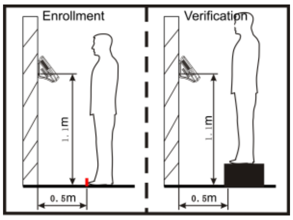
√ Recommended application method (as shown in the left figure): During enrollment and verification, the device installation position must be kept unchanged. If you really need to move the device, keep the installation height unchanged. Otherwise, the recognition effect of the equipment may be compromised.



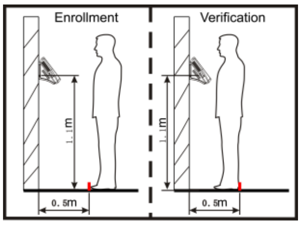
Several application methods affecting recognition effect



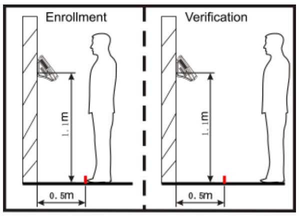
Too high



Too low

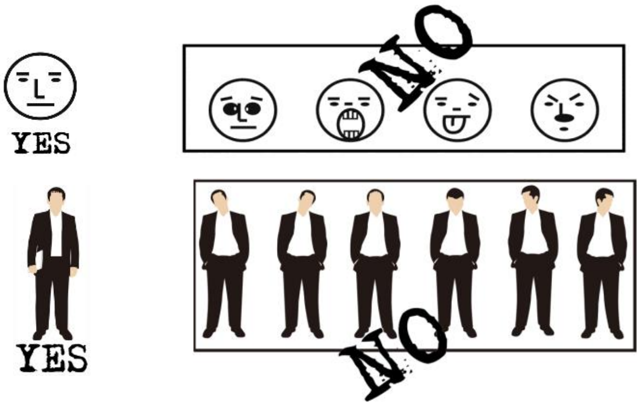


Too close



Too far

2. Facial Expression and Stance

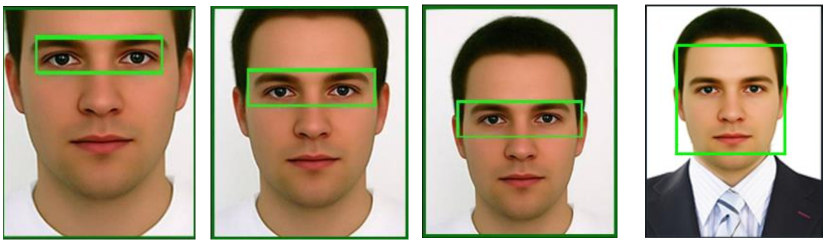


Note: During enrollment and verification, keep the facial expression and stance natural.

3. Posture for Enrollment and Comparison

During enrollment, you need to move forward or backward to ensure that your eyes are within the green frame.

During comparison, ensure that the face is displayed in the center of the screen and is within the green frame.

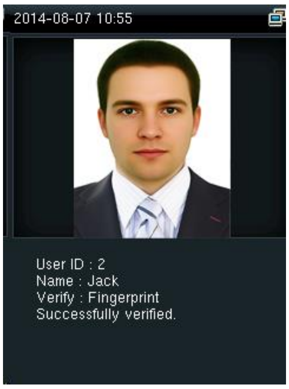


1.4 Verification Modes

1.4.1 1:N Fingerprint Verification

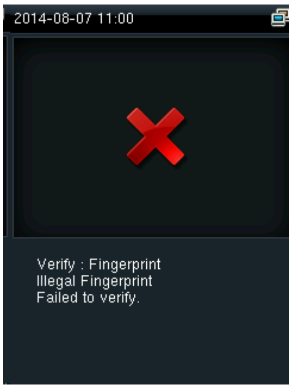
Under this fingerprint verification method, a fingerprint collected by the sensor is verified with all fingerprints stored in the device.

Please use the correct way to press fingerprint onto the fingerprint sensor (for detailed instruction, please refer to 1.2 Method of Pressing Fingerprint.



2014-08-07 10:55

User ID : 2
Name : Jack
Verify : Fingerprint
Successfully verified.



2014-08-07 11:00

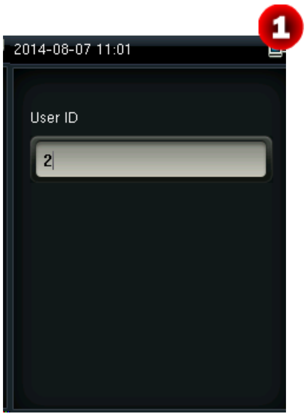
Verify : Fingerprint
Illegal Fingerprint
Failed to verify.

Verification Succeeds

Verification Fails

1.4.2 1:1 Fingerprint Verification

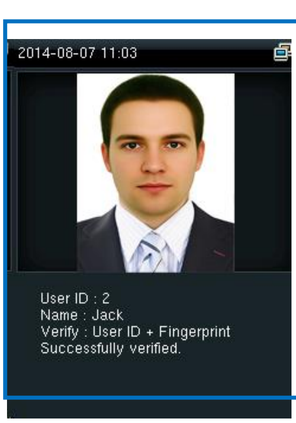
Under this fingerprint verification method, a fingerprint collected by the sensor is verified with the fingerprint corresponding to the entered user ID. Please use this method when difficulty is encountered in 1:N fingerprint verification.



2014-08-07 11:01

User ID

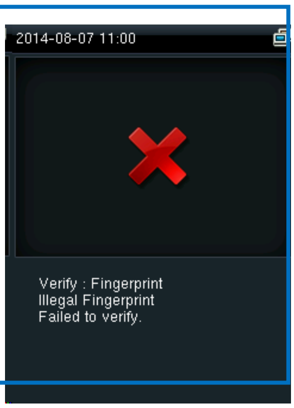
2



2014-08-07 11:03

User ID : 2
Name : Jack
Verify : User ID + Fingerprint
Successfully verified.

Or



2014-08-07 11:00

Verify : Fingerprint
Illegal Fingerprint
Failed to verify.

Input the user ID and press [M/OK] "Fingerprint" and press [M/OK]. Press finger onto the sensor afterwards.

Verification succeeds

Verification fails

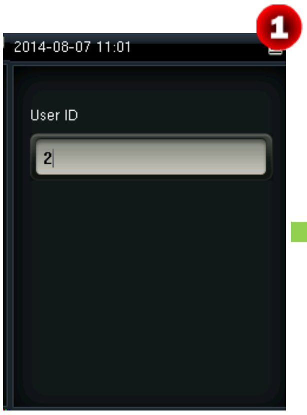
☺Remarks:

1. Input user ID in the initial interface and press [M/OK] button. If "Incorrect user ID"is displayed, this means the user ID does not exist.

2. When the device displays "please press your finger again" press your finger again onto the fingerprint sensor. If verification still fails after 2 attempts, it will exit to the initial interface.

1.4.3 Password Verification

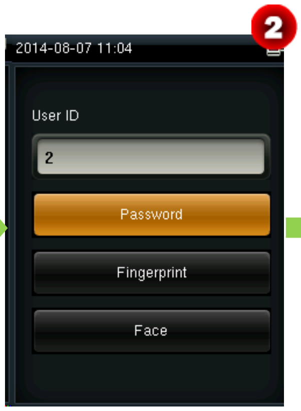
Under this verification method, the entered password is verified with the password of the entered user ID.



2014-08-07 11:01

User ID

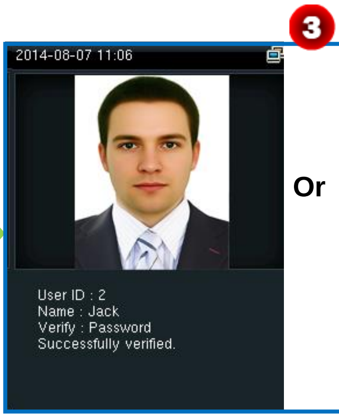
2



2014-08-07 11:04

User ID

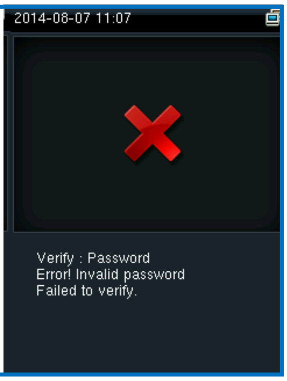
2



2014-08-07 11:06

User ID : 2
Name : Jack
Verify : Password
Successfully verified.

Or



2014-08-07 11:07

Verify : Password
Error! Invalid password
Failed to verify.

Input the user ID and press [M/OK].

Choose "Password" and press [M/OK].

Verification Succeeds

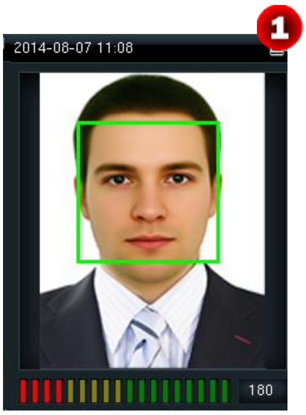
Verification Fails

☺**Remarks:**

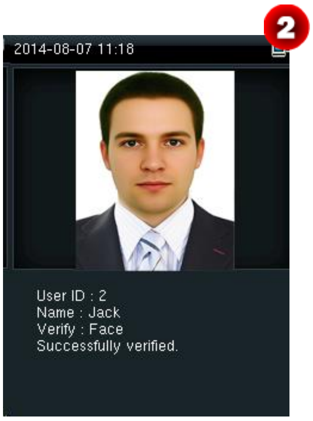
If "Incorrect password":s displayed, please enter the password again. If verification still fails after 2 attempts, it will exit to the initial interface.

1.4.4 1:N Face-based Attendance

Compare the facial image captured by the camera with all facial data in the device.



Conduct comparison in the correct way on the main interface.

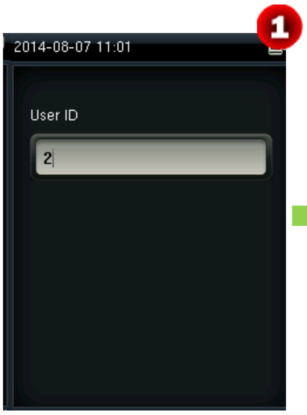


User ID : 2
Name : Jack
Verify : Face
Successfully verified.

Verification passed.

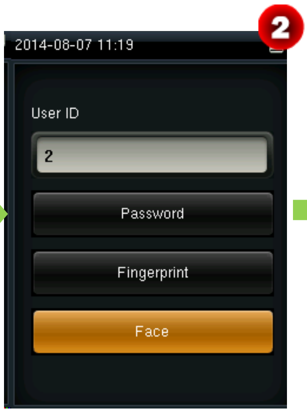
1.4.5 1:1 Face-based Attendance

Compare the captured facial image with the facial image associated with the entered user ID.



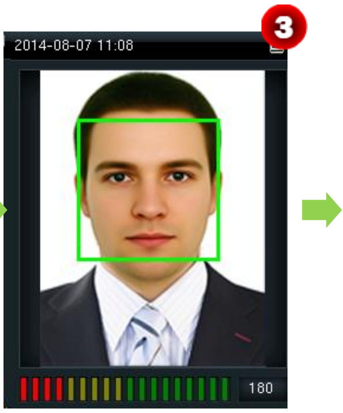
User ID
2

Enter the user ID into the main interface by using the keypad and then press [M/OK].

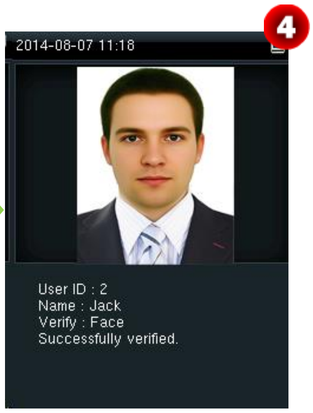


User ID
2

Select [Face] and then press [M/OK].



Compare the faces in the right way.

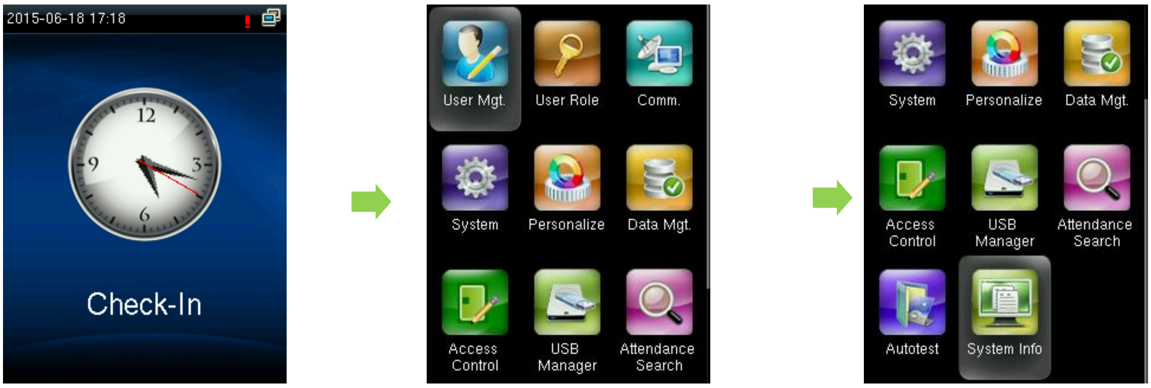


User ID : 2
Name : Jack
Verify : Face
Successfully verified.

Verification passed.

2 Main Menu

When the device is in standby mode, press [M/OK] to open the Main Menu.



Functions of the main menu are described as follows:

User Mgt.: To add, browse and manage user information, including the user ID, permission, verification mode, fingerprint, face, password, user photo, and access control rights, and to add, edit and delete basic personnel information.

User Role: To set user roles for accessing into the menu and changing settings.

Comm.: To set the related parameters of the communication between the device and PC, including Ethernet parameters such as IP address, serial Comm, PC connection and Wiegand settings.

System: To set system-related parameters to meet user requirements to the maximum extent in terms of functions, display and others, including the system time, date, attendance parameters, face parameters, fingerprint parameters, factory settings restoration, and USB disk-based upgrade.

Personalize: This includes interface display, voice, bell, punch state key mode and shortcut key settings.

Data Mgt.: To manage data in the device, for example, to delete attendance records, all data, user roles, and user photos, clear publicity pictures, and back up and restore device data.

Access Control: To set the user access time period and the parameters of the control lock and related device.

USB Manager: To upload and download setting reports and download attendance reports. The user information and attendance data in the device can be imported into related software for processing, or the user information can be imported into other fingerprint devices through a USB disk.

Attendance Search: The attendance search and exception search functions enable employees to query records and exceptions that are saved in the device after successful attendance.

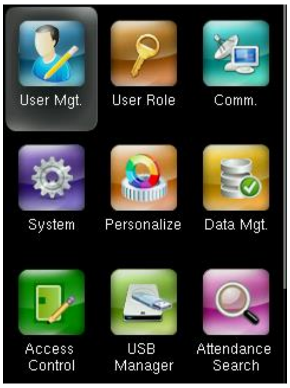
Autotest: To automatically test different module's functions, including the LCD, voice, keyboard, fingerprint sensor, camera* and clock RTC test.

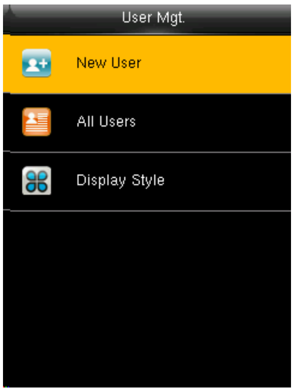
System Info: To check device capacity, device and firmware information.

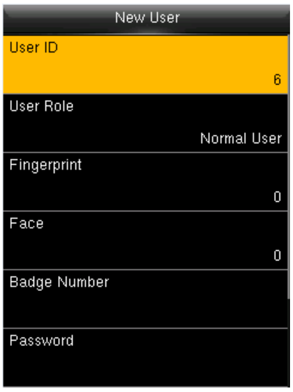
3 User Management

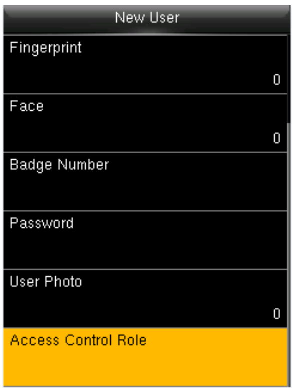
3.1 Adding User

The basic user information in the device includes the user ID, user role, verification mode, fingerprint, face, badge number, password, user photo, and access control rights. The access control rights include the belonged group, verification mode, whether the duress fingerprint is defined, and use time period. In the company's access control management, operations such as adding, deleting, query, and modifying need to be performed on the personnel information in the device.





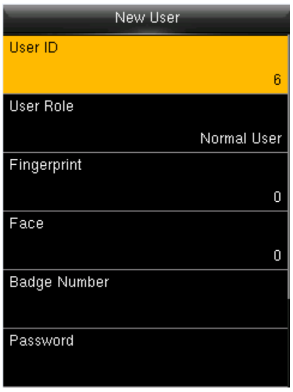


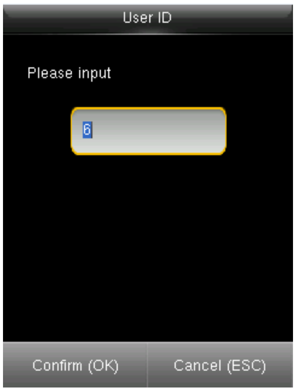


Press **M/OK** > **User Mgt.** > **New User** to access the interface of adding a user, in which you can enter a user ID, select a user role (normal user or super administrator), register a fingerprint, register a badge number, set a password, and set access control rights.
In the initial interface, press [M/OK] > User Mgt. > New User to enter New User setting interface. Settings include inputting User ID, Name, choosing User Role, registering Fingerprint and Badge Number, setting Password and setting Access Control Role.

3.1.1 Entering a User ID

The device automatically assigns user IDs for personnel, starting from 1 and so on. The user ID can also be entered manually.

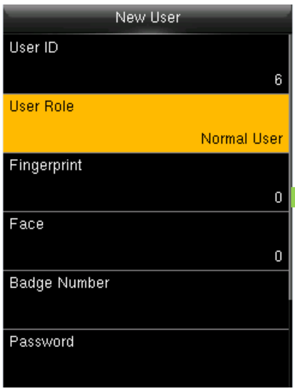




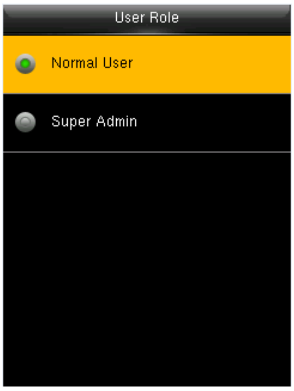
Select **User ID** and
press **M/OK** for confirmation.

Press the number keys on the keypad to enter a user ID and
press **M/OK** for confirmation.

3.1.2 Setting the User Role



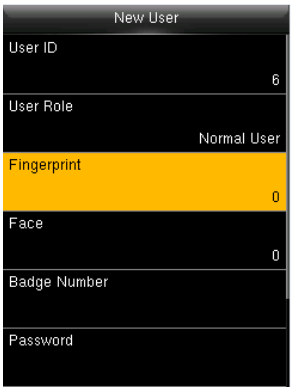
Press ▼ to select **User Role** and then press **M/OK**.



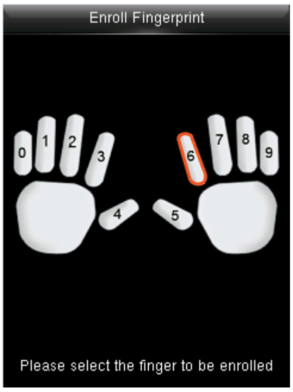
Press ▲/▼ to select **Normal User** or **Super Admin**.

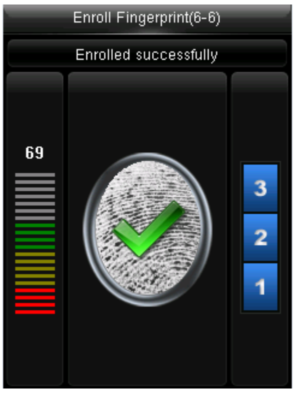
A super administrator can check in and out by using a fingerprint, face or password and enter the menu. A super administrator has the operation permissions over all menu items.
A normal user can check in and out only by using a fingerprint, face or password.

3.1.3 Registering a Fingerprint



Press ▼ to select **Fingerprint** and press **M/OK** for confirmation.

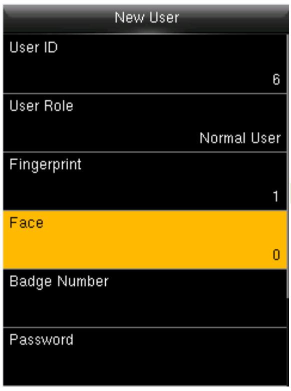




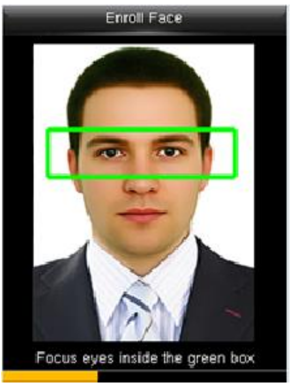
Press the same finger in the right way for three continuous times until the registration succeeds.

For the method of pressing a fingerprint, see 1.2 "Method of Pressing Fingerprint." If registration fails, the device shows a prompt and returns to the fingerprint registration interface. Repeat the previous operation.

3.1.4 Registering a Face



Press ▼ to select **Face** and press **M/OK** for



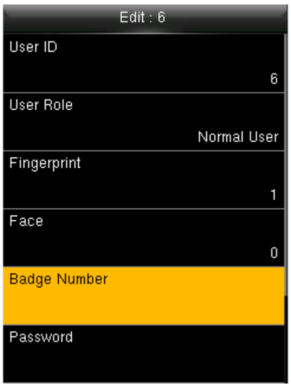
Follow the prompts on the device to place eyes in

See 1.3 "Standing Position, Facial Expression and Stance". During face registration, when the green frame is in the middle, a user photo will be taken automatically and saved in the device.

confirmation.

the green frame until the registration succeeds.

3.1.5 Registering a Badge Number*


Edit : 6

User ID: 6

User Role: Normal User

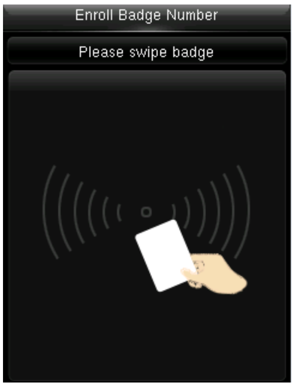
Fingerprint: 1

Face: 0

Badge Number

Password

Press ▼ to select **Badge Number** and press **M/OK** for confirmation.

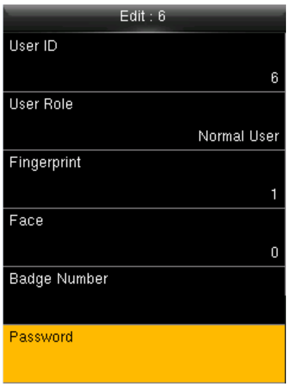

Enroll Badge Number

Please swipe badge

Swipe the badge slightly in the induction area until the device senses the badge.

The device saves and displays the read badge number on the screen.

3.1.6 Registering a Password


Edit : 6

User ID: 6

User Role: Normal User

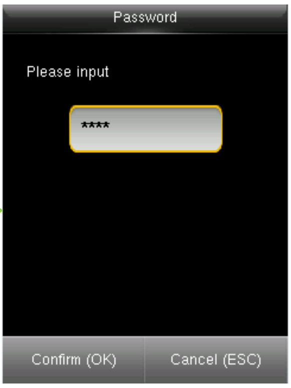
Fingerprint: 1

Face: 0

Badge Number

Password

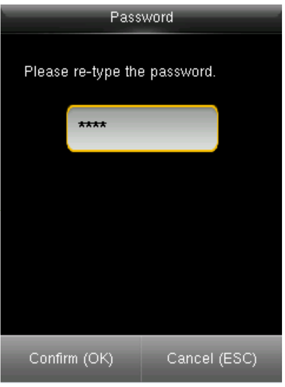
Press ▼ to select **Password** and press **M/OK** for confirmation.


Password

Please input

****

Use the numeric keypad to enter a password and press **M/OK** for confirmation.


Password

Please re-type the password.

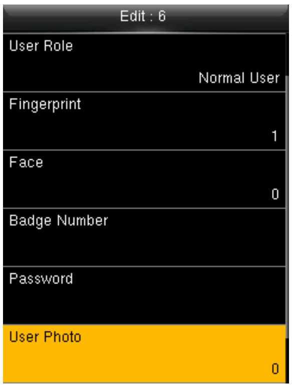
****

Re-enter the password for confirmation.

The equipment supports a 1-8 digit password.

3.1.7 Registering a Photo

When a user registered with a portrait passes the verification, the registered user portrait is displayed besides information such as the user ID and name.



Edit : 6

User Role: Normal User

Fingerprint: 1

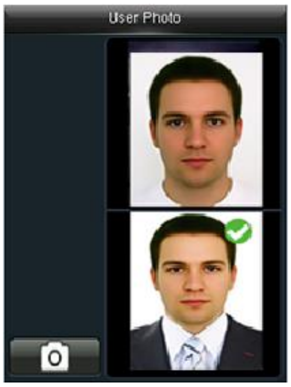
Face: 0

Badge Number

Password

User Photo: 0

Press ▼ to select "User Photo" and press **M/OK** for confirmation.



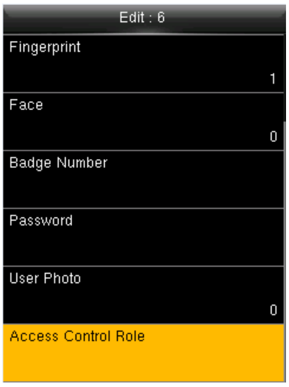
User Photo

Stand in front of the screen naturally and press **M/OK** to take a photo.

When the photo taken during facial registration is used, photo taking is not required.

3.1.8 Setting the Access Control Rights

You can set which group a user belongs to, access verification mode, whether to register a duress fingerprint, and whether to use the group time period. By default, the unlocking permission is granted to newly enrolled users.



Edit : 6

Fingerprint: 1

Face: 0

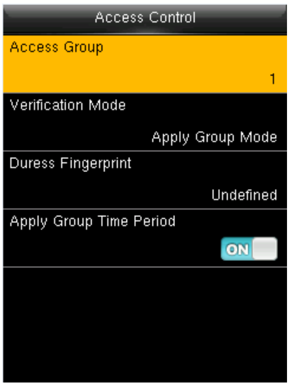
Badge Number

Password

User Photo: 0

Access Control Role

Press ▼ to select **Access Control Role** and then press **M/OK**.



Access Control

Access Group: 1

Verification Mode: Apply Group Mode

Duress Fingerprint: Undefined

Apply Group Time Period: ON

Press ▲/▼ to select a different verification mode.

Access Group: Select the belonged group. By default, a newly enrolled user belong to group one.

Verification Mode: Select a user verification mode. A total of 22 user verification modes are supported, including group verification mode, face/fingerprint/password/badge, only fingerprint, only user ID, password, only badge, fingerprint/password, fingerprint/badge, password/badge, user ID&fingerprint, fingerprint&password, password&badge, fingerprint&password&badge, password&badge, user ID&fingerprint&password, fingerprint&badge&user ID, only face, face&fingerprint, face&password, face&badge, face&fingerprint&badge, and face&fingerprint&password.

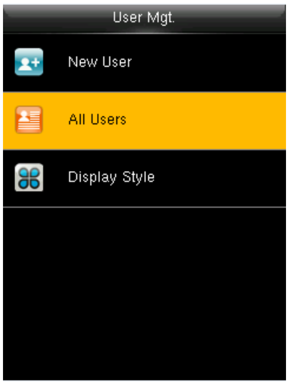
Duress Fingerprint: A fingerprint registered in the device is specially specified as a duress fingerprint. In any case, a duress alarm is generated when a fingerprint matches a duress fingerprint.

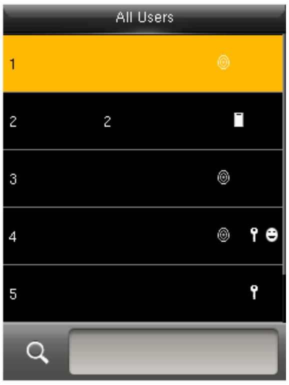
Apply Group Time Period: The default value is **1**.

Note: For settings of the access control group and the time period, see 9 "Access Control."

3.2 User Management

During daily company management, when a personnel change occurs, the personnel information needs to be updated on the device. Operations such as user adding, deleting, query and modifying can be performed.





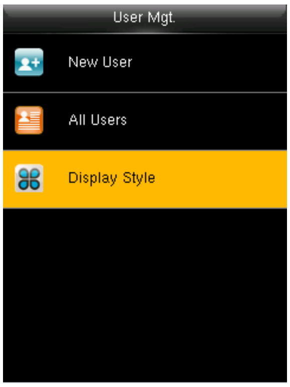
Querying a user: Enter a user ID to be queried in the user list. The device automatically locates the user with this user ID.

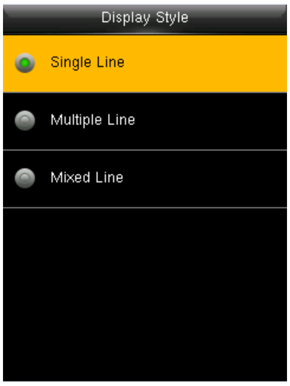
Modifying user information: Query to locate the person whose user information needs to be modified and press **M/OK** to modify the person information.

Deleting a user: You can select to delete a user, delete a fingerprint only, delete a face only, delete a password only, or delete a user photo only.

Display Style

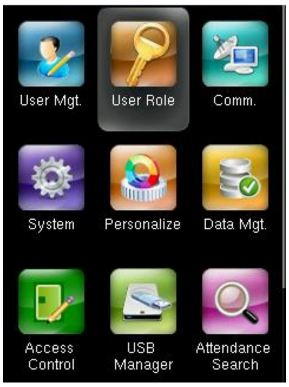
Select the display style of the user list, including single line, multiple line and mixed line.

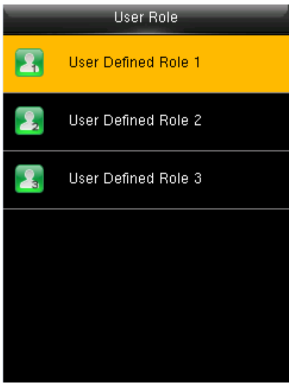




4 User Role

Set the permissions for a defined role to perform operations on the menu. Three roles can be created at most.

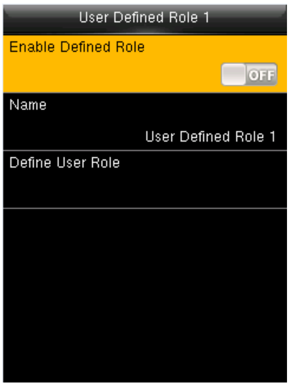



User Role

User Defined Role 1

User Defined Role 2

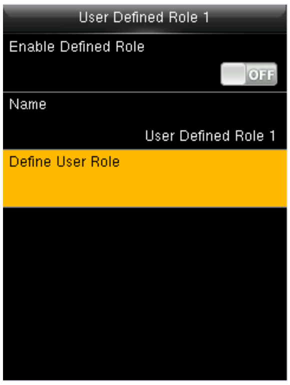
User Defined Role 3


User Defined Role 1

Enable Defined Role OFF

Name User Defined Role 1

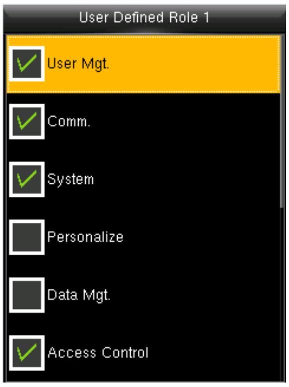
Define User Role


User Defined Role 1

Enable Defined Role OFF

Name User Defined Role 1

Define User Role


User Defined Role 1

☑ User Mgt.

☑ Comm.

☑ System

□ Personalize

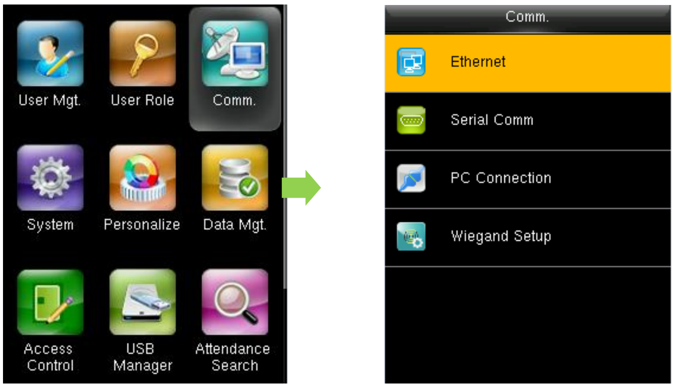
□ Data Mgt.

☑ Access Control

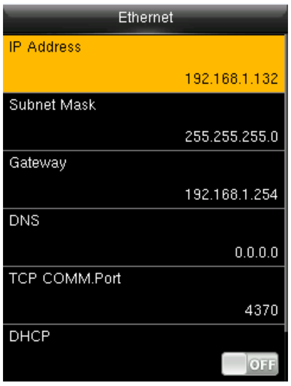
Access **User Role** from the main menu, enable a role and assign permissions. The name cannot be entered but can be uploaded with software or a default name can be used.

5 Comm. Settings

Set the parameters related to communication between the device and a PC over the Ethernet, including the IP address, gateway, subnet mask, baud rate, device ID, and connection password.



5.1 Ethernet Settings


Ethernet

IP Address 192.168.1.132

Subnet Mask 255.255.255.0

Gateway 192.168.1.254

DNS 0.0.0.0

TCP COMM.Port 4370

DHCP OFF

IP Address: The default IP address is **192.168.1.201** and can be changed based on requirements.

Subnet Mask: The default subnet mask is **255.255.255.0** and can be changed based on requirements.

Gateway: The default gateway address is **0.0.0.0** and can be changed based on requirements.

DNS: The default DNS address is **0.0.0.0** and can be changed based on requirements.

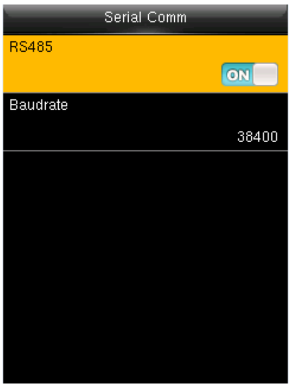
TCP COMM. Port: The default value is **4370** and can be changed based on requirements.

DHCP: This is the Dynamic Host Configuration Protocol, which uses the server to allocate dynamic IP addresses to network clients.

Displaying the network icon in the status bar: Set whether to display the network icon in the status bar of the main interface.

5.2 Serial Comm. Settings

When the device communicates with a PC in serial mode (RS485), check the following settings:



Serial Comm

RS485 ON

Baudrate 38400

Baudrate: The rate of the communication with a PC has four options: 19200, 38400, 57600, and 115200. It is recommended to use 38400 for RS485 communication.

Note: When the 485 reader feature is enabled in access control management and the RS485 communication here is also enabled, a prompt will be displayed, indicating that the device needs to be restarted for the settings to take effect.

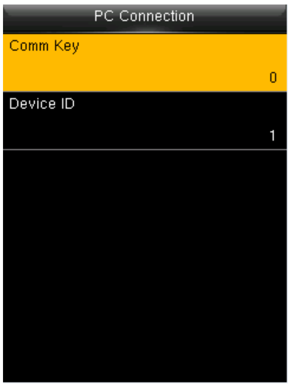
5.3 Connection Setting

To improve security of data, Comm Key for communication between the device and PC needs to be set.

If a Comm Key is set in the device, the correct connection password needs to be entered when the device is connected to the PC software, so that the device and software can communicate.

Comm Key: The default password is 0 (no password) and can be set to another value. After setting, this password must be entered for the communication between software and the device. Otherwise, the connection fails. **Comm Key** can be 1~6 digits.

Device ID: The device ID ranges from1 to 254. If the communication method is RS485, inputting this device ID in the software communication interface is required.



PC Connection

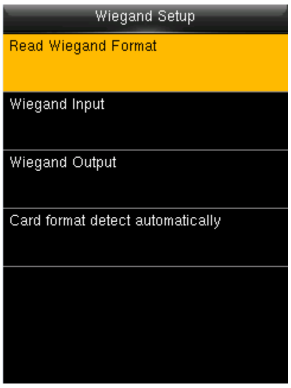
Comm Key 0

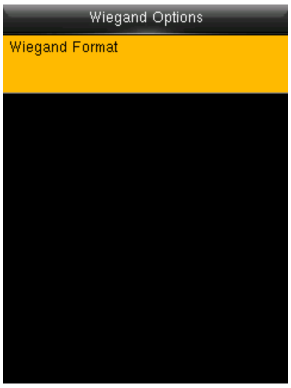
Device ID 1

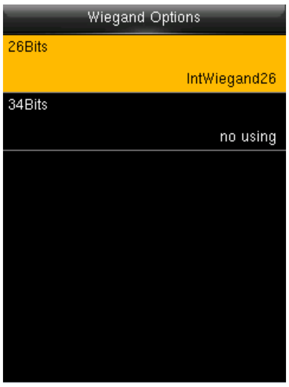
5.4 Wiegand Setup

Set the Wiegand communication formats of the internal card module and external Wiegand device.

5.4.1 Setting of Card Format for the Device

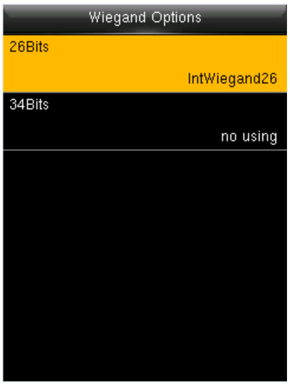






26Bits IntWiegand26

34Bits no using



26Bits IntWiegand26

34Bits no using

Set the Wiegand format matching the card module of the device. After a unified Wiegand format is used, correct card numbers can be read. The Wiegand format can be set to **IntWiegand26**, **IntWiegand26a**, **IntWiegand34**, or **IntWiegand34a** so that card numbers read by the device are in the preset format.

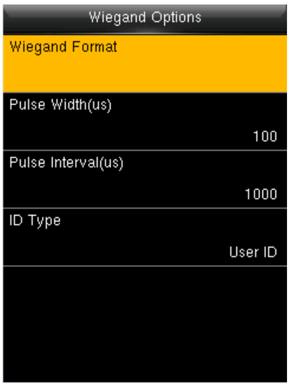
Wiegand Format	**Description**
IntWiegand26	ECCCCCCCCCCCCCCCCCCCCCCCCO This is composed of 26 binary numbers, with bit 1 being the even parity check bit for bits 2-13 and bit 26 being the odd parity check bit for bits 14-25 and bits 2-15 being the card number.
IntWiegand26a	ESSSSSSSSCCCCCCCCCCCCCCCCO This is composed of 26 binary numbers, with bit 1 being the even parity check bit for bits 2-13, bit 26 being the odd parity check bit for bits 14-25, bits 2-9 being the area code and bits 10-15 being the card number.
IntWiegand34	ECCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO This is composed of 34 binary numbers, with bit 1 being the even parity check bit for bits 2-17 and bit 34 being the odd parity check bit for bits 18-33 and bits 2-15 being the card number.
IntWiegand34a	ESSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCO This is composed of 34 binary numbers, with bit 1 being the even parity check bit for bits 2-17, bit 34 being the odd parity check bit for bits 18-33, bits 2-9 being the area code and bits 10-15 being the card number.

Note: C stands for card number, E stands for even parity check, and O stands for odd parity check.

Note: This item is available for ID card machine but not MF card machine.

5.4.2 Wiegand Input

Set the Wiegand format of an externally connected reader.

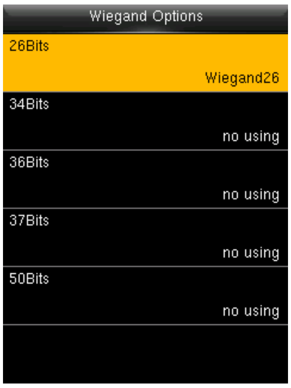

Wiegand Options

Wiegand Format

Pulse Width(us): 100

Pulse Interval(us): 1000

ID Type: User ID


Wiegand Options

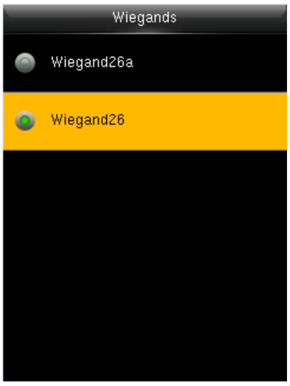
26Bits: Wiegand26

34Bits: no using

36Bits: no using

37Bits: no using

50Bits: no using


Wiegands

○ Wiegand26a

● Wiegand26

Wiegand Format: Users can choose among the following built-in Wiegand formats: Wiegand 26, Wiegand 26a, Wiegand 34, Wiegand 34a, Wiegand 36, Wiegand 36a, Wiegand 37, Wiegand 37a and Wiegand 50, in which no using means the format with this bit number is not used. The following table describes all formats.

Pulse Width (us): The width of pulse sent by Wiegand. The default value is 100 microseconds, which can be adjusted within the range of 20 to 100 microseconds.

Pulse Interval (us): The default value is 1000 microseconds, which can be adjusted within the range of 200 to 20000 microseconds.

ID Type: Input content included in Wiegand input signal. User ID or Badge Number can be chosen.

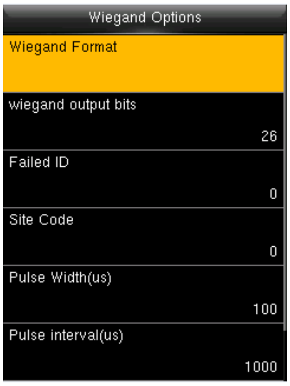
Definitions of Wiegand Formats:

Wiegand Format	Definition
Wiegand26	ECCCCCCCCCCCCCCCCCCCCCCCCO 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 number.
Wiegand26a	ESSSSSSSSCCCCCCCCCCCCCCCCO 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 are the site code, while the 10th to 25th bits are the card number.
Wiegand34	ECCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO 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 number.
Wiegand34a	ESSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCO 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 are the site code, while the 10th to 25th bits are the card number.
Wiegand36	OFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCMME 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 are the device code, the 18th to 33rd bits are the card number, and the 34th to 35th bits are the manufacturer code.
Wiegand36a	EFFFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCO Consists of 36 bits of binary code. The 1st bit is the even parity bit of the 2nd to 18th

Wiegand Format	Definition
	bits, while the 36th bit is the odd parity bit of the 19th to 35th bits. The 2nd to 19th bits are the device code, and the 20th to 35th bits are the card number.
Wiegand37	OMMMMSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCE 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 are the manufacturer code, the 5th to 16th bits are the site code, and the 21st to 36th bits are the card number.
Wiegand37a	EMMMFFFFFFFFFFSSSSSSCCCCCCCCCCCCCCCCO 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 35th bits. The 2nd to 4th bits are the manufacturer code, 5th to 14th bits are the device code, 15th to 20th bits are the site code, and the 21st to 36th bits are the card number.
Wiegand50	ESSSSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO 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 are the site code, and 18th to 49th bits are the card number.

✍ **Note: C** denotes card number, **E** denotes even parity bit, **O** denotes odd parity bit, **F** denotes device code, **M** denotes manufacturer code, **P** denotes parity bit, and **S** denotes site code.

5.4.3 Wiegand Output



Wiegand Options

Wiegand Format

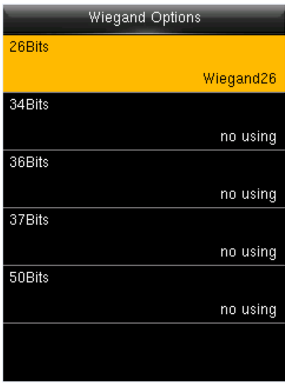
wiegand output bits 26

Failed ID 0

Site Code 0

Pulse Width(us) 100

Pulse interval(us) 1000



Wiegand Options

26Bits Wiegand26

34Bits no using

36Bits no using

37Bits no using

50Bits no using

Wiegand Format: Users can select the standard Wiegand formats built in the system. See the definitions of all kinds of general Wiegand formats in 5.4.2 "Wiegand Input." Although multiple choices are supported, the actual format is determined by **Wiegand output bits**.

Wiegand output bits: the bit length of Wiegand data. After **Wiegand output bits** is set, the device will find the Wiegand format of this bit number in **Wiegand Format**.

For example, if **Wiegand26**, **Wiegand34a**, **Wiegand36**, **Wiegand37a** and **Wiegand50** are selected for **Wiegand Format**, but **Wiegand output bits** is set to **36**, the 36 bit Wiegand36 format will be adopted eventually.

Failed ID: It is defined as the output value of failed user verification. The output format depends on the **[Wiegand Format]** setting. The default value ranges from 0 to 65535.

Site Code: It is similar to device ID except that it can be set manually and repeatable with different devices.

The default value ranges from 0 to 256.

Pulse Width (μs): The width of pulse sent by Wiegand. The default value is 100 microseconds, which can be adjusted within the range of 20 to 100 microseconds.

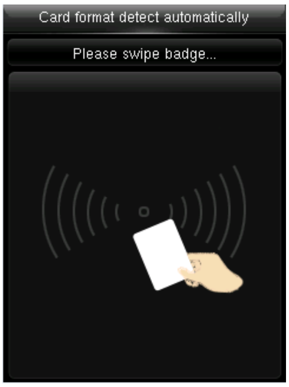
Pulse Interval (μs): The default value is 1000 microseconds, which can be adjusted within the range of 200 to 20000 microseconds.

ID Type: Output content after successful verification. User ID or card number can be chosen.

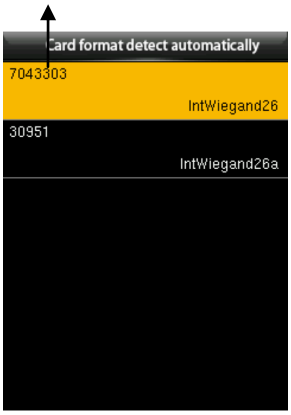
5.4.4 Card Format Detect Automatically

[Card Format Detect Automatically] aims at assisting user with quickly detecting the card type and its corresponding format. Various card formats are preset in the device. After card swiping, the system will detect it as different card numbers according to every format; user only requires to choose the item equivalent to the actual card number, and set the format as the Wiegand format for the device. This function is also applicable to card reading function and auxiliary Wiegand reader.

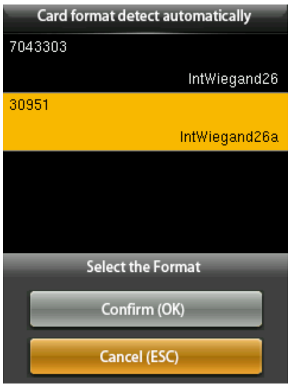
Card number obtained based on the IntWiegnad26 format parsing



After entering automatic detection, swipe the badge in the card swiping area (on the device or reader).



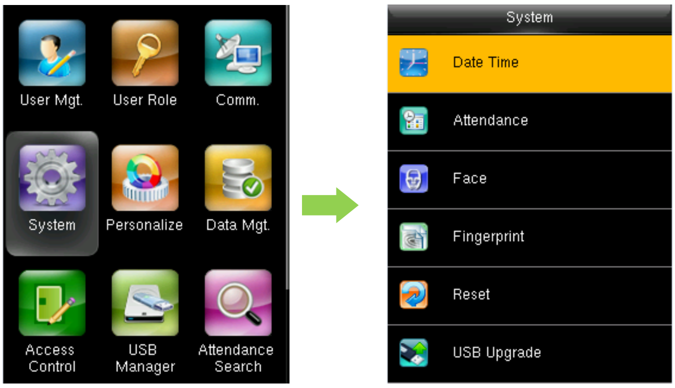
The Wiegand format and parsed card number are automatically detected.



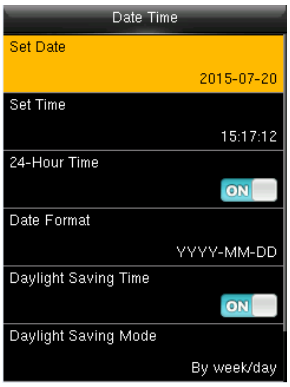
Select the number consistent with the actual card number, and the corresponding format is the Wiegand format which should be selected for reading this type of card.

6 System Settings

Set system-related parameters to to meet user requirements to the maximum extent in terms of functions, display and others, including the time and date, attendance parameters, and fingerprint parameters.



6.1 Time and Date



Date Time

Set Date 2015-07-20

Set Time 15:17:12

24-Hour Time ON

Date Format YYYY-MM-DD

Daylight Saving Time ON

Daylight Saving Mode By week/day

Set Date and **Set Time**: Set the date and time for the device.

24-Hour Time: Set the time display mode on the main interface. When it is set to **ON**, the time is displayed in 24-hour system; when it is set to **OFF**, the time is displayed in 12-hour system.

Date Format: Set the format of dates displayed on all interfaces of the device.

Daylight Saving Time:

The daylight saving time, or DST, is a system which artificially stipulates local time for energy saving. The unified time used during the implementation of this system is called daylight saving time. In summertime when the daybreak is early, the time is usually set one hour ahead artificially so that people sleep and get up early, which reduces lighting consumption and makes full use of sunlight resource to save lighting power. When autumn comes, the time is set back. The countries adopting the daylight saving time have different specific provisions.

In order to meet requirements for daylight saving time, the device is specially customized with a feature which sets the time one hour ahead at XX:XX on day XX in month XX and sets the time back at XX:XX on day XX in month XX.

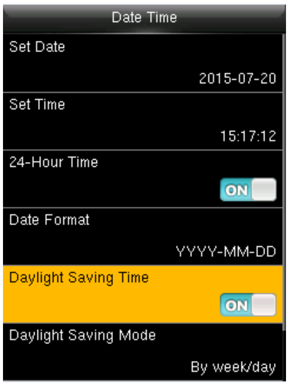
Operation instructions:

Set **Daylight Saving Time** to **ON**.

2) Enter the start time and end time of DST.

For example, the device is set to start DST at 08:00 on April 1 and the time is set one hour ahead; the device resumes normal time at 08:00 on October 1.

3) Press **OK** to save the setting. Press **ESC** to quit without saving.


Date Time

Set Date: 2015-07-20

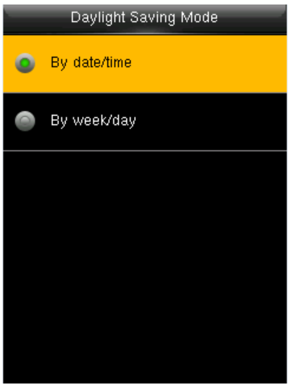
Set Time: 15:17:12

24-Hour Time: ON

Date Format: YYYY-MM-DD

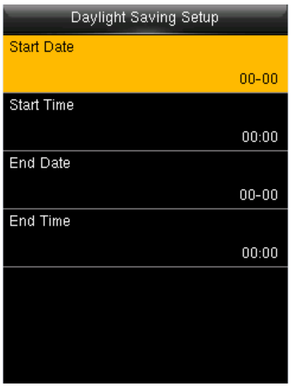
Daylight Saving Time: ON

Daylight Saving Mode: By week/day


Daylight Saving Mode

● By date/time

○ By week/day

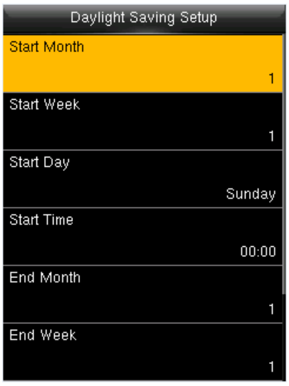

Daylight Saving Setup

Start Date: 00-00

Start Time: 00:00

End Date: 00-00

End Time: 00:00


Daylight Saving Setup

Start Month: 1

Start Week: 1

Start Day: Sunday

Start Time: 00:00

End Month: 1

End Week: 1

Enable DST Conversion mode of DST Time setting in date mode Time setting in week mode

Daylight Saving Mode: The date mode (month-day-hour) (default) or week mode (month-week-hour) can be selected.

Daylight Saving Setup: Set the start time and end time of DST.

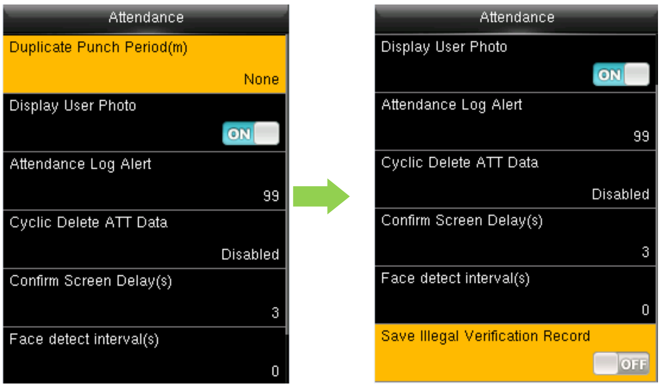
The date mode and week mode are described as follows:

1. If the DST start month is set to be later than the DST end month, the DST end month is in the next year of the DST start month. For example: The DST starts at 4:00, 2012-9-1, and ends at 4:00, 2013-4-1.

2. In week mode, assume that the DST start day is set to the sixth Sunday in September, and the current year is 2012, but the calendar shows that September of 2013 has five not six weeks. In this case, the system starts DST at corresponding time on the last Sunday of this month.

3. Assume that the DST start day is set to Monday of the first week of September, and the current year is 2012, but the calendar shows that the first week of September does not have Monday. In this case, the system automatically locates the first Monday of this month.

6.2 Attendance Parameters


Attendance

Duplicate Punch Period(m): None

Display User Photo: ON

Attendance Log Alert: 99

Cyclic Delete ATT Data: Disabled

Confirm Screen Delay(s): 3

Face detect interval(s): 0

Save Illegal Verification Record: OFF

Duplicate Punch Period (m): Within a set time period (unit: minutes), the duplicated attendance logs will not be reserved (value ranges from 1 to 999999 minutes).

Display User Photo: indicates whether to display a user photo when the user passes attendance check.

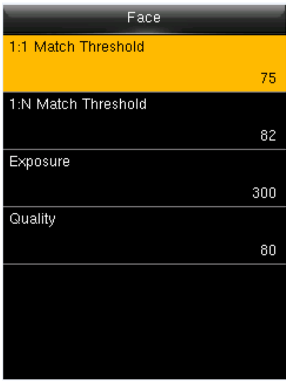
Attendance Log Alert: When the remaining storage is smaller than the set value, the device will automatically alert users to the remaining storage information. It can be disabled or set to a value ranged from 1 to 9999.

Cyclic Delete ATT Data: The number of attendance logs allowed to be deleted in one time when the maximum storage is attained. It can be disabled or set to a value ranged from 1 to 999.

Face Detect Interval: Set the interval time between comparisons for the same face.

Save Illegal Verification Record: To set if failed verifications, such as those caused by access in invalid Time Schedules or illegal Combined Verification, will be saved when the advanced access control function is turned on.

6.3 Face Parameters



Face

1:1 Match Threshold
75

1:N Match Threshold
82

Exposure
300

Quality
80

1:1 Match Threshold: the similarity with the face template registered in the device in 1:1 verification mode. When the similarity is larger than this value, matching succeeds. Otherwise, matching fails. The valid value is in the range of 70-120. The higher the threshold is set, the lower the misjudgment is, leading to higher rejection rate, and vice versa.

1:1:N Match Threshold: the similarity with the face template registered in the device in 1:N comparison mode. When the similarity is larger than this value, matching succeeds. Otherwise, matching fails. The valid value is in the range of 80-120. The higher the threshold is set, the lower the misjudgment is, leading to higher rejection rate, and vice versa.

Recommended match thresholds:

Rejection rate	Misjudgment rate	Matching threshold	
		1:N	1:1
High	Low	85	80
Medium	Medium	82	75
Low	High	80	70

Exposure: to set the camera exposure value, 300 by default.

Quality: the quality threshold for facial image acquisition. When the quality of an image is larger than this value, the device receives this facial image and starts algorithm processing. Otherwise, the device filters this facial image. The default value is 80 (within 50-150).

☺Note: Improper adjustments of **Exposure** and **Quality** seriously affect the device service effect. If you need to adjust the parameters, please follow the instructions of our after-sales service personnel for operations.

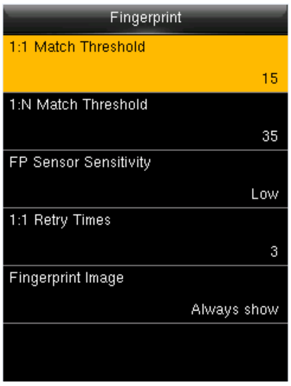
6.4 Fingerprint Parameters

1:1 Match Threshold: Under 1:1 Verification Method, only when the similarity between the verifying fingerprint and the user's registered fingerprint is greater than this value can the verification succeed.

1:N Match Threshold: Under 1:N Verification Method, only when the similarity between the verifying fingerprint and all registered fingerprints is greater than this value can the verification succeed.

Recommended Match Threshold:

		Match Threshold	
FRR	**FAR**	**1: N**	**1:1**
High	Low	45	25
Medium	Medium	35	15
Low	High	25	10



Fingerprint

1:1 Match Threshold 15

1:N Match Threshold 35

FP Sensor Sensitivity Low

1:1 Retry Times 3

Fingerprint Image Always show

FP Sensor Sensitivity: To set the sensibility of fingerprint collection. It is recommended to use the default level "**Medium**". When the environment is dry, resulting in slow fingerprint detection, you can set the level to "**High**" to raise the sensibility; when the environment is humid, making it hard to identify the fingerprint, you can set the level to "**Low**".

1:1 Retry Times: In 1:1 Verification or Password Verification, users might forget the registered fingerprint or password, or press the finger improperly. To reduce the process of re-entering user ID, retry is allowed; the number of retry can be within 1~9.

Fingerprint Image: To set whether to display the fingerprint image on the screen in registration or verification. Four choices are available: Show for enroll, Show for match, Always show, None.

6.4 Reset to Factory Settings

Reset data such as communication settings and system settings to factory settings.

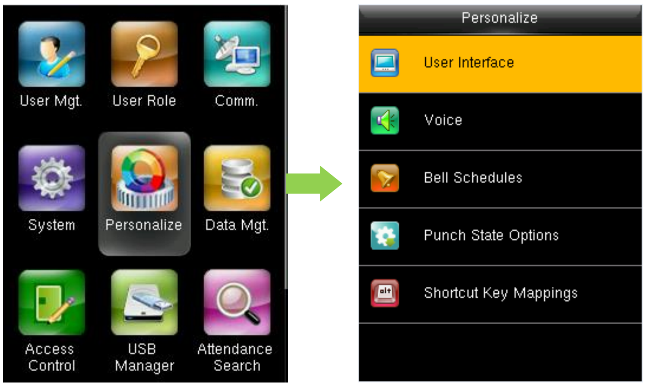
✍ **Remarks:** When resetting to factory settings, the user date and Attendance logs will not be affected.

6.5 USB Upgrade

This option enables the device firmware to be upgraded with the upgrade file in a USB disk.

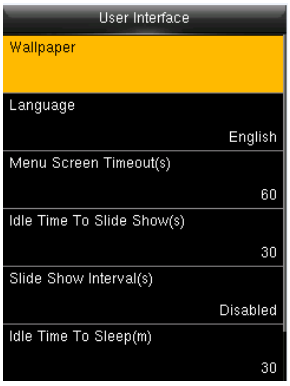
ⓘ If upgrade file is needed, please contact out technical support. Firmware upgrade is not recommenced under normal circumstances.
The upgrade with a USB disk is possible only for machines supporting the USB flash disk feature.

7 Personalize Settings



7.1 User Interface Settings

Users are able to customize the display style of the main interface based on their personal preference.



User Interface

Wallpaper

Language: English

Menu Screen Timeout(s): 60

Idle Time To Slide Show(s): 30

Slide Show Interval(s): Disabled

Idle Time To Sleep(m): 30

Wallpaper: Select the wallpaper of main screen as required, you can find wallpapers of various styles in the device.

Language: Select the language of device as required.

Menu Screen Timeout (s): When there is no operation in the menu interface and the time exceeds the set value, the device will automatically exit to the initial interface. You can disable it or set the value to 60~99999 seconds.

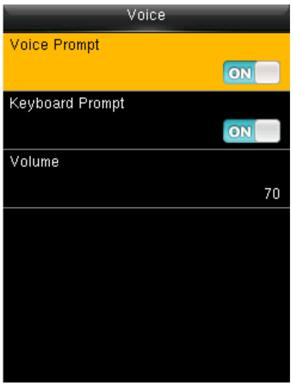
Idle Time To Slide Show (s): When there is no operation in the initial interface and the time exceeds the set value, a slide show will be shown. It can be disabled (set to "**None**") or set to 3~999 seconds.

Slide Show Interval (s): This refers to the interval between displaying different slide show pictures. It can be disabled or set to 3~999 s.

Idle Time To Sleep (m): When there is no operation in the device and the set Sleep Time is attained, the device will enter standby mode. Press any key or finger to cancel standby mode. You can disable this function, or set the value to 1~999 minutes. If this function is turned to **[Disabled]**, the device will not enter standby mode.

Main Screen Style: Choosing the position and ways of the clock and status key.

7.2 Voice Settings


Voice

Voice Prompt ON

Keyboard Prompt ON

Volume 70

Voice Prompt: Select whether to enable voice prompts during operating, press **[M/OK]** to enable it.

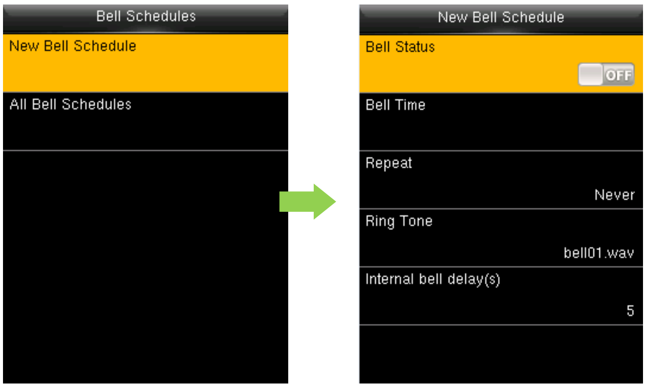
Keyboard Prompt: Select whether to enable keyboard voice while pressing keyboard, press **[M/OK]** to enable it.

Volume: Set the volume of device. Press ▶ key to increase the volume, press ◀ key to decrease the volume.

7.3 Bells Settings

Many companies choose to use bell to signify on-duty and off-duty time. When reaching the scheduled time for bell, the device will play the selected ringtone automatically until the ringing duration is passed.

1. Adding a bell schedule


Bell Schedules

New Bell Schedule

All Bell Schedules

New Bell Schedule

Bell Status OFF

Bell Time

Repeat Never

Ring Tone bell01.wav

Internal bell delay(s) 5

Bell Status: **[ON]** is to enable the bell, while **[OFF]** is to disable it.

Bell Time: The bell rings automatically when reaching the specified time.

Repeat: To set whether to repeat the bell.

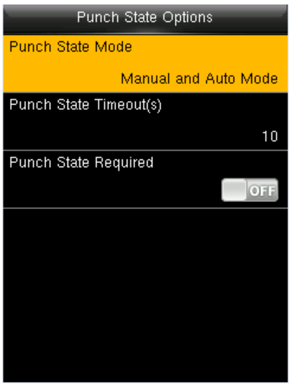
Ring Tone: Ringtone played for bell.

Interval bell delay (s): To set the ringing length. The value ranges from 1 to 999 seconds.

2. Editing and deleting a bell schedule

The edit operation is similar to the operation of adding a bell schedule. To delete a bell schedule, select the bell schedule to be deleted and then conduct deletion.

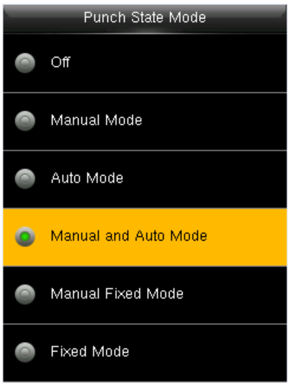
7.4 Punch States Settings


Punch State Options

Punch State Mode: Manual and Auto Mode

Punch State Timeout(s): 10

Punch State Required: OFF


Punch State Mode

○ Off

○ Manual Mode

○ Auto Mode

● Manual and Auto Mode

○ Manual Fixed Mode

○ Fixed Mode

Punch State Mode: To choose the **Punch State Mode**, which includes the following modes:

1. **Off:** To disable the punch state key function. The punch state key set under **Shortcut Key Mappings** menu will become invalid.

2. **Manual Mode:** To switch the punch state key manually, and the punch state key will disappear after **Punch State Timeout**.

3. **Auto Mode:** After this mode is chosen, set the switching time of punch state key in **Shortcut Key Mappings**; when the switching time is reached, the set punch state key will be switched automatically.

4. **Manual and Auto Mode:** Under this mode, the main interface will display the auto-switching punch state key, meanwhile supports manually switching punch state key. After timeout, the manually switching punch state key will become auto-switching punch state key.

5. **Manual Fixed Mode:** After punch state key is manually switched, the punch state key will remain unchanged until being manually switched next time.

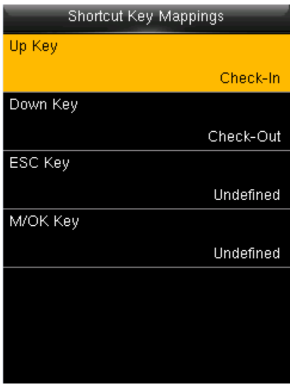
6. **Fixed Mode:** Only the fixed punch state key will be shown and it cannot be switched.

Punch State Timeout (s): The timeout time of the display of punch state. The value ranges from 5~999 seconds.

Punch State Required: Whether it is necessary to choose attendance state in verification.

7.5 Shortcut Keys Settings

Shortcut keys can be defined as punch state keys or menu function key. When the device is on the main interface, pressing the set shortcut key will display the attendance state or enter the menu operation interface.



Shortcut Key Mappings

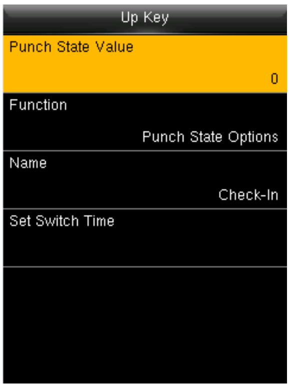
Up Key: Check-In

Down Key: Check-Out

ESC Key: Undefined

M/OK Key: Undefined

Select the shortcut key to be defined and
press **M/OK**.



Up Key

Punch State Value: 0

Function: Punch State Options

Name: Check-In

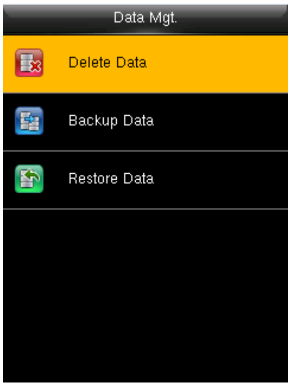
Set Switch Time

Set the state.

When the state key is selected, automatic switching can be set. Automatic switching refers to that the device automatically switches the punch state when a preset time point is reached.

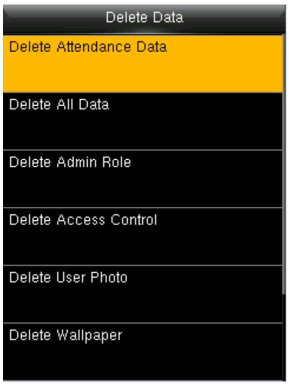
2. When the state key is selected, the device does not enable the state key if the prohibition mode is enabled in state key mode setting.

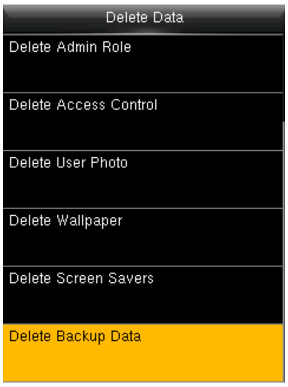
8 Data Mgt.



8.1 Deleting Data

To manage data in the device, which includes delete attendance data, delete all data, delete admin role and delete screen savers etc.

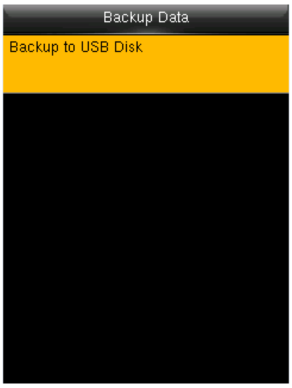




Delete Attendance Data: To delete all attendance data in the device.
Delete All Data: To delete all user information, fingerprints and attendance logs etc.
Delete Admin Role: To make all Administrators become Normal Users.
Delete Access Control: To delete all access data.
Delete User Photo: To delete all user photos in the device.
Delete Wallpaper: To delete all wallpapers in the device.
Delete Screen Savers: To delete all screen savers in the device. (For details of uploading screen savers, please refer to **Appendix 1 Image Uploading Rule**
Delete Backup Data: To delete all backup data.

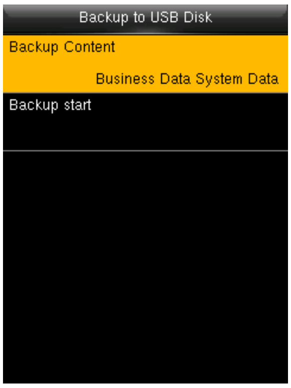
8.2 Data Backup

To backup the business data, or configuration data to the U disk.



Backup Data

Backup to USB Disk

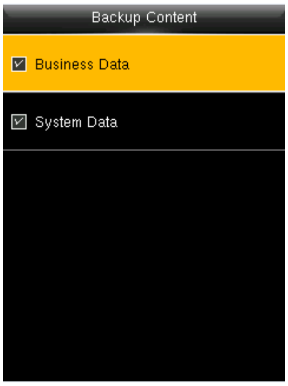


Backup to USB Disk

Backup Content

Business Data System Data

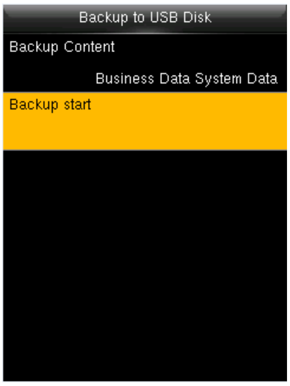
Backup start



Backup Content

☑ Business Data

☑ System Data

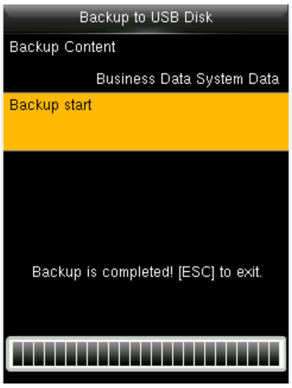


Backup to USB Disk

Backup Content

Business Data System Data

Backup start



Backup to USB Disk

Backup Content

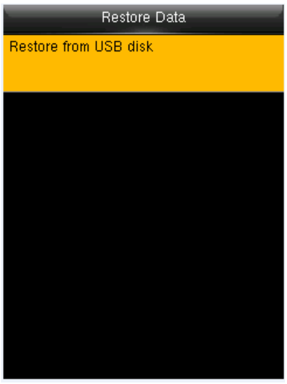
Business Data System Data

Backup start

Backup is completed! [ESC] to exit.

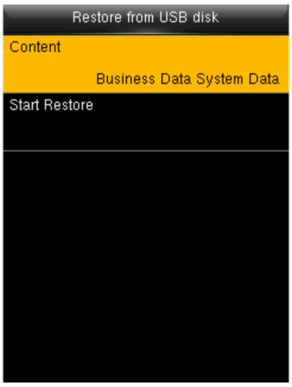
8.3 Data Restoration

To restore the data in the U disk to the device.



Restore Data

Restore from USB disk



Restore from USB disk

Content

Business Data System Data

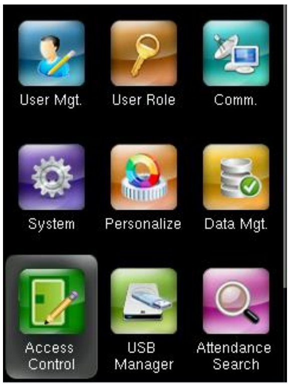
Start Restore

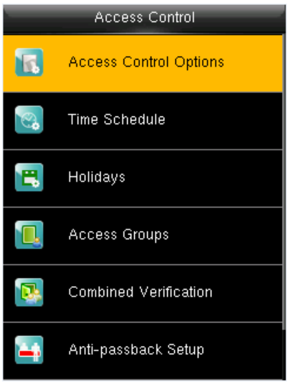
Select the restoration mode.

Select the content to be restored and then start restoration.

9 Access Control

Access Control is used to set the user access time period and the parameters of the control lock and related device.




Access Control

Access Control Options

Time Schedule

Holidays

Access Groups

Combined Verification

Anti-passback Setup

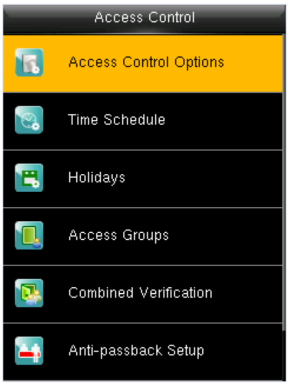
To gain access, the registered user must meet the following conditions:

1. User's access time falls within either user's personal time zone or group time zone.
2. User's group must be in the access combo (when there are other groups in the same access combo, verification of members of those groups are also required to unlock the door).

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

9.1 Access Control Options Settings

Set the parameters of device control lock and related device.


Access Control

Access Control Options

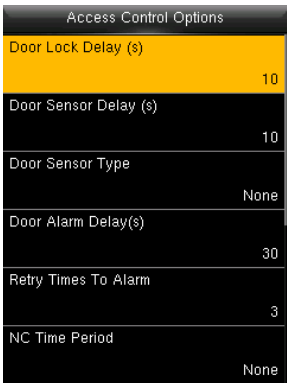
Time Schedule

Holidays

Access Groups

Combined Verification

Anti-passback Setup


Access Control Options

Door Lock Delay (s) 10

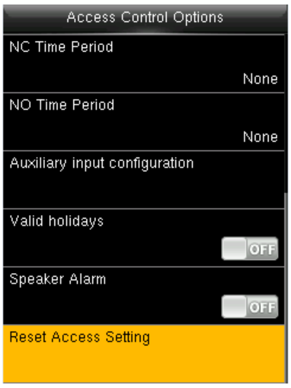
Door Sensor Delay (s) 10

Door Sensor Type None

Door Alarm Delay(s) 30

Retry Times To Alarm 3

NC Time Period None


Access Control Options

NC Time Period None

NO Time Period None

Auxiliary input configuration

Valid holidays OFF

Speaker Alarm OFF

Reset Access Setting

Door Lock Delay (s): The period of time of unlocking (from door opening to closing automatically) after the electronic lock receives an open signal sent from the device (value ranges from 0 to 10 seconds).

Door Sensor Delay (s): When the door is opened, the door sensor will be checked after a time period; if the state of the door sensor is inconsistent with that of the door sensor mode, alarm will be triggered. The time period is the **Door Sensor Delay** (value ranges from 0 to 255 seconds).

Door Sensor Type: It includes **No**, **Normally Open** and **Normally Closed**. **No** means door sensor is not in use;

Normally Open means the door is opened when electricity is on; **Normally Closed** means the door is closed when electricity 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 0 to 9 times), the alarm will be triggered. If the set value is 0, the alarm will not be triggered after failed verification.

NC Time Period: To set time period for Normally Closed mode, so that no one can gain access during this period.

NO Time Period: To set time period for Normally Open, so that the door is always unlocked during this period.

Auxiliary Input Configuration: To set the **Aux output/lock open time** and **Aux Output type** for the device with auxiliary connector. **Aux Output type** includes **None**, **trigger door open**, **trigger Alarm**, and **trigger Door open and Alarm**.

Verify Mode by RS485: To turn on RS485 reader function; it is the verification method used by the device when it is the master/slave device.

Valid holidays: To set if **NC Time Period** or **NO Time Period** settings are valid in set holiday time period. Choose **[ON]** to enable the set **NC** or **NO** time period in holiday.

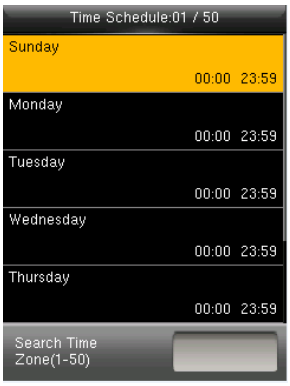
Speaker Alarm: When the **[Speaker Alarm]** is enabled, the speaker will raise an alarm when the device is being dismantled.

Reset Access Setting: To reset parameters of door lock delay, door sensor delay, door sensor type, door alarm delay, retry times to alarm, NC time period, NO time period, auxiliary input configuration, normally open / close for holidays, speaker alarm, anti-passback direction, device status, duress function, alarm on 1:1 match, alarm on 1: N match, alarm on password and alarm delay. However, the content of the Access Data Deletion in **[Data Mgt.]** will not be affected.

Remarks: After setting **NC Time Period**, please lock the door well, otherwise alarm might be triggered during **NC Time Period**.

9.2 Time Schedule Settings

ach user is allowed to set a maximum of three time periods, which are in OR relationship. The time is valid as long as the time during verification meets one of the periods. The format of each time interval in a time period is HH:MM-HH:MM, that is, with the accuracy of minute in 24-hour system.


Time Schedule:01 / 50

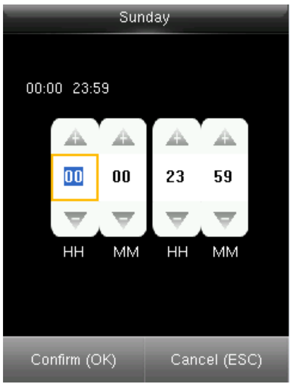
Sunday 00:00 23:59

Monday 00:00 23:59

Tuesday 00:00 23:59

Wednesday 00:00 23:59

Thursday 00:00 23:59


Sunday

00:00 23:59

00 00 23 59

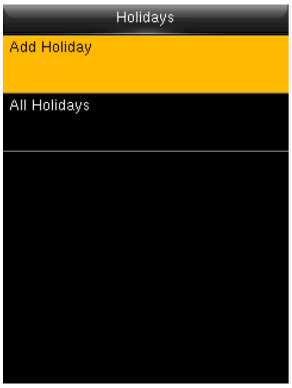
When the end time is earlier than the start time (for example, 23:57-23:56), this means closing all day long. When the end time is later than the start time (for example, 00:00-23:59), this means that this interval is valid.

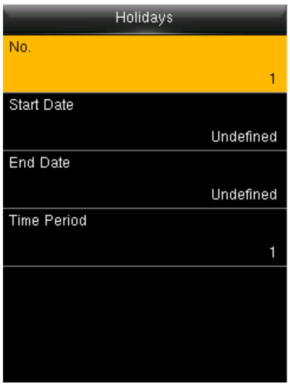
Valid Time Schedule: 00:00 ~ 23:59 (Whole-day valid) or when the end time is greater than the start time.

Note: By default, the number one time period of the system means opening all day long (that is, unlocking for newly enrolled users).

The concept of holiday and festival is introduced into access control. On holidays or festivals, special access control time may be required, but changing everyone's access control time is very tedious. Therefore, the access control time on holidays and festivals, which applies to all staff, can be set.

If the access control time on holidays and festivals is set, the opening period of time on holidays and festivals subjects to the time period set here.




Holidays

No. 1

Start Date Undefined

End Date Undefined

Time Period 1

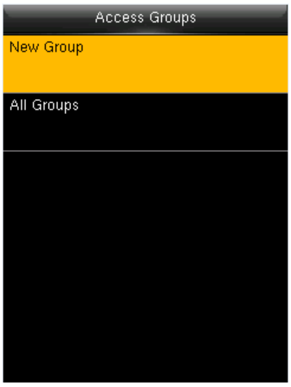
9.4 Access Groups Settings

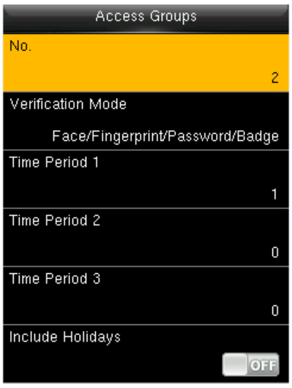
Grouping is to manage users in groups.

Group users' default time zone is set to be the group time zone, while users can set their personal time zone. When the group verification mode overlaps the user verification mode, the user verification modes prevails. Each group can set 3 time zones at most, as long as one of them is valid, the group can be verified successfully. By default, the newly enrolled user belongs to Access Group 1, and can also be allocated to other access group.

Operation instructions:

- Adding a group time period




Access Groups

No.
2

Verification Mode
Face/Fingerprint/Password/Badge

Time Period 1
1

Time Period 2
0

Time Period 3
0

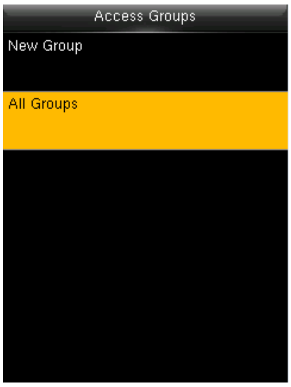
Include Holidays
OFF

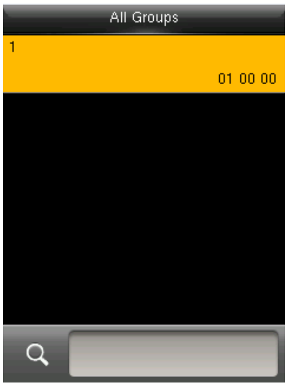
A total of 21 verification modes are supported: face/fingerprint/password/badge, only fingerprint, only user ID, password, only badge, fingerprint/password, fingerprint/badge, password/badge, user ID&fingerprint, fingerprint&password, password&badge, fingerprint&password&badge, password&badge, user ID&fingerprint&password, fingerprint&badge&user ID, only face, face&fingerprint, face&password, face&badge, face&fingerprint&badge, and face&fingerprint&password.

Period of time on holidays and festivals: 1. When the holiday or festival is set to be valid, the personnel in the group can open the door only when group time period overlaps holiday and festival time period.

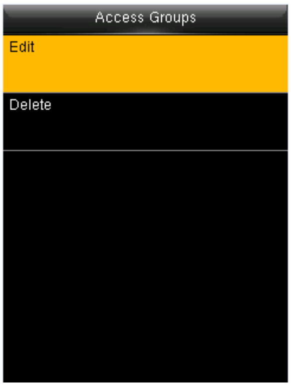
2. When the holiday or festival is set to be invalid, the access control time of the personnel in this group is not affected by holidays or festivals.

- Editing and deleting a group time period




All Groups

1
01 00 00



During editing, the number is not allowed to be modified, and other operations are similar to those of adding an access control group. Press **ESC** to quit.

To delete a group time period, select the access control group to be deleted and delete it.

9.5 Combined Verification Settings

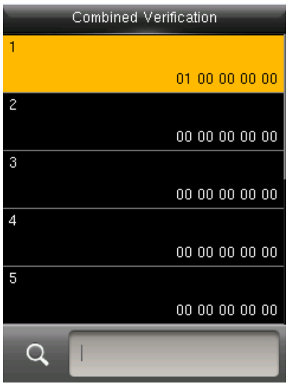
Combine two or more members to achieve multi-verification and improve security.

In a Combined Verification, the range of user number is: 0 ≤ N ≤ 5; the users can all belong to a single group, or belong to 5 different groups at most.

Operation instructions:

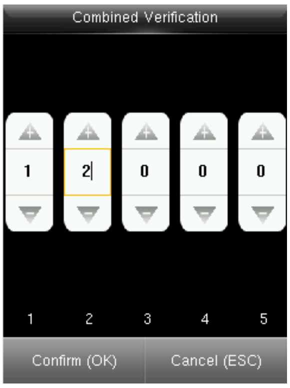
Adding a unlocking combination

For example, the following figures show how to add a combination which can be unlocked only when both group 1 and 2 succeed in verification:



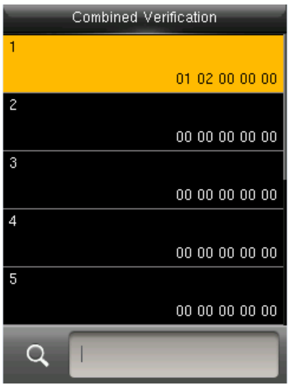
Combined Verification

1	01 00 00 00 00
2	00 00 00 00 00
3	00 00 00 00 00
4	00 00 00 00 00
5	00 00 00 00 00



Combined Verification

1	2	3	4	5
1	2	0	0	0



Combined Verification

1	01 02 00 00 00
2	00 00 00 00 00
3	00 00 00 00 00
4	00 00 00 00 00
5	00 00 00 00 00

2) Editing and deleting a unlocking combination

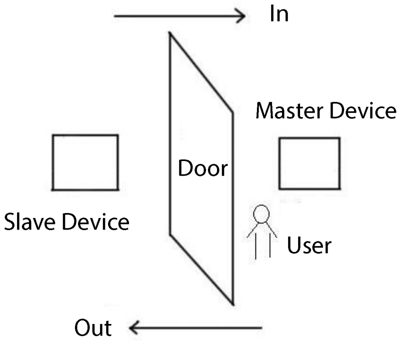
For editing, directly enter to modify the combined group, similar to the operation of adding a unlocking combination.

To delete a Combined Verification, set all access group numbers to 0.

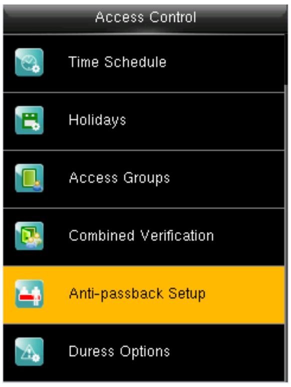
9.6 Anti-Passback Settings*

To avoid some persons following users to enter the door without verification, resulting in security problem, users can enable anti-passback function. The check-in record must match with check- out record so as to open the door.

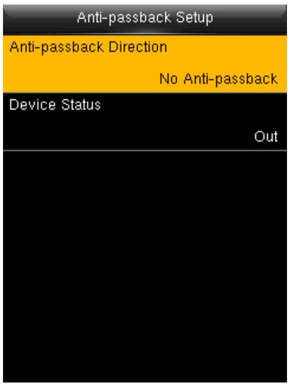
This function requires two devices to work together: one is installed inside the door (master device), the other one is installed outside the door (slave device). The two devices communicate via Wiegand signal. The Wiegand format and Output type (User ID / Badge Number) adopted by the master device and slave device must be consistent.



Operation instructions



Access Control



Anti-passback Setup

Anti-passback Direction: No Anti-passback

Device Status: Out

Press ▼ to select **Anti-Passback Setup**. Press **OK** to enter the **Anti-Passback Setup** interface.

- **Anti-Passback Direction**

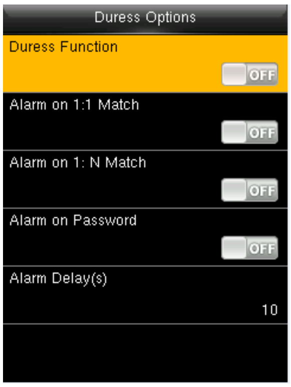
No Anti-Passback: Anti-Passback function is disabled, which means passing verification of either master device or slave device can unlock the door. Attendance state is not reserved.
Out Anti-Passback: After a user checks out, only if the last record is a check-in record can the user check out again; otherwise, the alarm will be triggered. However, the user can check in freely.
In Anti-Passback: After a user checks in, only if the last record is a check-out record can the user check in again; otherwise, the alarm will be triggered. However, the user can check out freely.
In/Out Anti-Passback: After a user checks in/out, only if the last record is a check-out record can the user check in again, or a check-in record can the user check out again; otherwise, the alarm will be triggered.
Null and Save: Anti-Passback function is disabled, but attendance state is reserved.

- **Device Status**

None: To disable the Anti-Passback function.
Out: All records on the device are check-out records.
In: All records on the device are check-in records

9.7 Duress Options Settings

When users come across duress, select duress alarm mode, the device will then open the door as usual and send the alarm signal to the backstage alarm.



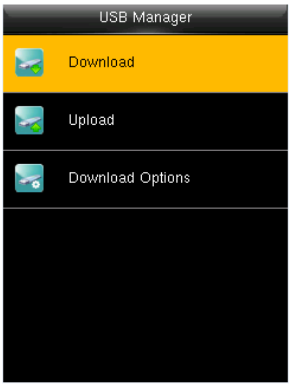
Duress Options
Duress Function OFF
Alarm on 1:1 Match OFF
Alarm on 1: N Match OFF
Alarm on Password OFF
Alarm Delay(s) 10

Duress Function: In **[ON]** state, press "Duress Key" and then press any registered fingerprint or ID Number (within 10 seconds), duress alarm will be triggered after successful verification. In **[OFF]** state, pressing "Duress Key" will not trigger the alarm.
Alarm on 1:1 Match: In **[ON]** state, when a user uses 1:1 Verification Method to verify any registered fingerprint, alarm will be triggered. In **[OFF]** state, no alarm signal will be triggered.
Alarm on 1: N Match: In **[ON]** state, when a user uses 1:N Verification Method to verify any registered fingerprint, alarm will be triggered. In **[OFF]** state, no alarm signal will be triggered.
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): When duress alarm is triggered, the device will send out alarm signal after 10 seconds (default); the alarm delay time can be changed (value ranges from 0 to 999 seconds).

12 USB Manager*

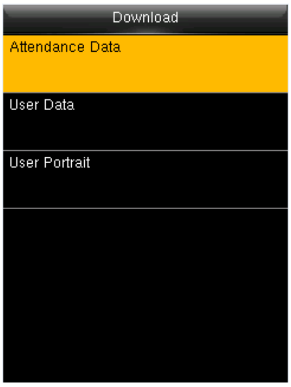
The user information, fingerprint template and attendance data in the device can be imported into related software for processing, or the user information and fingerprints can be imported into other fingerprint devices through a USB disk.

Before uploading/downloading data from/to the USB disk, insert the USB disk into the USB slot first.



Select **USB Manager** in the main menu.

12.1 USB Download

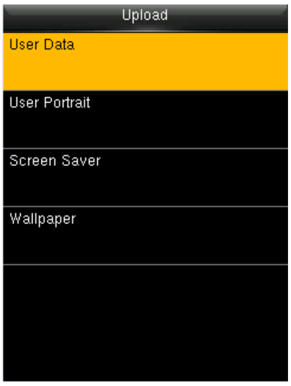


Attendance Data: To download attendance data in specified time period into USB disk.

User Data: To download all user information and fingerprints from the device into USB disk.

User Portrait: To download all user photos from the device into a USB disk.

12.2 USB Upload



User Data: To upload all the user information and fingerprints from USB disk into the device.

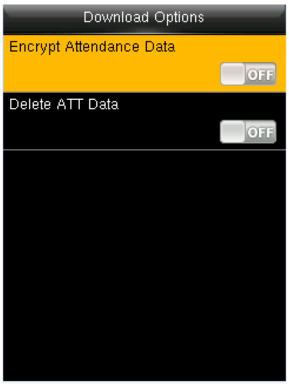
User Portrait: Upload a .JPG picture file named the user ID in a USB disk to the device, and the user portrait in the USB disk will be displayed on the device for preview. During uploading, you can choose **Upload selected picture** or **Upload all pictures**. After uploading, the portrait is displayed when the device is verifying an employee's fingerprint.

Screen Saver: To upload all screen savers from USB disk into the device. You can choose **[Upload selected picture]** or **[Upload all pictures]**. The images will be displayed on the device's main interface after upload

Wallpaper: To upload all wallpapers from USB disk into the device. You can choose **[Upload selected picture]** or **[Upload all pictures]**. The images will be displayed on the screen after upload

12.3 Download Options Settings

To encrypt attendance data in the USB disk or delete attendance data.



Download Options

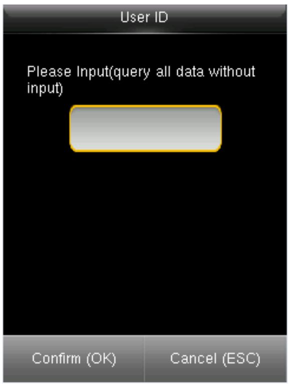
Encrypt Attendance Data OFF

Delete ATT Data OFF

13 Attendance Search

After an employee successfully checks in and out, the record will be saved in the device. The attendance search allows employees to query employee attendance records.

Searching Attendance Record

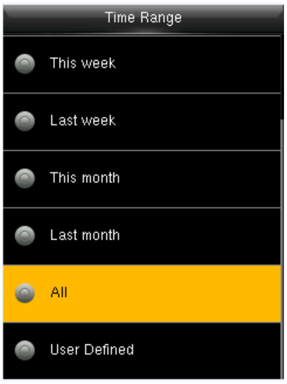


User ID

Please Input(query all data without input)

Confirm (OK) Cancel (ESC)

Enter the user ID of an employee whose attendance records need to be queried. If no user ID is entered, the attendance records of all employees are queried.



Time Range

○ This week

○ Last week

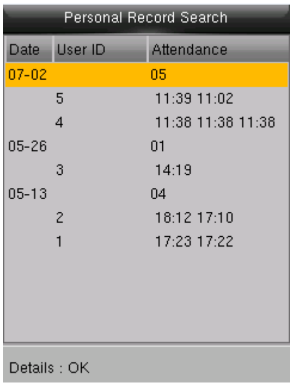
○ This month

○ Last month

○ All

○ User Defined

Select the time period for query.

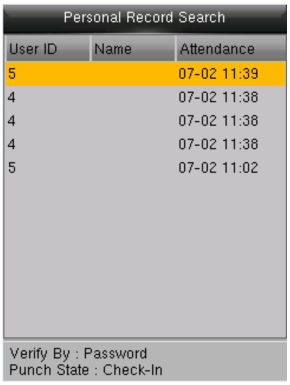


Personal Record Search

Date	User ID	Attendance
07-02		05
	5	11:39 11:02
	4	11:38 11:38 11:38
05-26		01
	3	14:19
05-13		04
	2	18:12 17:10
	1	17:23 17:22

Details : OK

Press ▼ to select a attendance record and press **M/OK**.



Personal Record Search

User ID	Name	Attendance
5		07-02 11:39
4		07-02 11:38
4		07-02 11:38
4		07-02 11:38
5		07-02 11:02

Verify By : Password
Punch State : Check-In

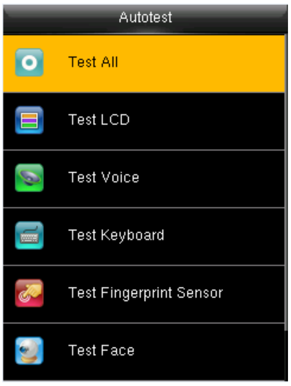
Record details

User ID: user ID of an employee whose attendance records need to be queried. If no user ID is entered, the attendance records of all employees are queried. After a user ID is entered, attendance records of the employee with the user ID are queried.

Time Range: Select the time period for query, including user defined, yesterday, this week, last week, this month, last month and all time periods.

14 Autotest

To automatically test whether all modules in the device function properly, which include the LCD, voice, keyboard, fingerprint sensor and RTC (Real-Time Clock).



Test All: To test LCD, voice, keyboard, fingerprint sensor and RTC. During the test, press **[M/OK]** to continue to the next test, while press **[ESC]** to exit the test.

Test LCD: To test the display effect of LCD screen by displaying full color, pure white, and pure black to check whether the screen displays colors properly. During the test, press **[M/OK]** to continue to the next test, while press **[ESC]** to exit the test.

Test Voice: The device automatically tests whether the voice files stored in the device are complete and the voice quality is good. During the test, press **[M/OK]** to continue to the next test, while press **[ESC]** to exit the test.

Test Keyboard: To test all keys to see if every key functions properly. Press any key in the **Keyboard** testing interface; if the pressed key is consistent with the key sign shown on the screen, then the key functions properly. Press **[M/OK]** or [ESC] to exit the test.

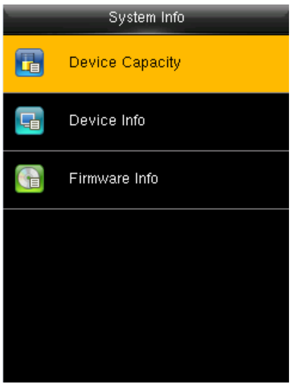
Test Fingerprint Sensor: To test the fingerprint sensor by pressing fingerprint to check if the collected fingerprint image is clear. When pressing fingerprint on the sensor, the image will be displayed on the screen. Press **[M/OK]** or **[ESC]** to exit the test.

Test Face: The device automatically tests whether the camera is in proper operation and checks whether the captured images are clear and usable. Press **ESC** to quit this test.

Test Clock RTC: To test the Real-Time Clock. The device tests whether the clock works properly and accurately by checking the stopwatch. Press **[M/OK]** to start counting time, and press it again to stop counting, to see if the stopwatch counts time accurately. Press **[ESC]** to exit the test.

15 System Information

Check data capacity, device and firmware information.



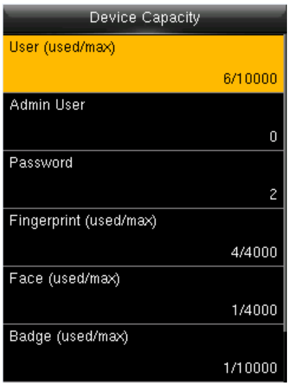
System Info

Device Capacity

Device Info

Firmware Info

Select "System Information" in the main menu.



Device Capacity

User (used/max) 6/10000

Admin User 0

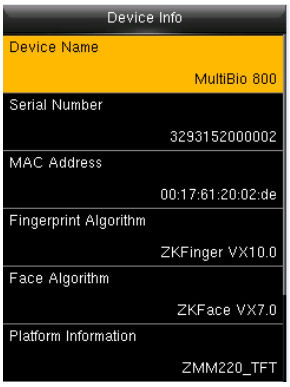
Password 2

Fingerprint (used/max) 4/4000

Face (used/max) 1/4000

Badge (used/max) 1/10000

Data capacity information



Device Info

Device Name MultiBio 800

Serial Number 3293152000002

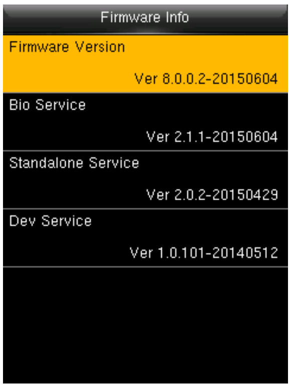
MAC Address 00:17:61:20:02:de

Fingerprint Algorithm ZKFinger VX10.0

Face Algorithm ZKFace VX7.0

Platform Information ZMM220_TFT

Device information



Firmware Info

Firmware Version Ver 8.0.0.2-20150604

Bio Service Ver 2.1.1-20150604

Standalone Service Ver 2.0.2-20150429

Dev Service Ver 1.0.101-20140512

Firmware information

Device Capacity: To display the number of registered users, administrators, passwords, fingerprints, badges, attendance logs and so on.

Device Info: To display the device name, serial number, MAC address, fingerprint algorithm, platform information, manufacturer and manufacturer date.

Firmware Info: To display the firmware version, Bio service, push service, standalone service and Dev service.

16 Appendices

Appendix 1 Image Uploading Rule

- **User photo:** It is required to create a file named as "**photo**" er the USB disk file, and put user photos into the file. The capacity is 8000 images, with each of them not exceeding 15k. The image name is x.jpg (x is the actual user ID, max. 9 digits). The photo format must be JPG.
- **Advertising image:** It is required to create a file named as "**advertise**"under the USB disk file, and put advertising images into the file. The capacity is 20 images with each of them not exceeding 30k. Image name and format are not restricted.
- **Wallpaper:** It is required to create a file named as "**wallpaper**"under the USB disk file, and put wallpapers into the file. The capacity is 20 images with each of them not exceeding 30k. Image name and format are not restricted.

✍**Note:** When each user photo and attendance photo does not exceed 10k, the device can save a total number of 10000 user and attendance photos.

Appendix 2 Wiegand Introduction

Wiegand26 Protocol is a standard protocol on access control developed by the Access Control Standard Subcommittee affiliated to the Security Industry Association (SIA). It is a protocol used for contactless IC card reader port and output.

The protocol defines the port between the card reader and controller which are widely used in access control, security and other related industries. This has standardized the work of card reader designers and controller manufacturers. The access control devices produced by our company also apply this protocol.

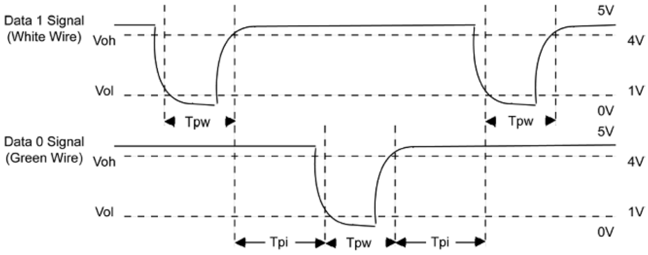
Digital Signal

Figure 1 shows the sequence diagram of the card reader sending digital signal in bits to the access controller. The Wiegand in this diagram follows the SIA access control standard protocol, which targets at 26-bit Wiegand card reader (with a pulse time within 20 μs to 100 μs and pulse hopping time within 200 μs and 20 ms). Data1 and Data0 signals are high level (greater than Voh) until the card reader is ready to send a data stream. The card reader send out asynchronous low level pulse (less than vol), transmitting data stream via Data1 or Data0 wire to access control box (as the sawtooth wave in figure 1). Data1 and Data0 pulses do not overlap or synchronize. Figure 1 shows the maximum and minimum pulse width (successive pulses) and pulse hopping time (the time between two pulses) allowed by the F series fingerprint access control terminals.

Table1: Pulse Time

Sign	Definition	Card Reader Typical Value
Tpw	Pulse Width	100 µs
Tpi	Pulse Interval	1 ms

Figure1: Sequence Diagram



Appendix 3 Statement on Human Rights and Privacy

Dear Customers:

Thank you for choosing the hybrid biometric products designed and manufactured by us. As a world-renowned provider of biometric technologies and services, we pay much attention to the compliance with the laws related to human rights and privacy in every country while constantly performing research and development.

We hereby make the following statements:

1. All of our fingerprint recognition devices for civil use only collect the characteristic points of fingerprints instead of the fingerprint images, and therefore no privacy issues are involved.
2. The characteristic points of fingerprints collected by our products cannot be used to restore the original fingerprint images, and therefore no privacy issues are involved.
3. We, as the equipment provider, shall not be held legally accountable, directly or indirectly, for any consequences arising due to the use of our products.
4. For any dispute involving the human rights or privacy when using our products, please contact your employer directly.

Our fingerprint products for police use, or development tools support the collection of the original fingerprint images. As for whether such a type of fingerprint collection constitutes an infringement of your privacy, please contact the government or the final equipment provider. We, as the original equipment manufacturer, shall not be held legally accountable for any infringement arising thereof.

The law of the People’s Republic of China has the following regulations regarding the personal freedom:

1. Unlawful arrest, detention or search of citizens of the People's Republic of China is prohibited; infringement of individual privacy is prohibited.
2. The personal dignity of citizens of the People's Republic of China is inviolable.
3. The home of citizens of the People's Republic of China is inviolable.
4. The freedom and privacy of correspondence of citizens of the People's Republic of China are protected by law.

At last we stress once again that biometrics, as an advanced recognition technology, will be applied in a lot of sectors including e-commerce, banking, insurance and legal affairs. Every year people around the globe suffer from great loss due to the insecurity of passwords. The biometric products actually provide adequate protection for your identity under a high security environment.

Appendix 4 Environment-Friendly Use Description

- The Environment Friendly Use Period (EFUP) marked on this product refers to the safety period of time in which the product is used under the conditions specified in the product instructions without leakage of noxious and harmful substances.
- The EFUP of this product does not cover the consumable parts that need to be replaced on a regular basis such as batteries and so on. The EFUP of batteries is 5 years.

Names and Concentration of Toxic and Hazardous Substances or Elements

Parts Name	**Toxic and Hazardous Substances or Elements**					
	Pb	**Hg**	**Cd**	**Cr6+**	**PBB**	**PBDE**
Chip resistor	×	○	○	○	○	○
Chip capacitor	×	○	○	○	○	○
Chip inductor	×	○	○	○	○	○
Chip diode	×	○	○	○	○	○
ESD components	×	○	○	○	○	○
Buzzer	×	○	○	○	○	○
Adapter	×	○	○	○	○	○
Screws	○	○	○	×	○	○

○: Indicates that this toxic or hazardous substance contained in all of the homogeneous materials for this part is below the limit requirement in SJ/T11363-2006.

×: Indicates that this toxic or hazardous substance contained in at least one of the homogeneous materials for this part is above the limit requirement in SJ/T11363-2006.

Note: 80% of the parts in this product are manufactured with non-hazardous environment-friendly materials. The hazardous substances or elements contained cannot be replaced with environment-friendly materials at present due to technical or economical constraints.