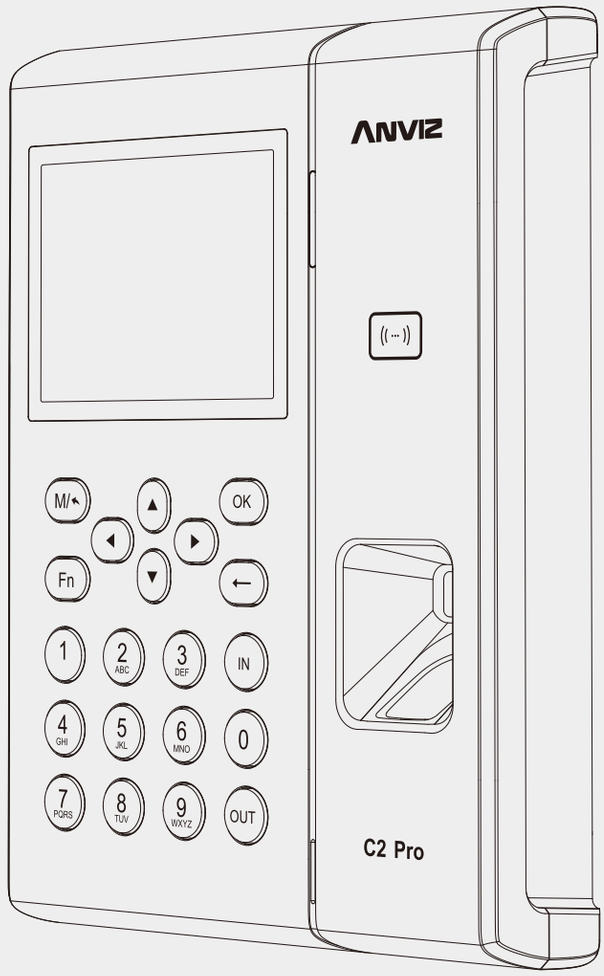
ANVIZ

User Manual V2.0

# C2 Pro

## Fingerprint & Card Access Control and Time Attendance Terminal




Need help?

To get help or learn more

https://www.anviz.com/download/go/c2-pro-user-manual.html

## Content


Safety Instructions ---- 3

Introduction ---- 3

- Components ---- 3
- Appearance Description ---- 3
- Installation ---- 4
- Installation Position ---- 5
- Installation Steps ---- 5
- Wiring Connection ---- 6

Device Operations ---- 8

- General Settings ---- 8
- Enroll Face ---- 9
- User Management ---- 10

Add User 10
Modify User 11
Delete User 11
Search User 12
Admin Level 12
Data Menu 12
Records Management 13
Import Users 13
Export Users 13
Backup DB 14
Restore DB 14
Report form 15
Communication Settings 15
Ethernet 15
WIFI 16
Internet 17
Comm. Mode 17
Cloud 19
Settings Menu 19
Device Information 20
Time 20
Time Settings 20
DST 21
Display settings 21
Basic Information 22
Update 22

Test 23
Advanced Settings 24
T&A (Time Attendance settings) 24
Application 25
Access 25
Time Zone 26
Group 26
Shifts 26
Measures (Suitable for FaceDeep 3 IRT and QR Series) 27
Thermometry 27
Mask 28
EU QR Code 29
FN Settings 29
Auto FN 29
Bluetooth 30

## Safety Instructions

Please read this safety instructions before you use the product to prevent injury to yourself and others, and prevent property damage. The term 'product' in this manual refers to the product and any items provided with the product.

● Do not install or repair the product arbitrarily. This may result in electric shock, fire, or product damage.

● Damages caused by any modifications or failure to follow installation instructions can void the manufacturer's Warranty.

● Do not install the product in a place with direct sunlight, humidity, dust, soot, or a gas leak. This may result in electric shock or fire.

● The optimal working environment of C2Pro is indoor. The device function fully under temperature: -10°C~50°C (14°F~122°F), humidity: 20-90%.

● Do not use damaged power supply adaptors, plugs, or loose electrical sockets.

Unsecured connections may cause electric shock or fire. The recommended power to C2Pro terminal is DC 12V ~ 2A.

● Do not drop the product or cause impacts to the product. The product may malfunction.

● When cleaning the product, mind the following (please take care of following). Wipe the product with a clean and dry towel (cloth or cotton).

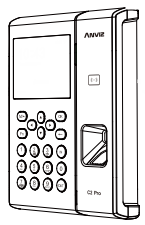
● If you need to sanitize the product, moisten the cloth or the wipe with a proper amount of rubbing alcohol and gently clean all exposed surfaces including fingerprint sensor. Use rubbing alcohol (containing 70% Isopropyl alcohol) and a clean, non-abrasive cloth like lens wipe.

● Do not apply liquid directly to the surface of the product.

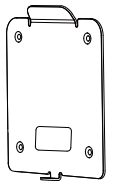
● Do not use the product for anything other than its intended use.

## Introduction

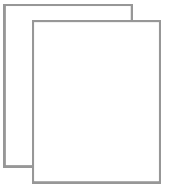
### Components



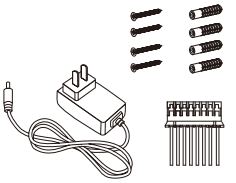
C2 Pro



Mounting Bracket

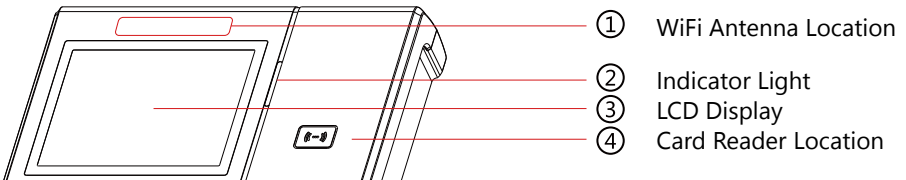


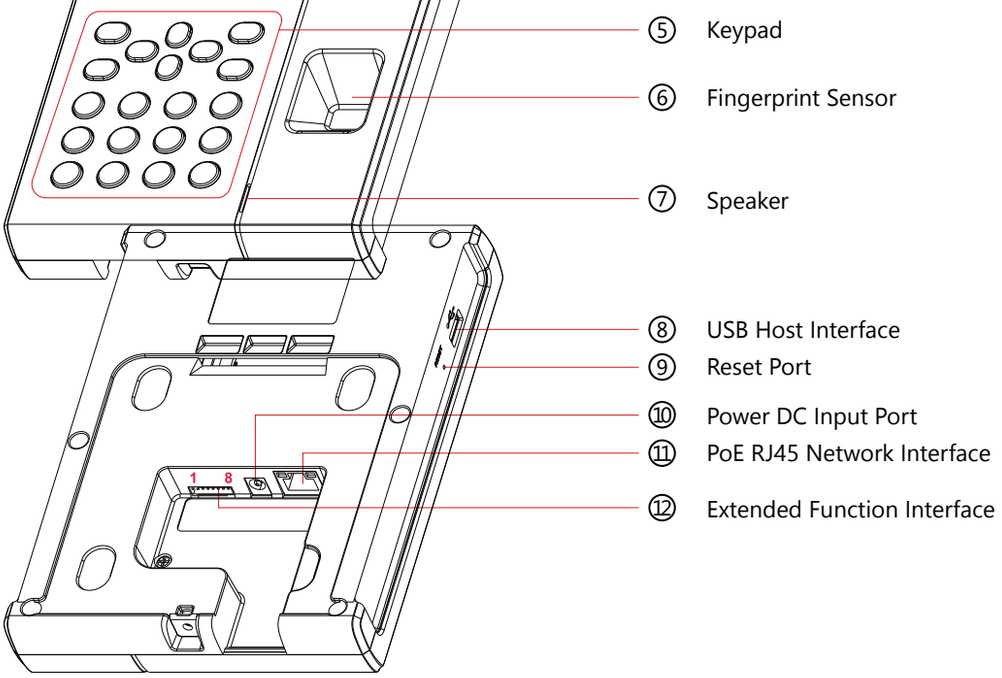
Quick Guide



Accessories

### Appearance Description



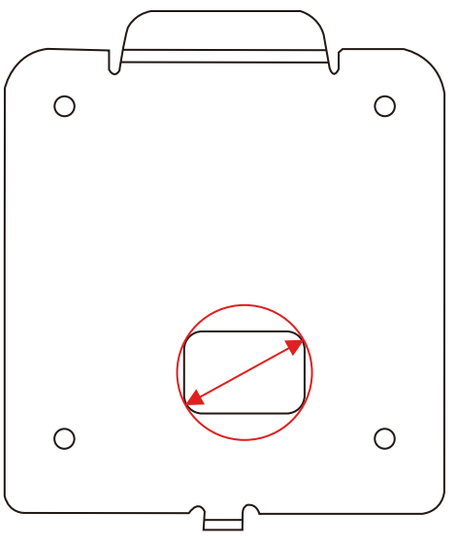



## Installation

**Step 1:**

Keep the mounting bracket parallel to the ground, at the height of 1.2m (47.24”) from the floor.

Drill 4 screw holes on the wall according to the mounting bracket.



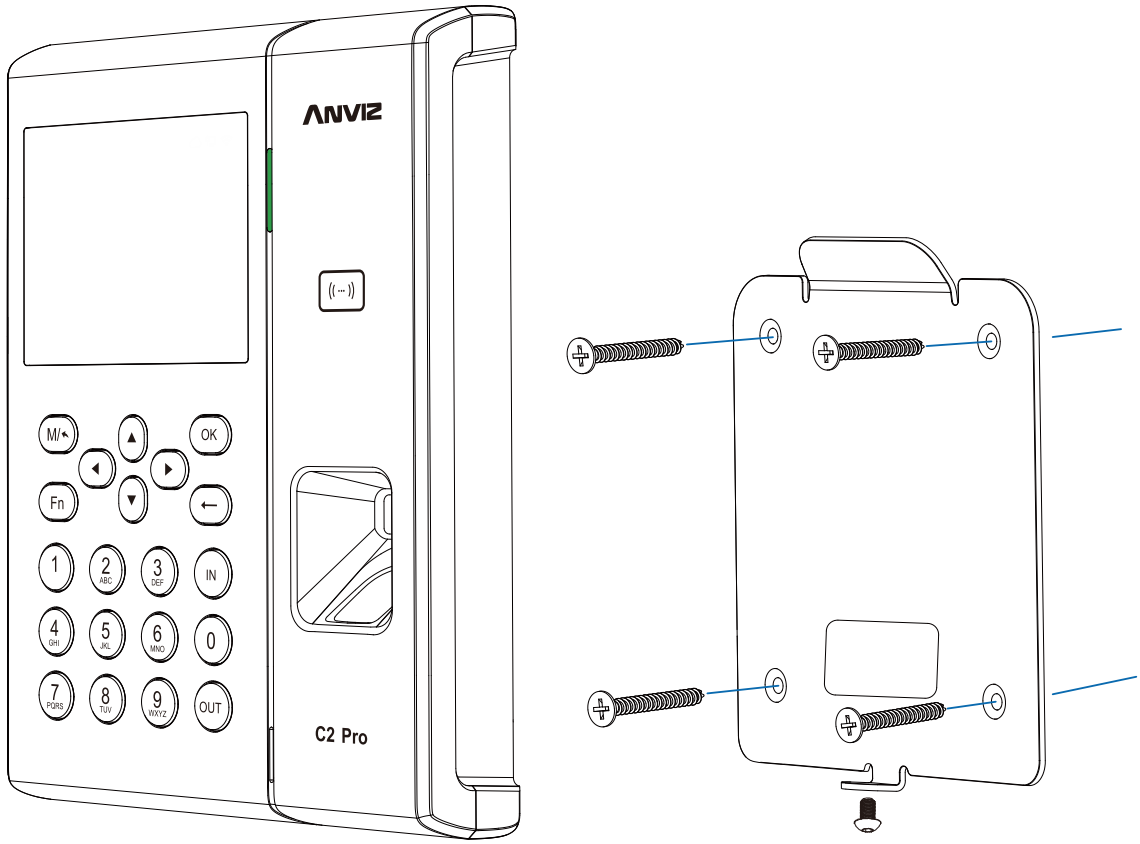
**Note:**

Outlet Hole D= 30mm ( 1.18 ” )

Diill outlet hole for device wiring

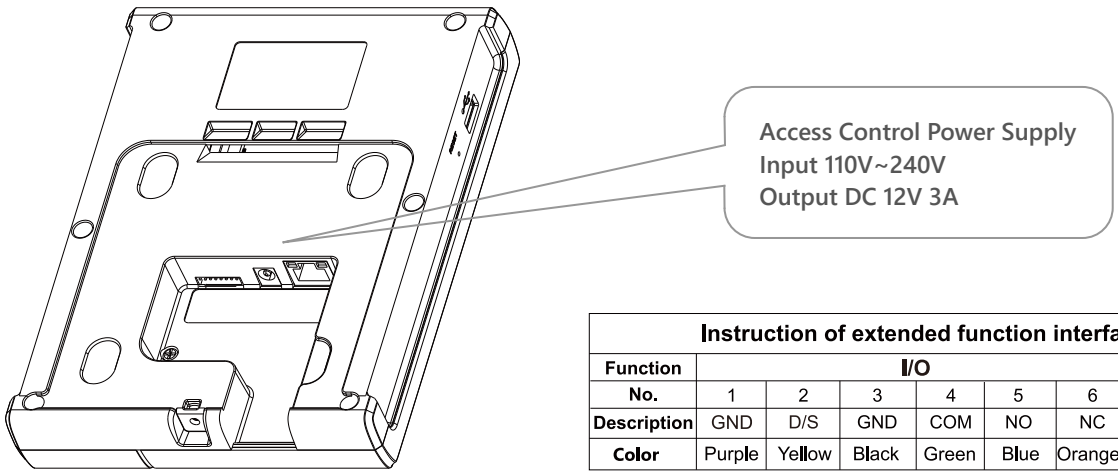
**Step 2:**

Please punch out the tail lines from the outlet hole before installing the mounting bracket and use the screws to fix the mounting bracket on the wall. Use the screwdriver to tighten the screws, follow the direction indicated below to complete the installation.

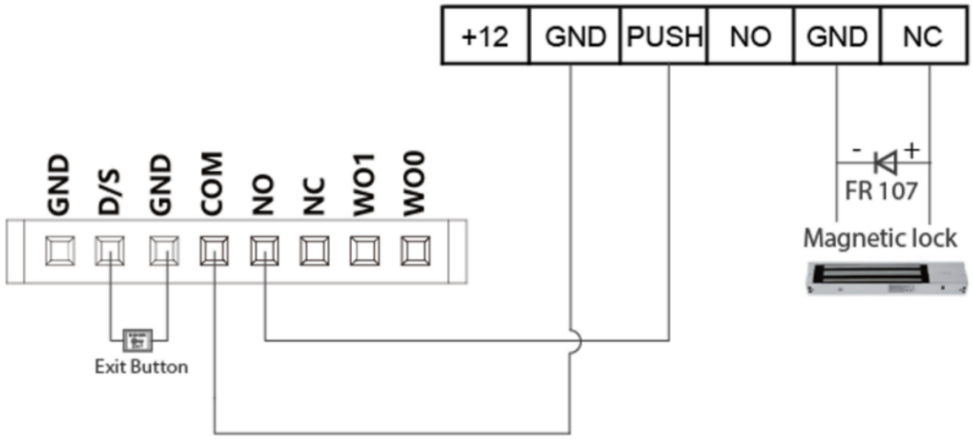



## Wiring Connection

### Wiring with Access Control Power Supply

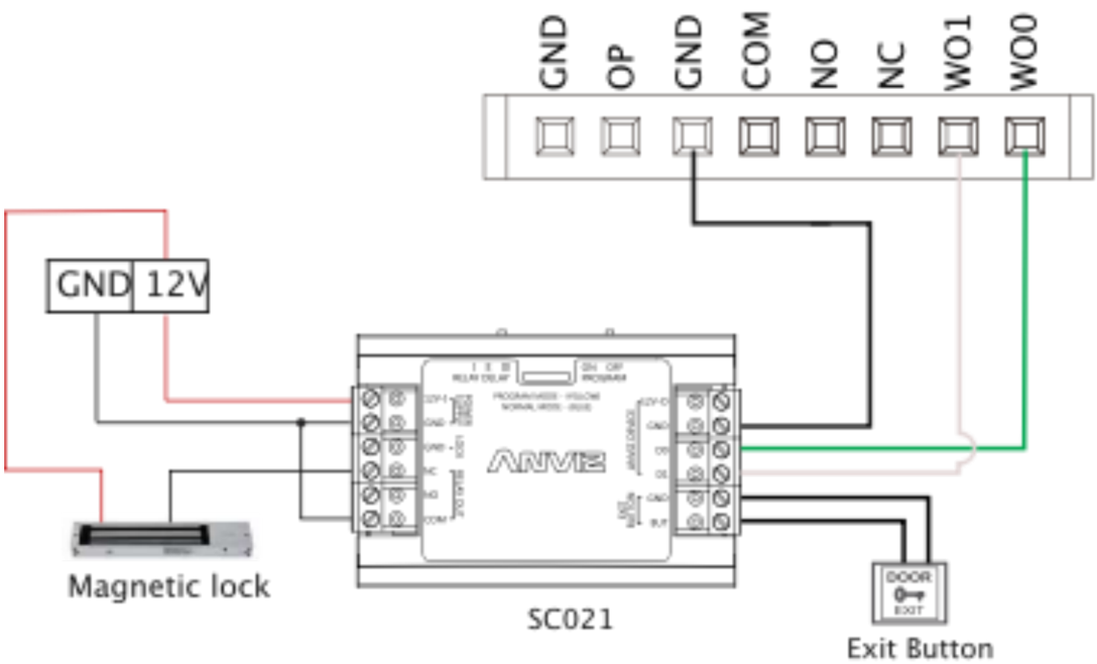



| Instruction of extended function interface | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Function** | **I/O** | | | | | | **Wiegand Output** | |
| **No.** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| **Description** | GND | D/S | GND | COM | NO | NC | WO1 | WO0 |
| **Color** | Purple | Yellow | Black | Green | Blue | Orange | White | Green |




### Wiring with Access Control Unit – SC011

SC011 and the C2Pro/C2CPro devices are authorized by Anviz wiegand to form a distributed access control system. Please contact support@anviz.com for more information.



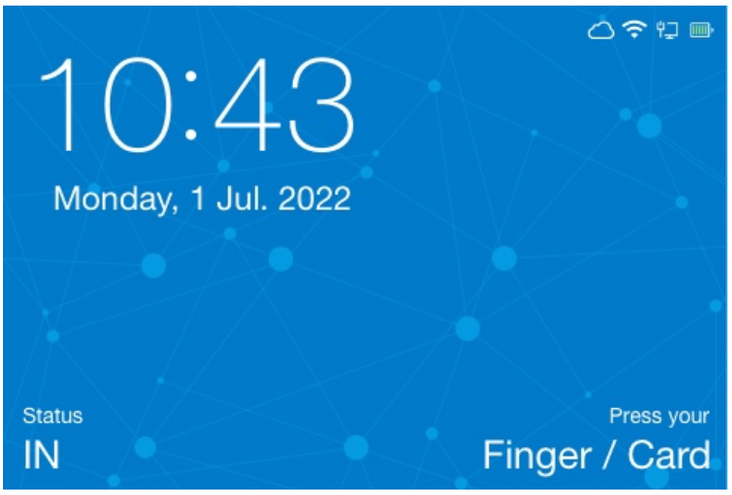

**Suggestion**: add more details about the wiegand settings for SC011 + Facedeep3, example:

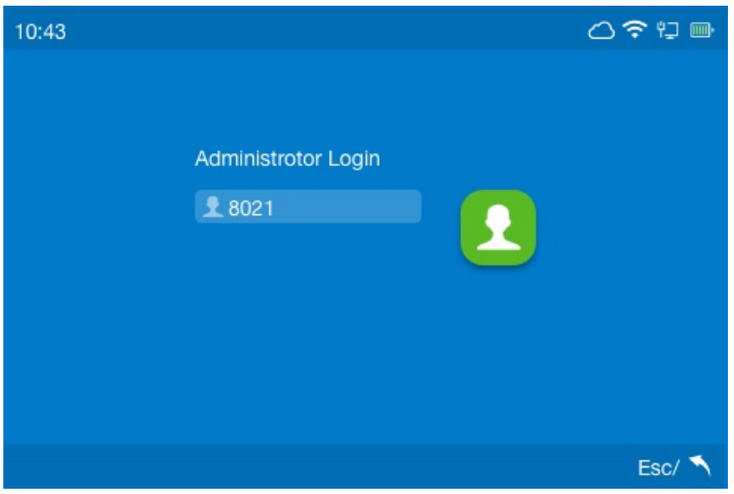
Please Configure the Wiegand Output of C2 PRO to Anviz Wiegand option, (Refer to Access Setting )and use the SC011 quickguide to configure the Wiegand communication correctly.

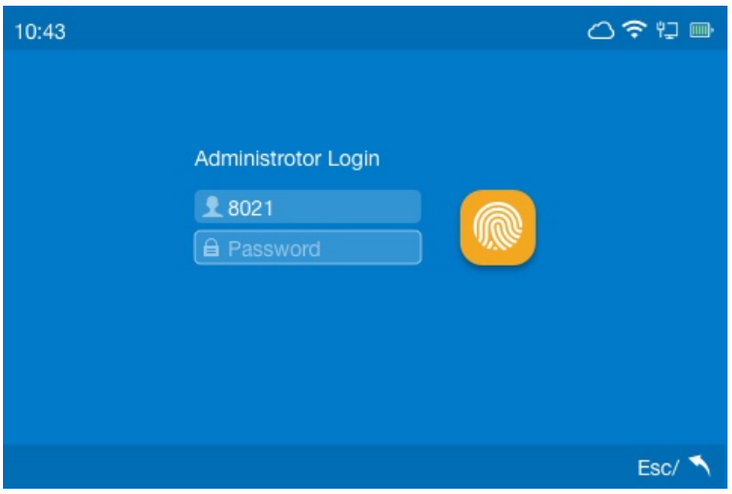
## Device Operation

## General Settings

Power On the terminal or On the Standby Interface, Press M Key on the keypad to activate the device.

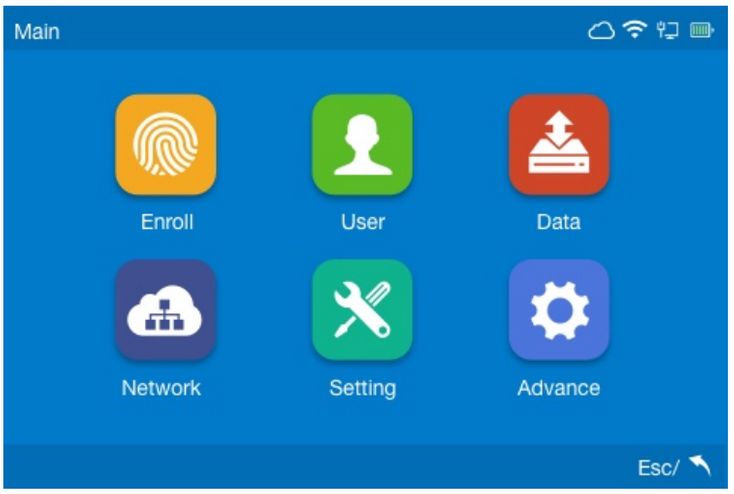



Press “0” as Administrator ID and press OK to continue, input the default password “12345” to access the main menu.

## Default administrator account: ID 0 and default password 12345




Menu Option：

**Enroll**: Shortcut icon to quick register users' fingerprint.

**User**: To Add, Modify, Search and Delete basic user information.

**Data**: Inquire user records on the device, import and export user records and user information, backup and restore device database, directly export the excel format report to the USB drive.

**Network**: Setup device network. Wi-Fi, TCP/IP and Cloud setup.

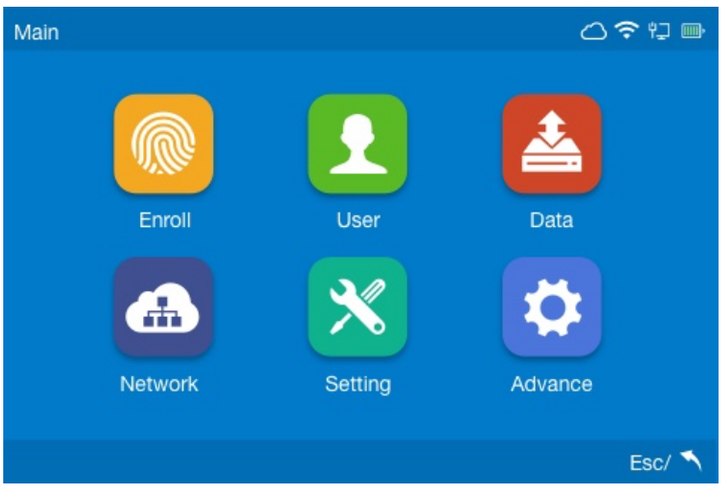
**Settings**: Device hardware basic parameter setup. Include time, device basic information, language display and firmware upgrade.

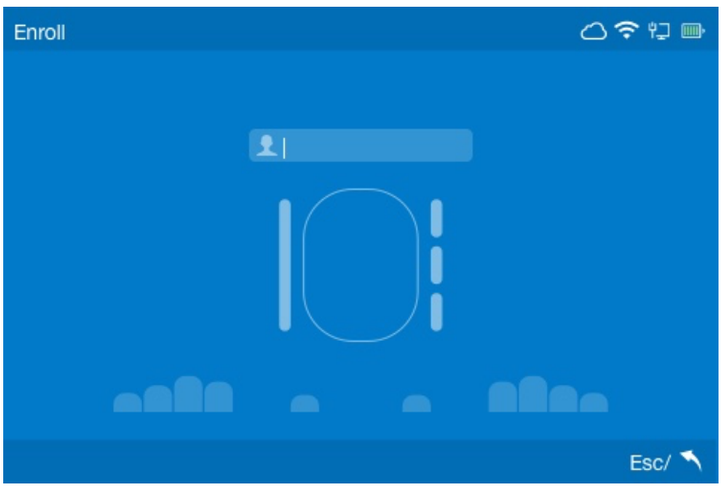
**Advanced**: Time attendance, Access Control, Default Verification mode and Automatic switch time attendance status.

> **Note:**
>
> To ensure the security of the device, we recommend modifying the default administrator password the first time you use the C2Pro.
>
> For detailed operating instructions, please see section "Admin Level".

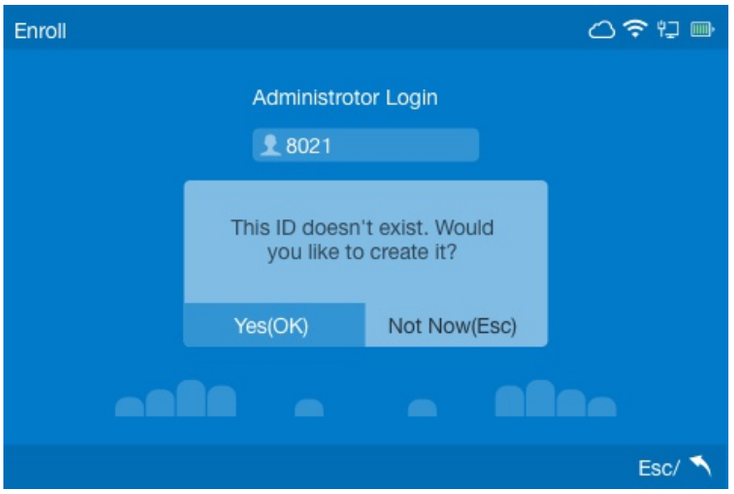
## Enroll

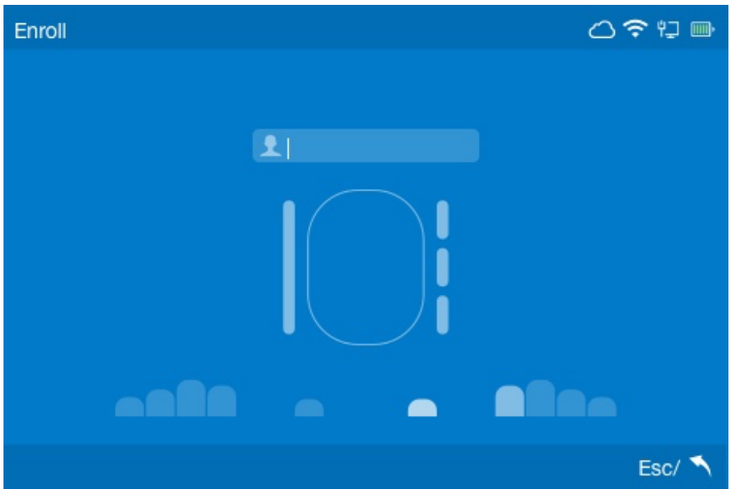
Tap on "Enroll" to enroll user Fingerprint quickly.

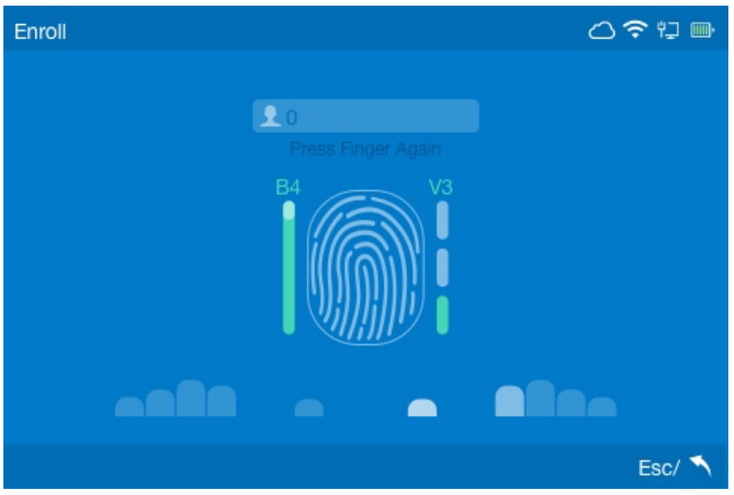


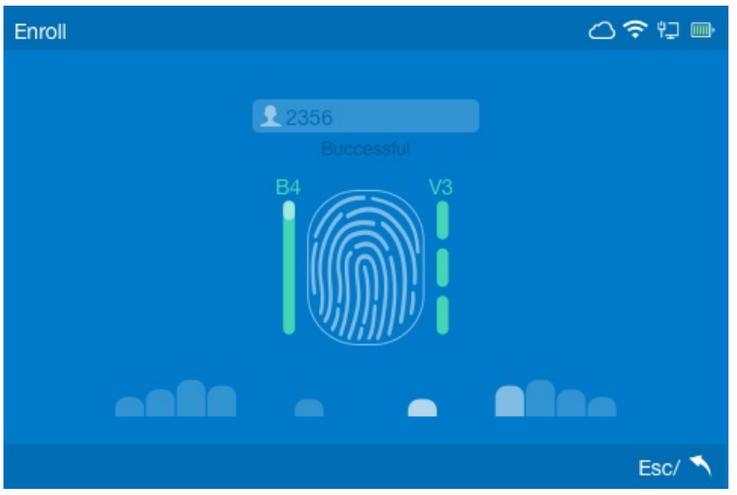




Input the unique identification number as User ID and tap "OK" to create a new User ID in the device. Press "OK" to continue to enroll user Fingerprint.



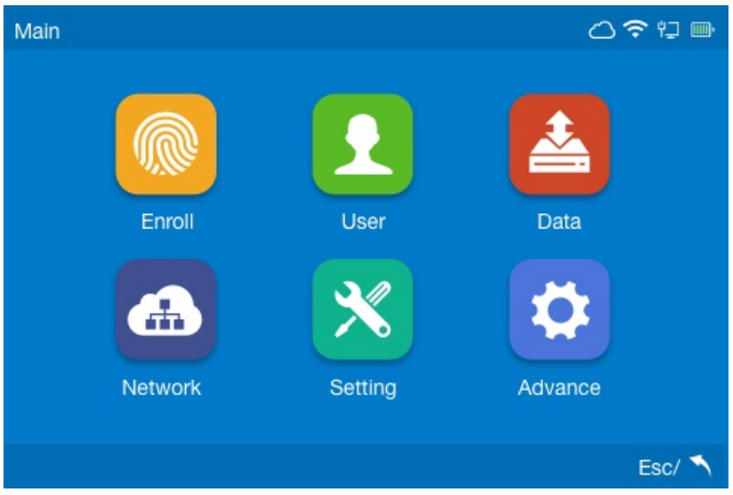



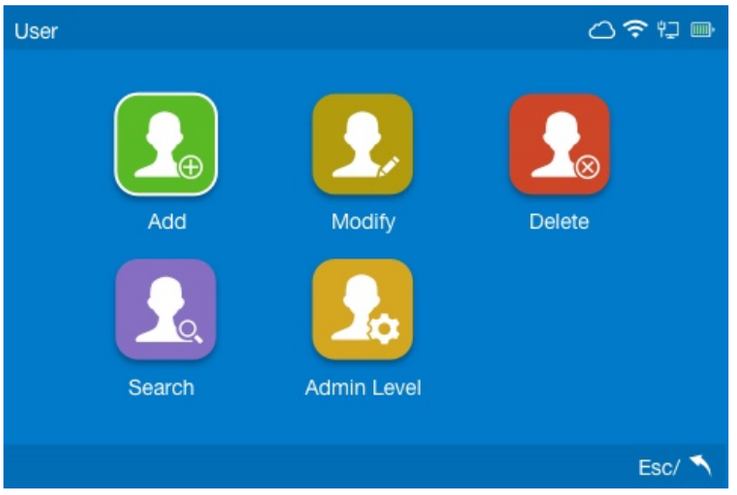

Please press the same finger on the sensor for three times until register success.

The device will automatically continue to register another fingerprint. Tap “M” back to exit the finger enrollment, and back to main menu.

## User

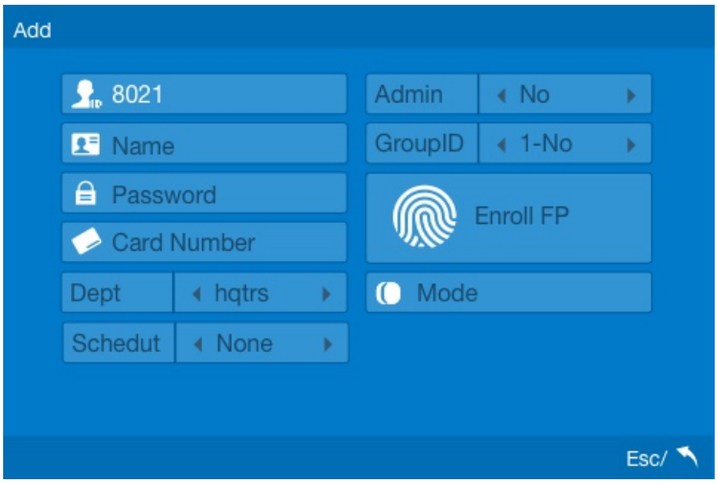
Tap on the User icon to User management interface.




## Add User

Tap on “Add” to create a new user. Input the user basic information.




**Note:**

**Enroll User ID**: The User ID is required and unique for each user

**Enroll User Password**: Input the maximum 6 digits as password

**Enroll User RFID Card**: Swipe the RFID Card on the device RFID Card read area, it will display the RFID Card number in the Card text bar.

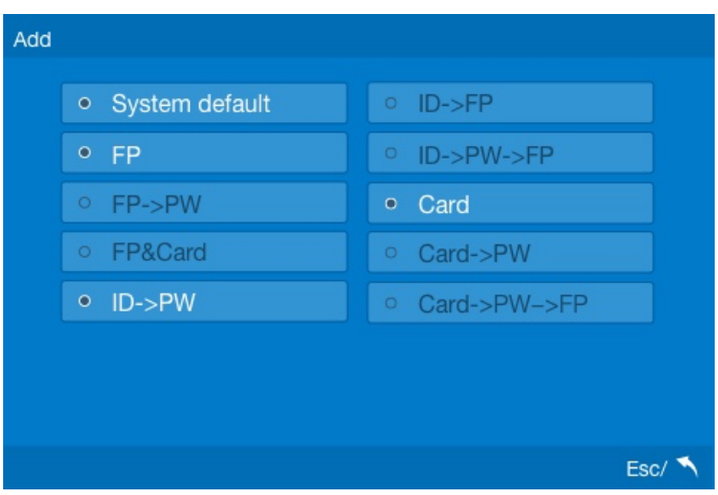
**Admin**: The device support different roles for user. (up to 17 roles. The default is User). For detailed operating instructions, please see Section “Admin Level”;

**Group ID**: The device supports 16 access control groups (The Default is Group 1, with whole period access control permission).

**Register FP**: Enroll user fingerprint.

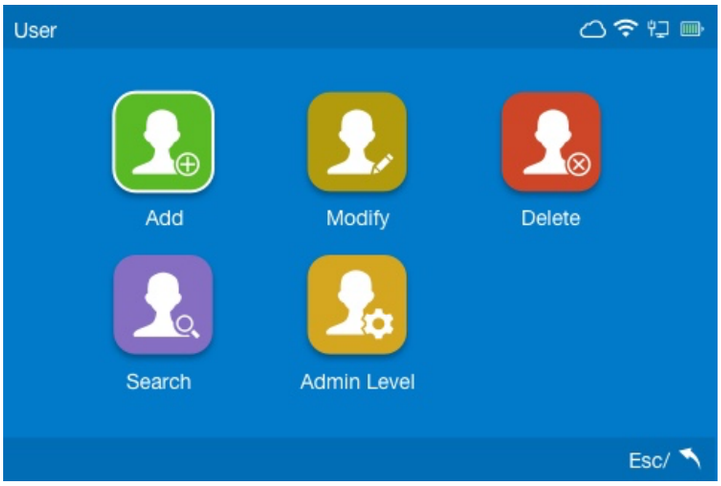
**Mode**: To setup use verify mode.

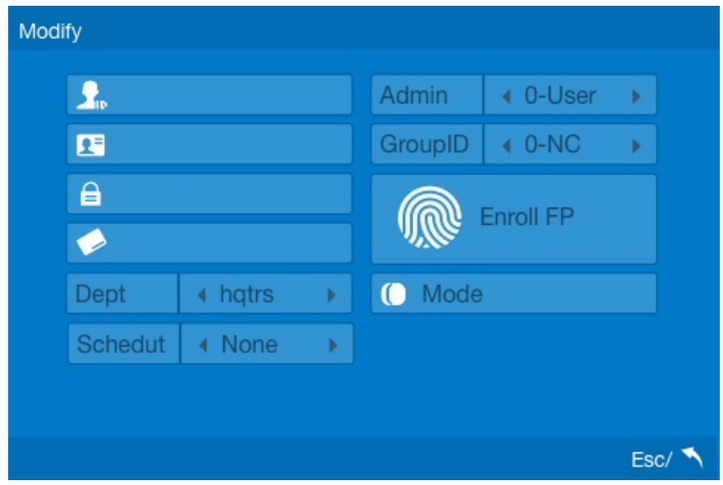
**System default**: Modify the authentication method. Unselect the “System default” first.



## Modify User

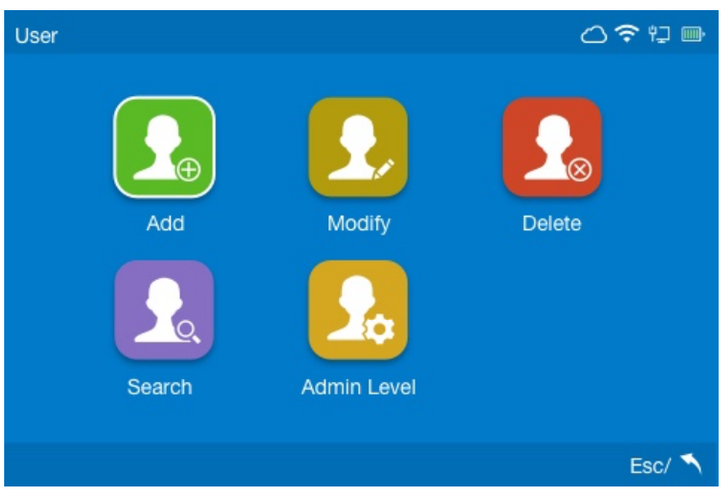
Tap on “Modify” to edit registered user. Input the registered user ID to modify user information and the fingerprint template.

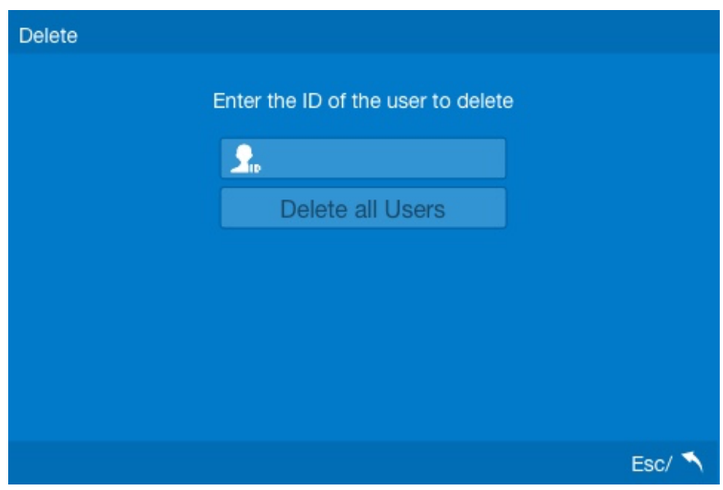


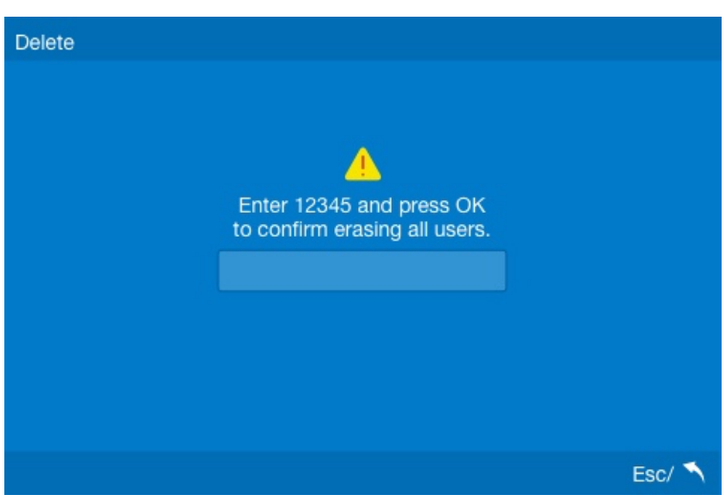

## Delete User

Tap on “Delete” to user delete interface. Please input the user ID you want to delete and click “yes” to confirm the operation.



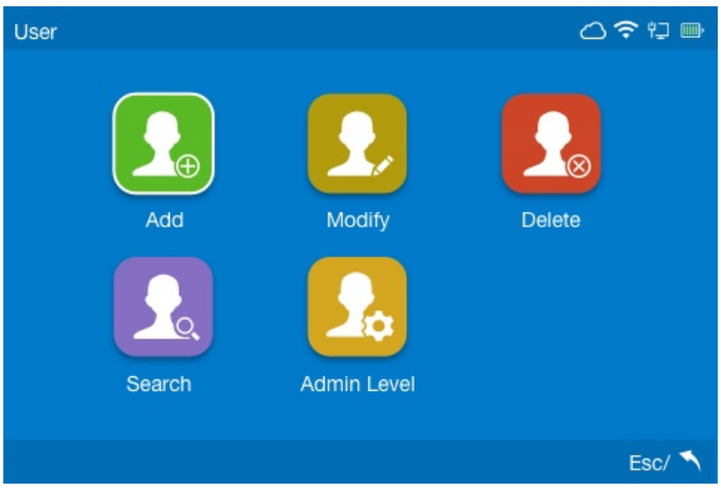



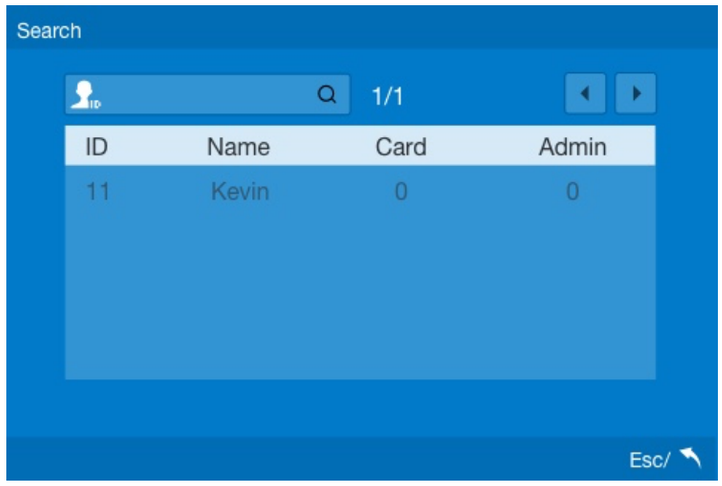

Delete all Users (Caution): Click “Delete all Users”. The device will ask to confirmation, input the super admin password to confirm the operation, default: “12345”



## Search

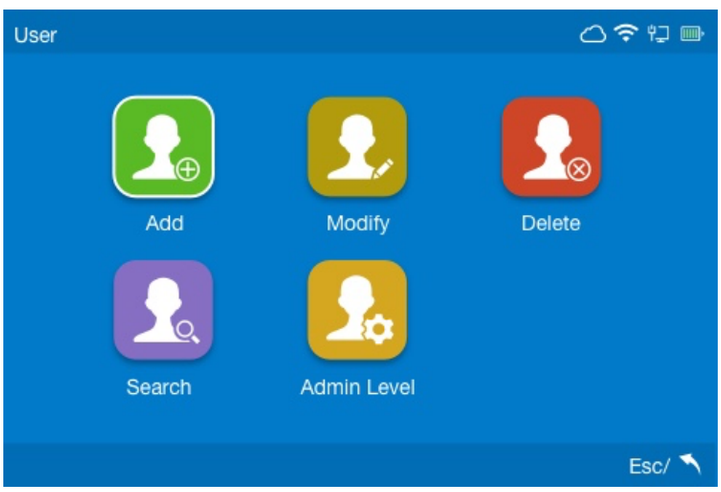
Click on “Search” to search user.  Input the user ID in the upper left corner, press “OK” for user search.
Press Directional keys to select the user and press “OK” to modify the user information.

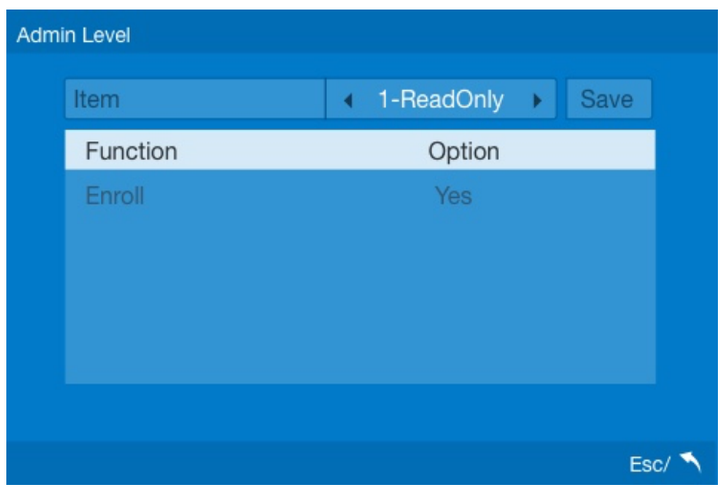


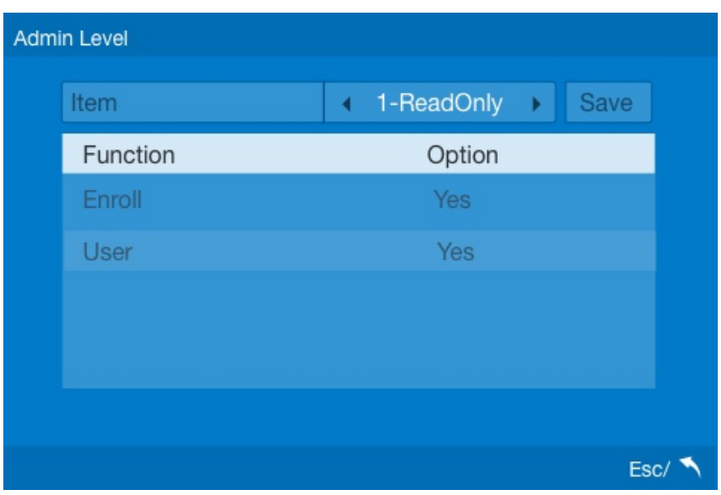

## Admin Level

Tap on “Admin Level” to setup the admin role privilege.



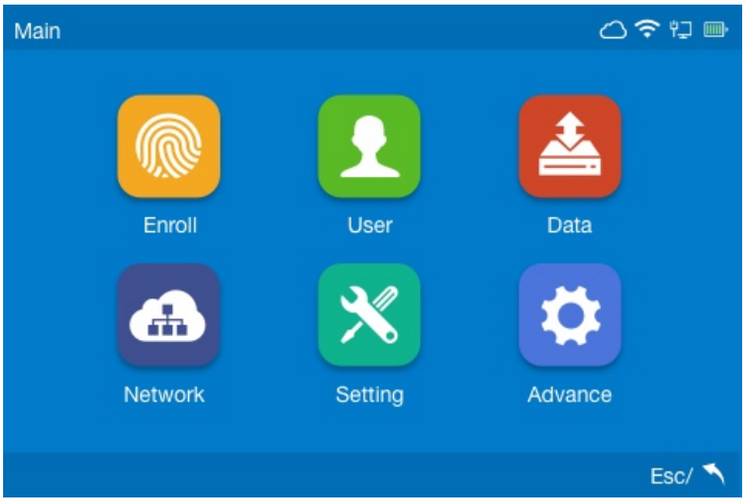



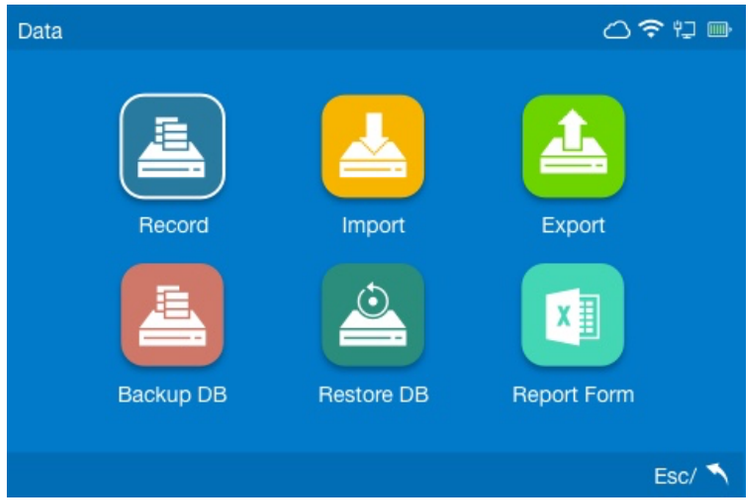

Press “Left” and “Right” Directional keys to select the Admin item from 1~16 and press “Up” and “Down”
directional key to select the permission of the Administrator.



## Data Menu

Click on the “Data” icon to access the time attendance data management interface.

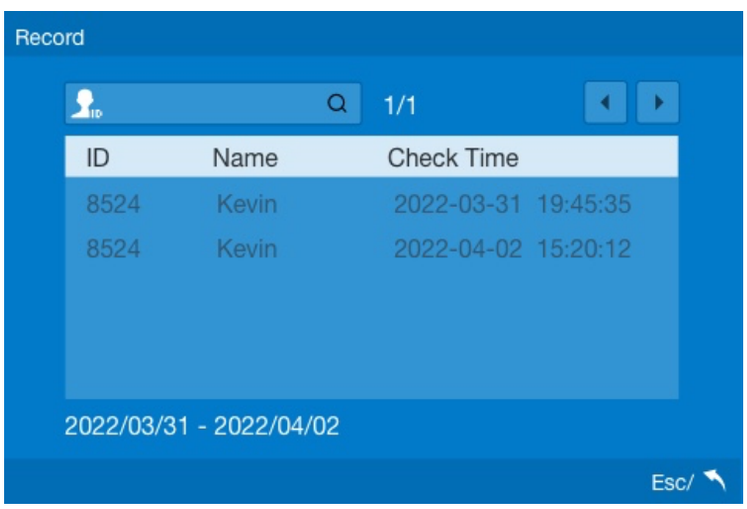



## Record

Click on the Record item to access the record interface, Press “Left” and “Right” Directional keys to select the data for the record and Input the user id in the upper left corner, press “OK” for user records search.

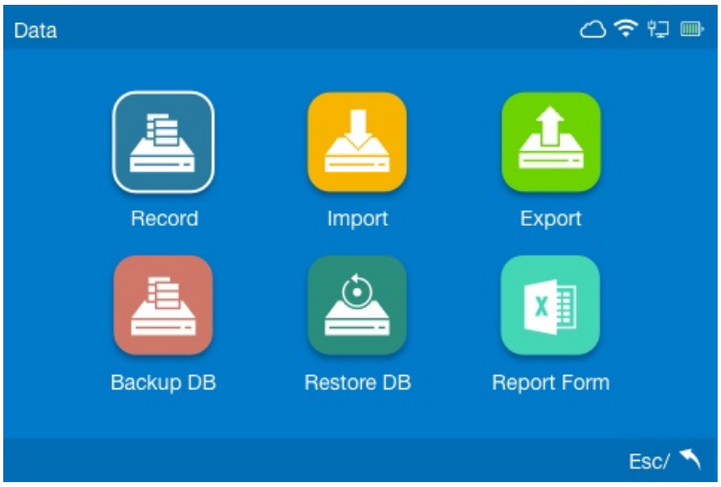
Press “Left” and “Right” Directional keys to page up and page down search the user records.

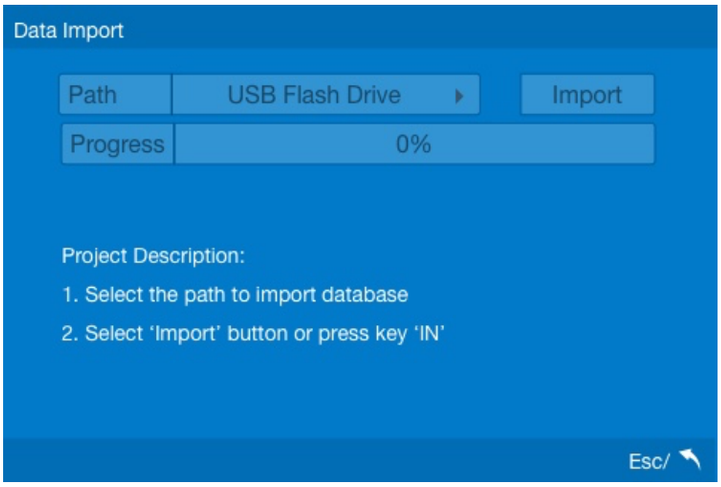



## Import

Click Import icon to access the data import interface. The terminal will import the data from USB Flash Driver.

You can upload user information from the CrossChex software or from another devices, via the USB disk driver.

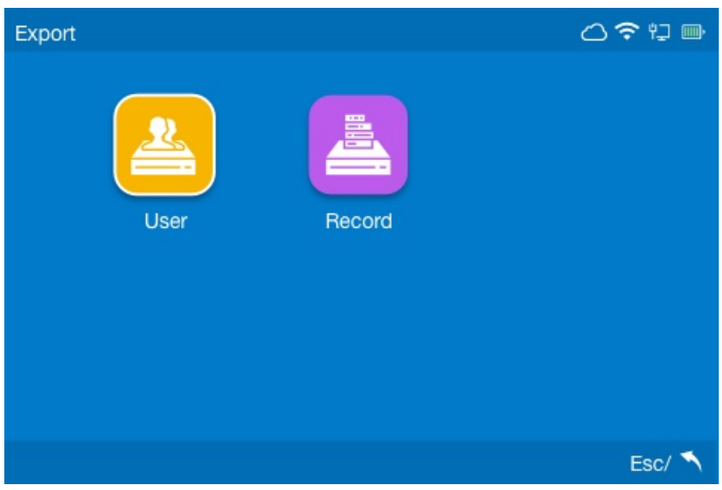



Notice : The USB records cannot import from CrossChex Software to terminal.

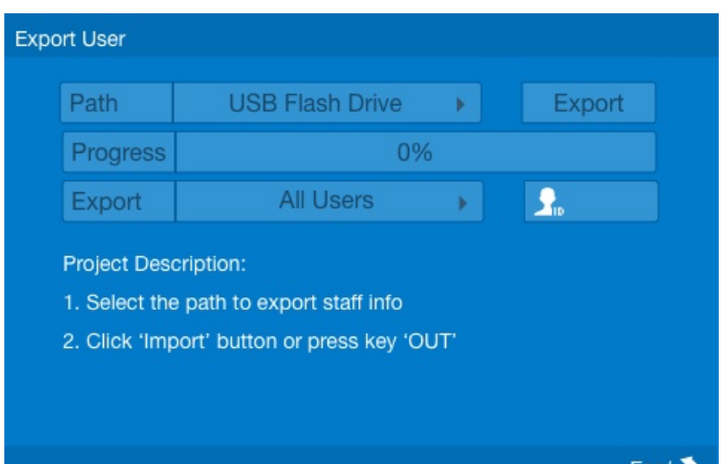
## Export

Click the Export icon to access the data backup interface, you can save the user information and attendance records to the USB Flash driver then import to the CrossChex Standard Software.



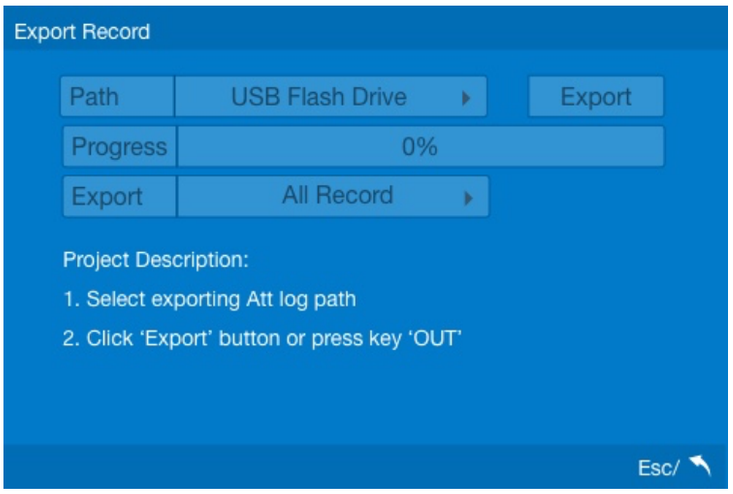

## Export User

Press Directional keys to select the export "All User" or "Specific User" (Assigned User), input the User Id to Export user information to the USB Flash Driver.



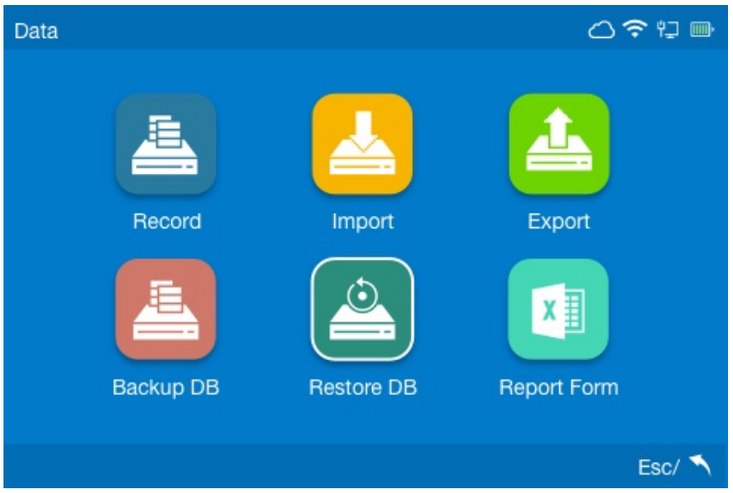
## Export Time Attendance Records

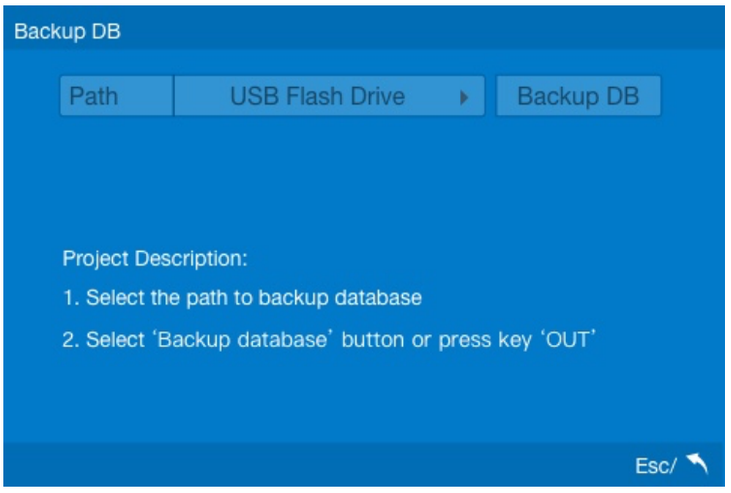
Press Directional keys to select the export “All Record” or “New Records” to the USB Flash Driver. Then import to the CrossChex Standard Software.

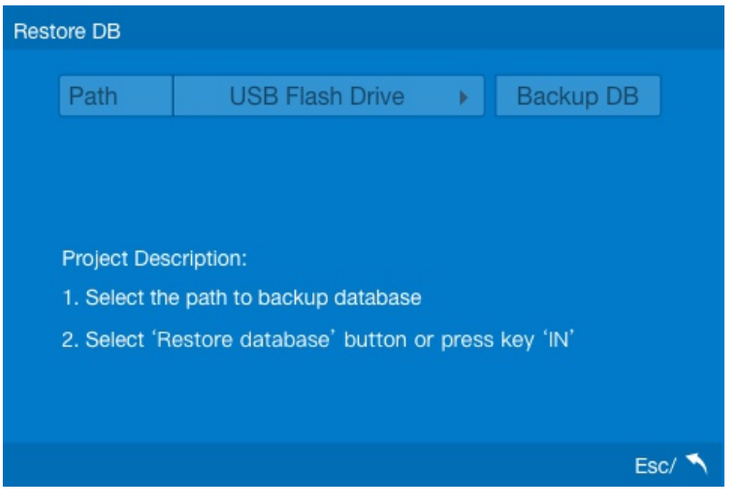



## Backup and Restore DB

Backup device database file to the USB flash driver and Restore the database from the USB flash to devices.

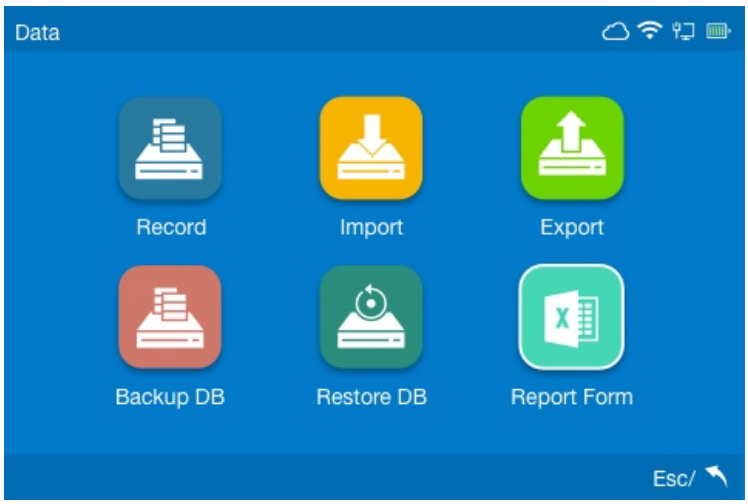


## Report form

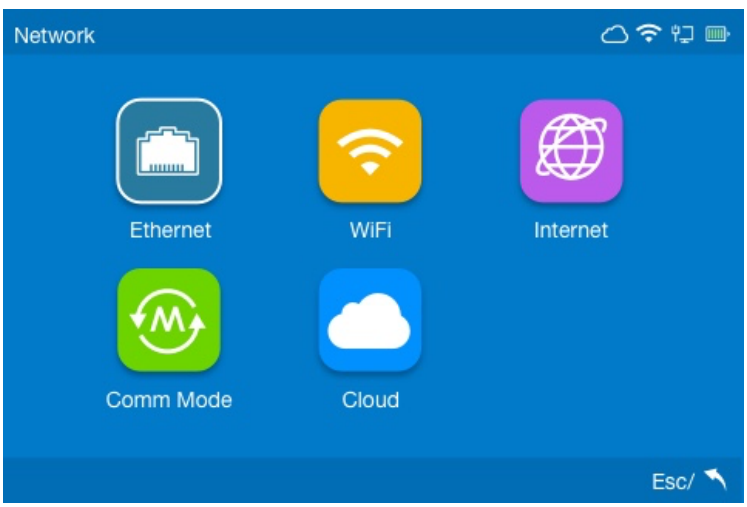
The Report Form can be export the specific user's time attendance report as an excel or text file to USB flash driver according to the date range.



Use the directional keys to assign user ID, edit the data and shift schedule to export data to USB Flash Driver. The files can be imported to third part HR or Payroll systems.

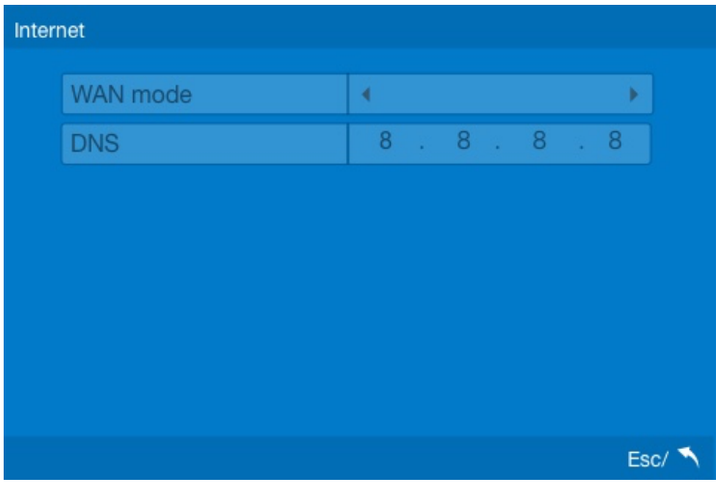
# Communication Settings

Click on the Network icon to access the network configuration interface. Before Setup the network please select the communication way in Internet option.




## Internet

Tap on the Internet icon to setup the preferred way to communicate the device.




**WAN mode**: Select the preferential communication method for your device, choose between WIFI or Ethernet.

If you have already connected or intend to connect the device by Ethernet, select the Ethernet option.

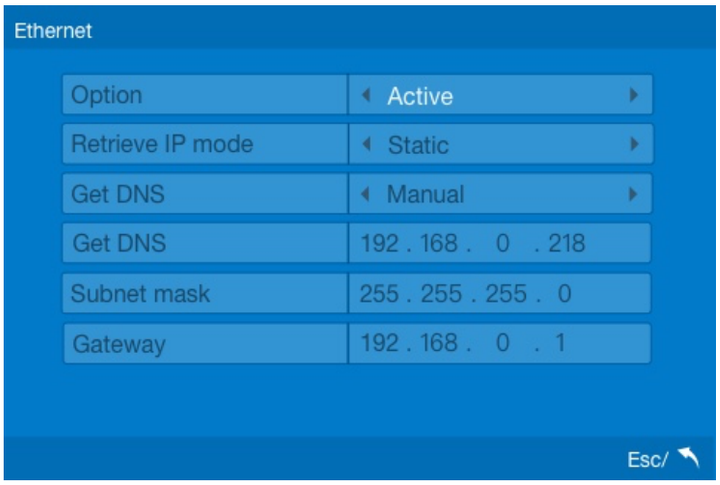
If you have already connected or intend to connect the device by WIFI, select the Wi-Fi option.

If you have already connected and configured the device by both ways, select the best performance way.

**DNS**: Please define the DNS address manually here if you choose the manually way to set up DNS in Ethernet and Wi-Fi configuration option.

## Ethernet

Click “Ethernet” option to set up the IP/Network settings for the device via the network cable.




**Option**: Active or inactive the network communication based on cable.

**Retrieve IP Mode**: Select “Static” for fixed IP or “DHCP” for dynamic IP mode.

**Static**: Fixed IP address that doesn't change.

**DHCP**: A network server that automatically provides and assigns IP addresses,

default gateway and other network parameters to client devices.

Please contact your system administrator or IT responsible for more details.

**Get DNS**: Select between “Manual” or “Auto”.

**Manual**: Get the DNS by setup in the “Internet” option

**Auto**: Get the DNS by local network system.

**Device IP**: Set the device IP manually in case Static IP mode (Default: 192.168.0.218).

Subnet Mask: Set the device Subnet mask manually in case Static IP mode

(Default: 255.255.255.0).

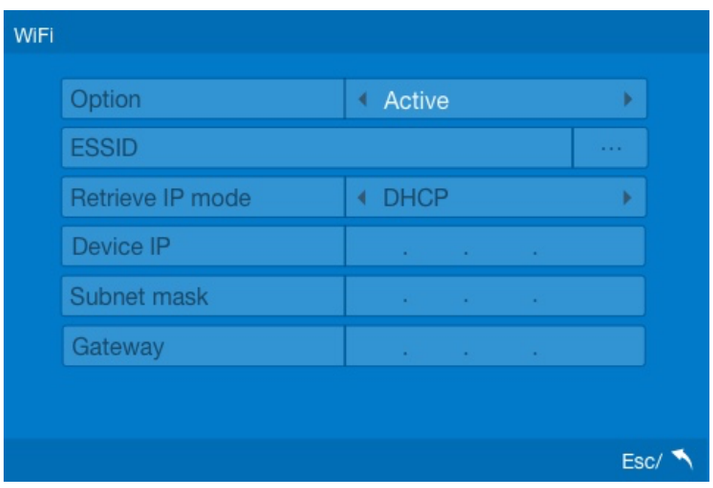
**Subnet Mask**: Set the device Subnet mask manually in case Static IP mode

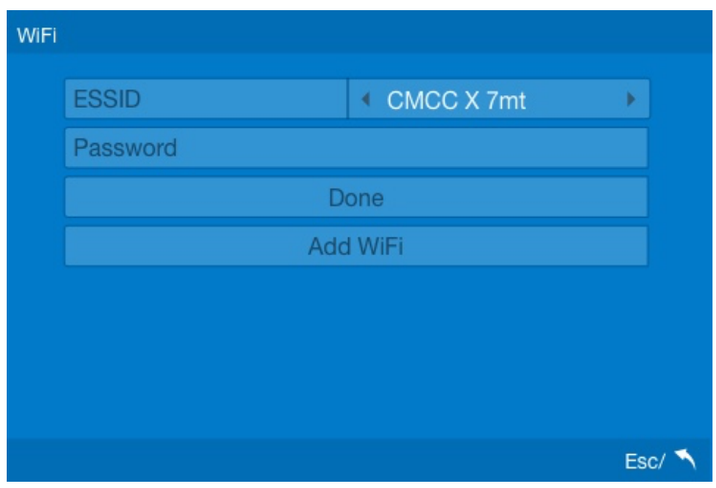
**Gateway**: Set the device Gateway manually in case Static IP mode

(Default: 192.168.0.1).

## WIFI

Click on the” WIFI” option to setup the wireless connection for the device:




Press “Up”and “Down”directional keys to select the ”...” and press “OK” key to setup WIFI connection.

directional keys to select the ESSID and input the WIFI Password. (Press FN key to input the password with characters). Click Done after choosing ESSID ans Input password to start WIFI authentication. Add WIFI: If the chosen ESSID is not on the search list, click Add WIFI to enroll it manually.

**Option**: Active or inactive the network communication based on WIFI.

**ESSID**: Displays the connected WIFI ESSID.

**IP Mode**: Select “Static” for fixed IP or “DHCP” for dynamic IP mode.

**Static**: Fixed IP address that doesn't change.

**DHCP**: A network server that automatically provides and assigns IP addresses,

default gateway and other network parameters to client devices.

Please contact your system administrator or IT responsible for more details.

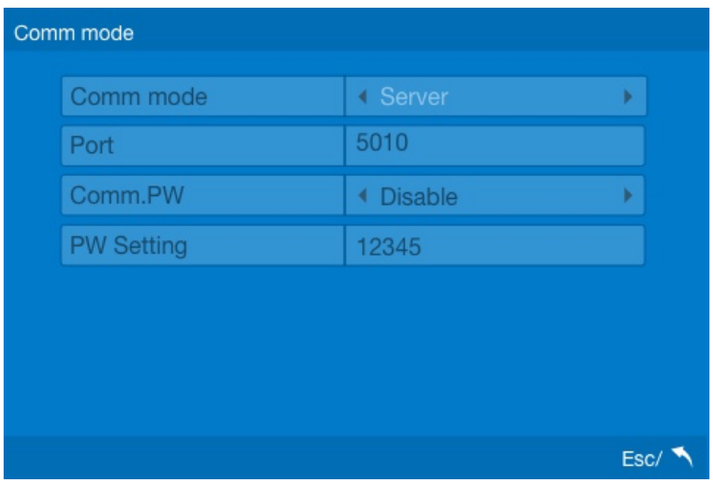
**Device IP**: Set the device IP manually in case Static IP mode(Default: 192.168.0.218).

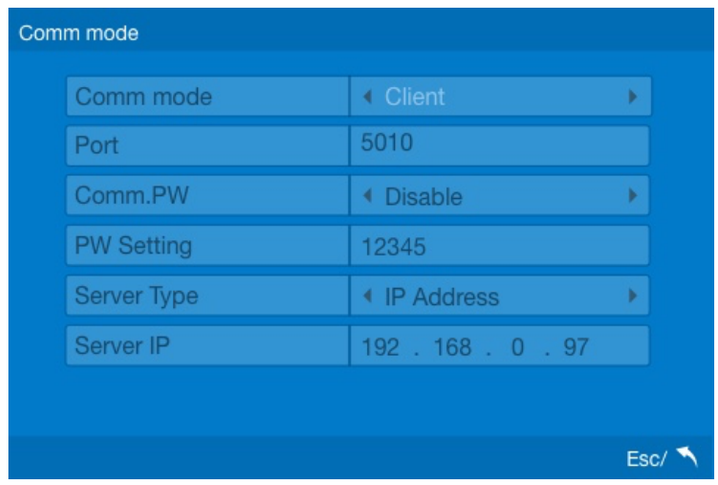
**Subnet mask**: Set the device Subnet mask manually in case Static IP mode (Default: 255.255.255.0).

**Gateway**: Set the device Gateway manually in case Static IP mode (Default: 192.168.0.1).

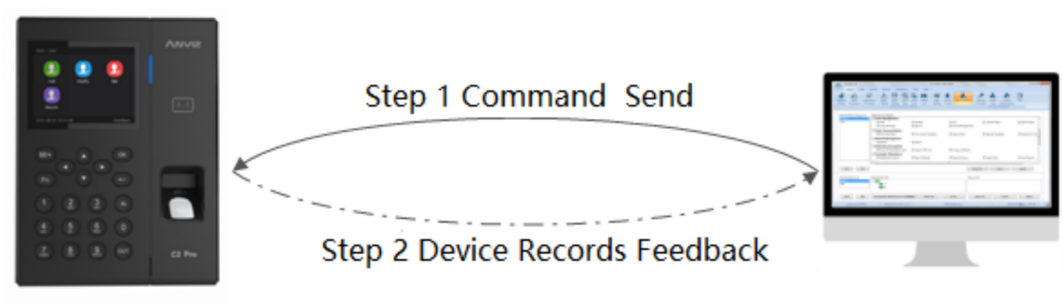
## Comm. Mode

The device supports two kinds of communication mode. Server mode and Client Mode.




requests. In this mode any PC on the same network can connect to the device.

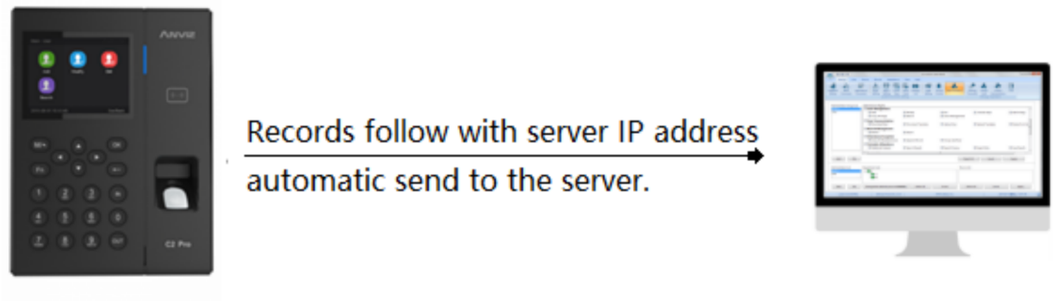



**Port**: The device default communication port is 5010. The port can be changed according to your requirement, make sure to modify the communication port of the software synchronously.

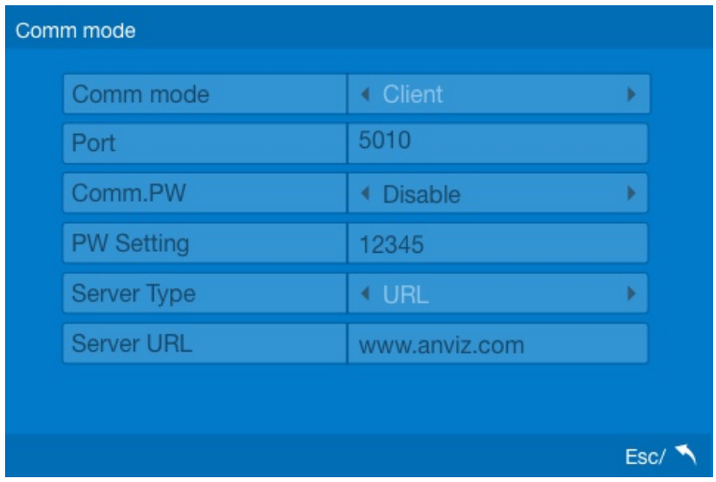
**Comm.PW**: Enable/Disable the network communication password.

**PW Setting**: Setup communication password.

**Client Mode**: The device works as a Client terminal. The device will automatically send the records to a specified server.




## Client Mode



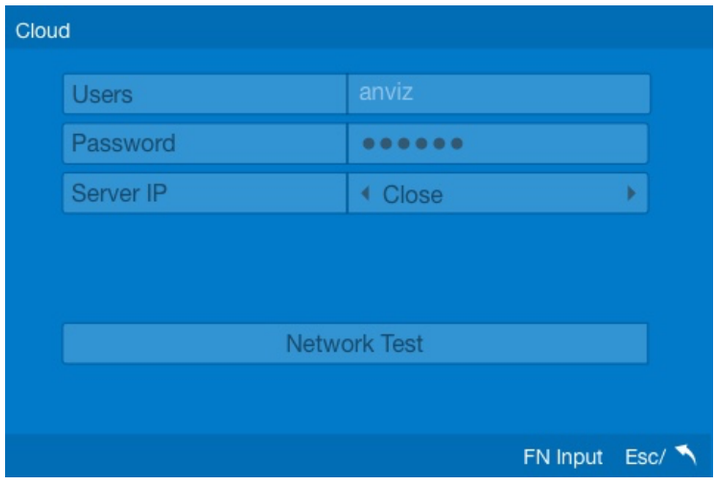

**Server Type (IP Address or URL)**: The device supports communication with specified server via the IP address or DDNS link.

**Server IP**: The specified server IP address. The device will only be able to communicate with the machine addressed on this IP address.

Server URL: Input the specified server's DDNS link.

## Cloud Communication

The C2Pro and C2C Pro device supports Anviz CrossChex Cloud System communication.
For more details, please refer to the Cloud menu.



**Users (**Need to change this to User ID)** : Enter the User ID/Company ID you registered in your CrossChex Cloud account.

**Passwd (**Can be used as full word Password)**: Enter the password created in your CrossChex Cloud account.

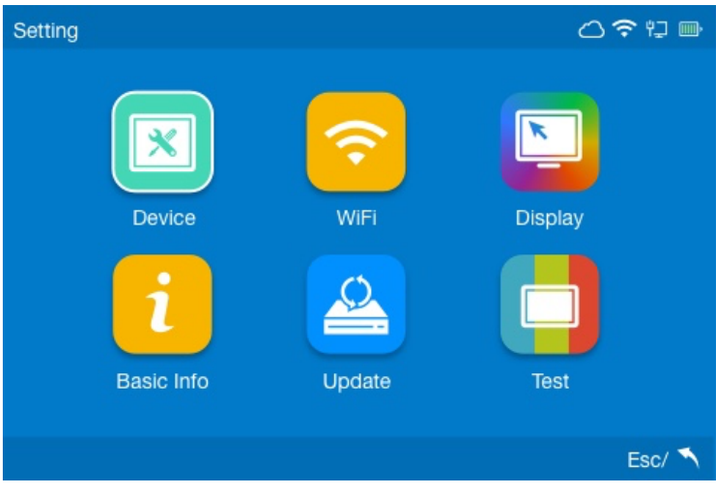
**Server IP**: Please select the server you are using for your CrossChex cloud account.

**Network Test**: Test the connectivity between the device and the CrossChex Cloud.

When succeed, the device will appear at the device tab of your Cloud Account automatically.

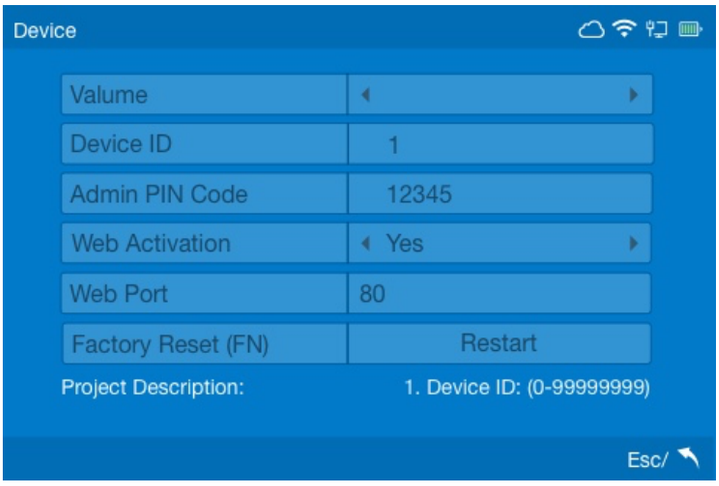
## Settings Menu

Tap on the “Setting” icon to access the settings interface.




## Device Information

Click on the “Device” icon to access the device information interface.




**Volume**: increase or decrease the device´s volume (0 to 5).

**Device ID**: Insert the Device ID (default: 1). In a same network, each device must have a unique ID.

**Admin PIN Code**: Set the Administrator password to log the internal device menu (default: 12345).

**Web Activation**: Enable/Disable the device management by web interface.

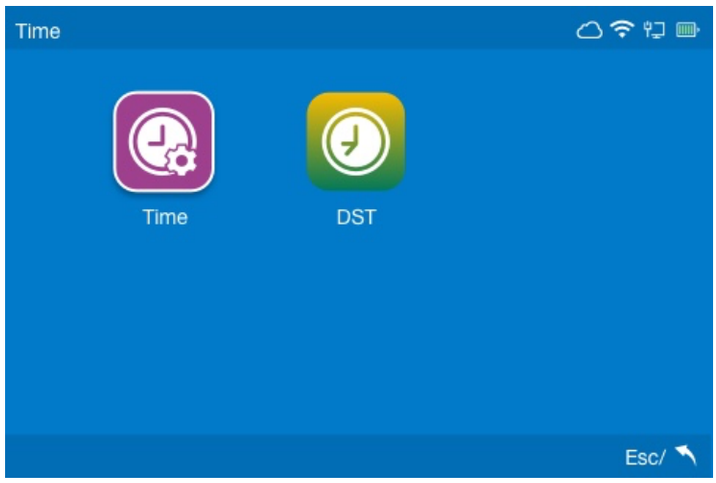
**Web port**: Select the web port for web management (default: 80).

**Factory Reset**: Set the device as factory mode. Caution: This process will delete all the users and records from the device.

**Restart**: Reboots the device, keeping stored all the existing information.

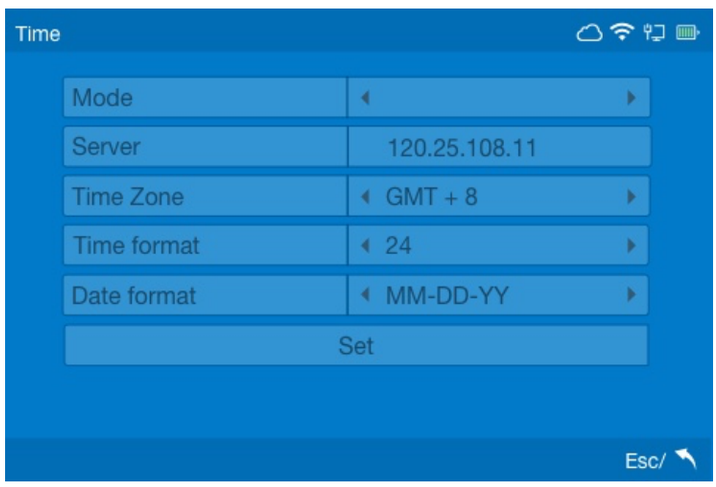
## Time

Tap on the "Time" icon to access the time adjustment interface.




## Time Settings

Tap on the time icon to access the time settings interface.




There are two modes to set the time:

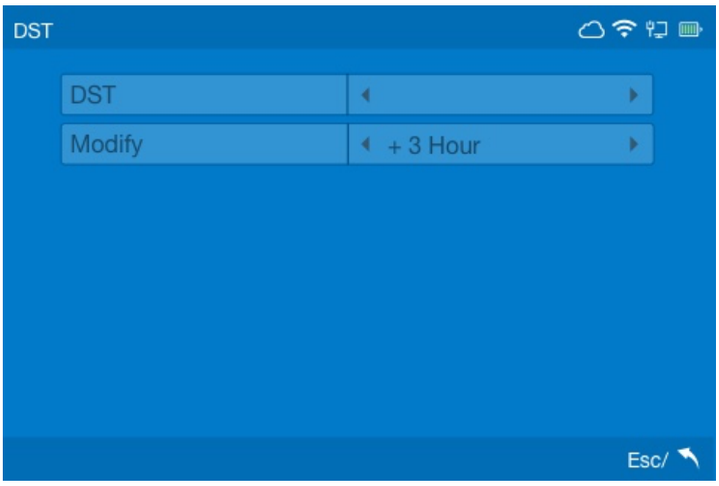
**Auto**: Automatic adjustment the device date/time according to NTP server (Necessary to input an available NTP server IP address manually).

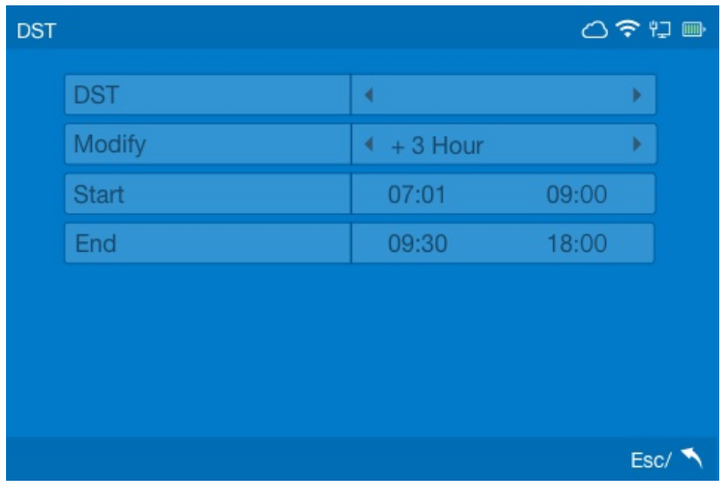
**Manual**: Adjust the device date/time manually.

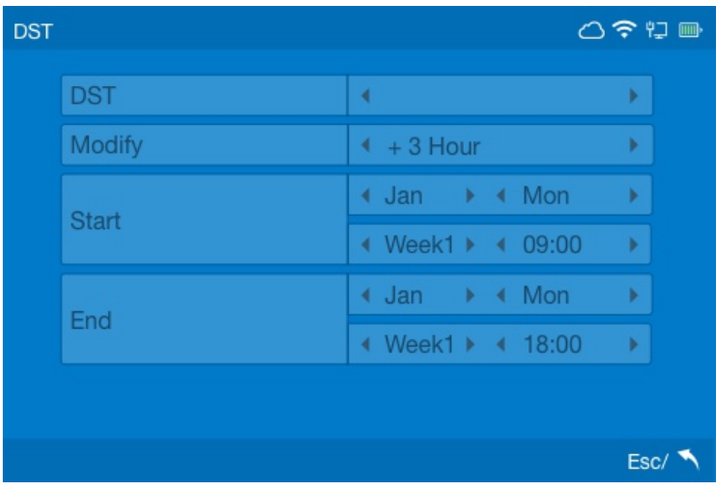
Click Set to save configuration.

## DST

**DST**: Daylight-saving time settings.



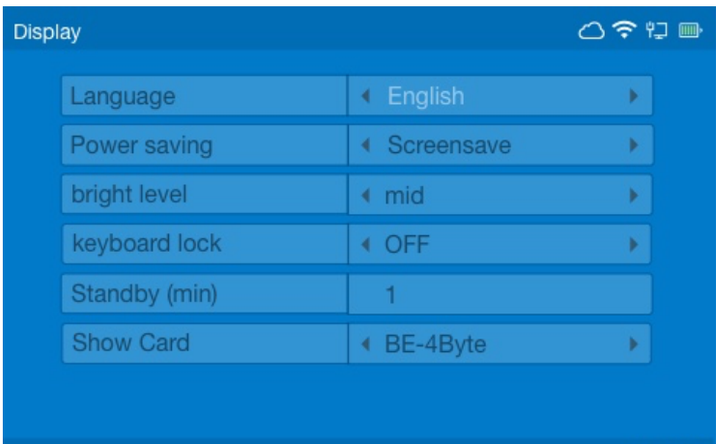




The Daylight-saving time is a manual method to set the local area time zone Deviation, according to where the device is located.

## Display settings

Tap on the “Display” icon to access the display settings interface.



**Language**: Select to switch the system language.

**Power Saving**: Energy saving display settings.

**Bright Level**: LCD screen brightness level.

**Keyboard lock （CAUTION）**: Disable the device keypad input. (Disable the non-admin user operate the device by keyboard)

**Standby(min)**: Bright screen standby time.

**Show Card**: Setup the registered RFID card number length and Number order display on the device.

**BE-3Byte**: Reads 3 bytes starting from the High to Low side of the RFID card number.

**BE-4Byte**: Reads 4 bytes starting from the High to Low side of the RFID card number.

**LE-3Byte**: Reads 3 bytes starting from the Low to High side of the RFID card number.

**LE-4Byte**: Reads 4 bytes starting from the Low to High side of the RFID card number.

When reading the card, please note the hexadecimal to decimal conversion, and distinguish between Wiegand 26 and Wiegand 34.

## Basic Information

Tap on the “Basic Info” icon to show the device´s basic information.

**Serial Number**: Contains the S/N of this device.

**Employee No**: Number of employees stored on the device´s memory.

**Card Count**: Number of RFID cards stored on the device´s memory.

**Fingerprint No**: Number of fingerprint templates stored on the device´s memory.

**Log**: Number of log records stored on the device memory.

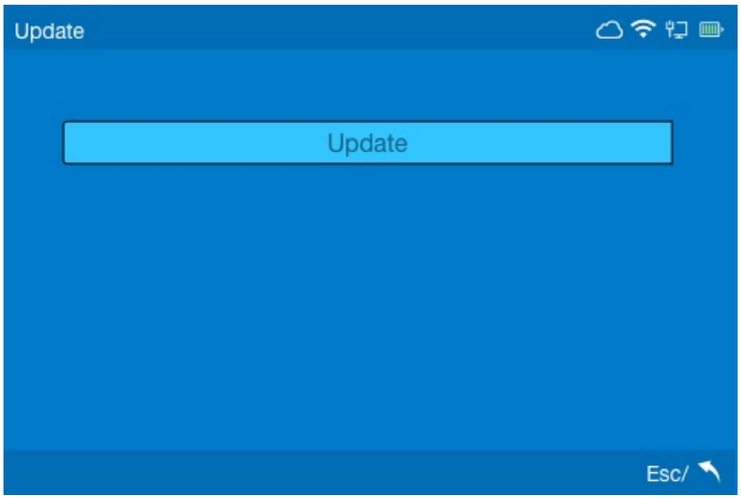
**Firmware Ver**: The current firmware version of this device.

**Kernel Ver**: The current kernel version of this device.

**File System Ver**: The current file system version of this device.

## Update

Tap on the “Update” icon to access the firmware update interface.

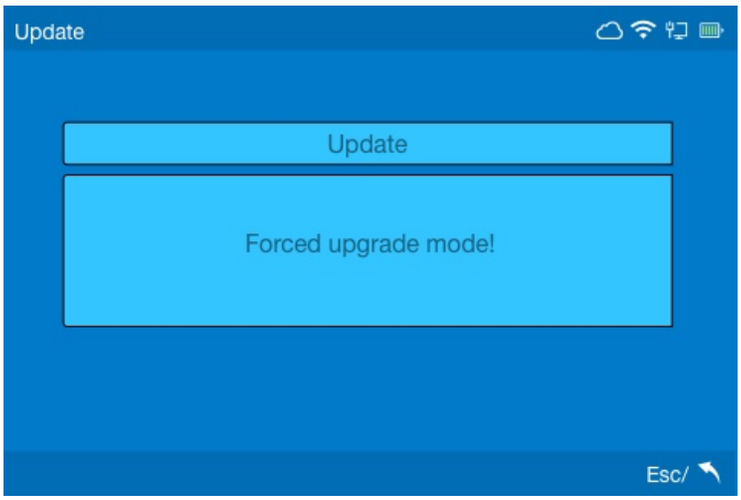



Follow the instruction to plug a USB flash driver with update file and press “Update” button to begin the update.

**Forced update mode** (hidden mode):

Caution: Please only use this mode after contacting Anviz support team.

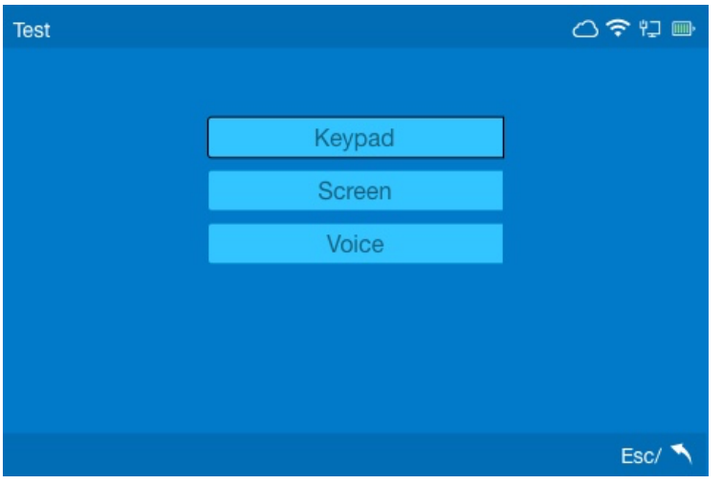
Press the “IN”,  1,2,3,4,5 and “Out” keys to active the forced update mode:




Click “Update” to conclude operation.

## Test

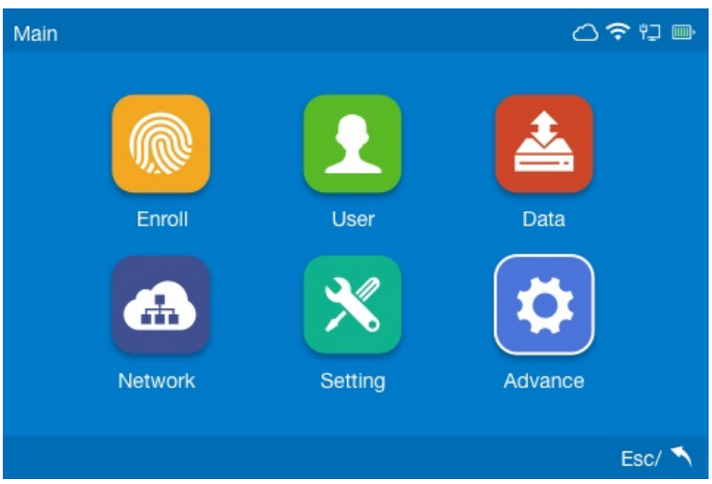
Click on the “Test” icon to access the device self-test mode.

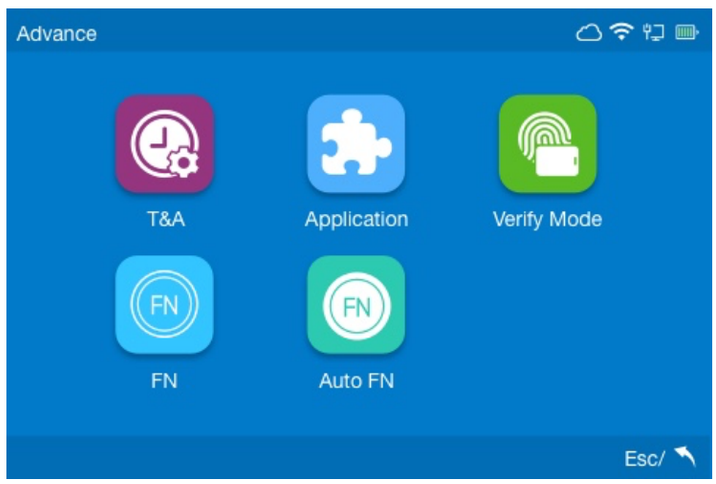



In this mode, the user can test device´s keyboard, LCD display and speaker (alarms and voices).

## Advanced Settings

Click on the “Advanced” icon to access the advance settings of the device.




### T&A (Time and Attendance Settings)

Click on the “T&A” icon to access the time Attendance settings of the device.

**Duplicate Punch Range(0-250min)**: Set the time interval for repeated punching of the same employee to prevent the system from generating duplicate punching records.

**Log Alarm Threshold (0-5000)**: The device will emit an alarm when the log records reach the number inserted on this field to inform the log memory is almost full.

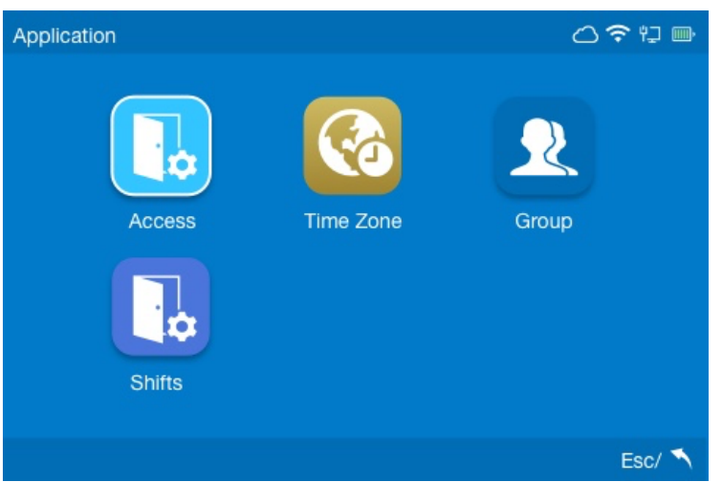
Identify Precision: Fingerprint template comparison accuracy.

**Check Finger**: Enable/disable the fingerprint touch active function. When disabled, the fingerprint sensor will keep always turned on.

**Intelligent update FP**: Automatically replaces the user fingerprint template on device´s by a new one whenever the device detects a better-quality user template than the previous stored in.

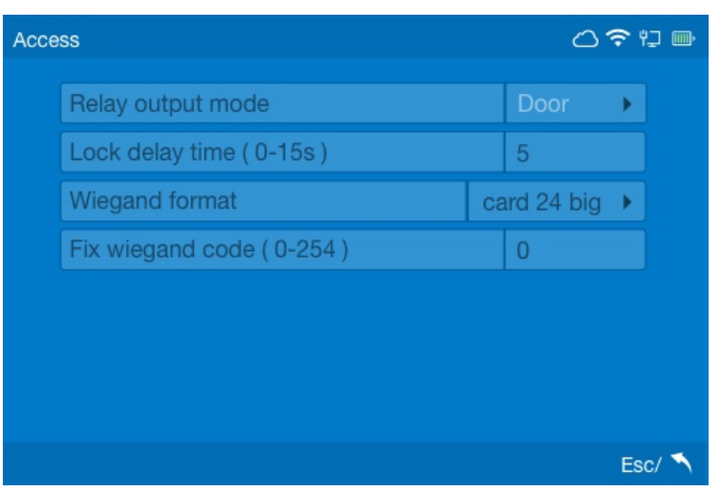
## Application

Click on the “Application” icon to access the application menu




## Access

Click on the “Access” icon to enter the access control interface.



**Relay Output Mode**: Define the device relay signal function.

(Door or Scheduled Ring)

**Lock Delay Time(0-15s)**: Setup the relay delay time 0~15 secs.

**Wiegand Format**: Define the terminal Wiegand output format, the terminal supports up to 11 Wiegand types.

Anviz Wiegand: Anviz own Wiegand format output, to be used with SC011 access control unit.

Wiegand 26: The registered User ID will be output as a standard Wiegand 26 format.

Wiegand 26BE: The registered RFID Card number will be from high to low output as a Wiegand 26 format.

Wiegand 26LE: The registered RFID Card number will be from low to high output as a Wiegand 26 format.

Wiegand 34BE: The registered RFID Card number will be from high to low output as a Wiegand 34 format.

Wiegand 34LE: The registered RFID Card number will be from low to high output as a Wiegand 34 format.

Card 24 Big: The registered RFID Card number will be from high to low output as a Wiegand 24 format.

Card 24 Little: The registered RFID Card number will be from low to high output as a Wiegand 24 format.

Card 32 Big: The registered RFID Card number will be from high to low output as a Wiegand 32 format.

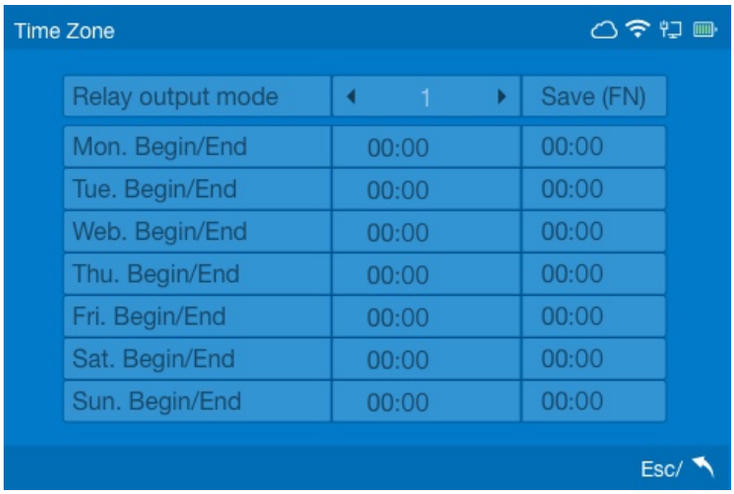
Card 32 Little: The registered RFID Card number will be from low to high output as a Wiegand 32 format.

Fix Facility Code: use to self-defined head of the Wiegand code output. The Fix Facility Code use to integrated with existing access control system

Fix Facility Code: Self-defined head of the Wiegand code output. To be integrated with existing access control system.

## Time Zone

Click on the “Time Zone” icon to enter the Time zone settings interface.

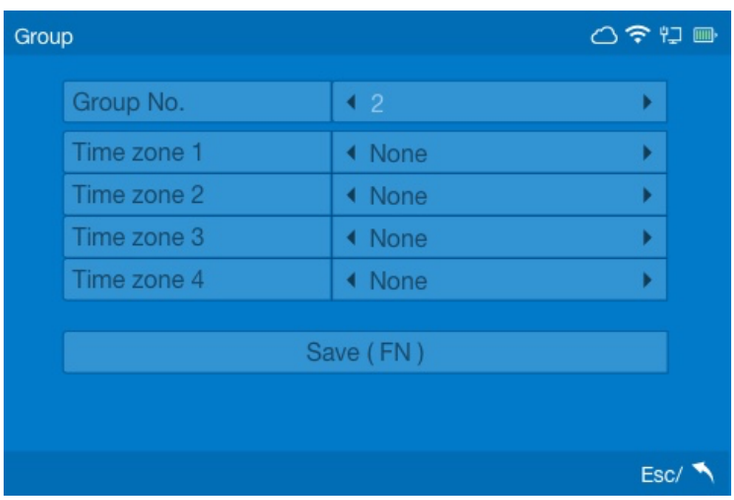



At this interface you can set rules for access control restriction according to the week day and time.

You can create up to 30 different access rules, they can be assigned with a user group (section Group).

## Group

Click on the “Group” icon to enter the group settings interface.



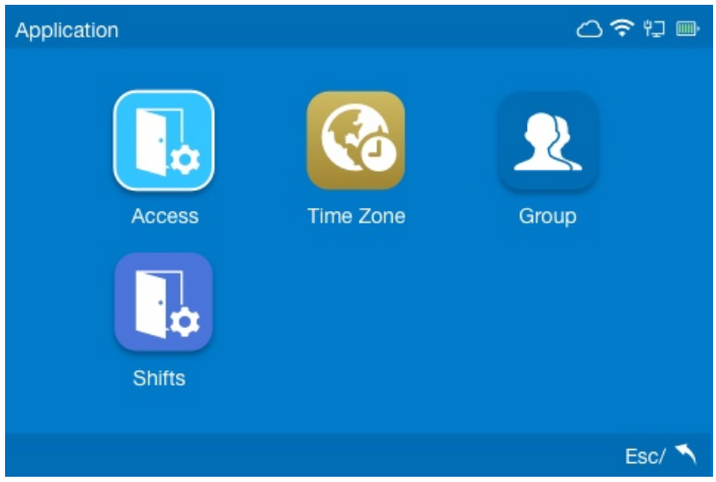

Select the Group number you and to modify and add the previous configured time zone(s) in there.

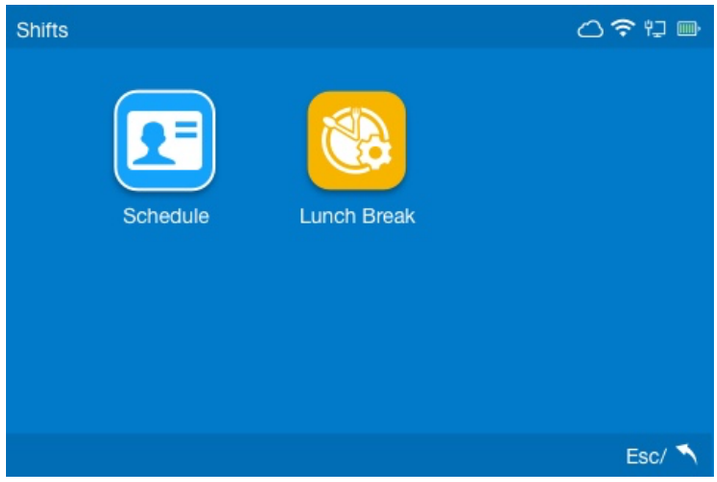
Each user group can accept up to 4 different time zones.

Make sure to set the user group correctly when adding/modifying User (section User).

Click save to store operation.

## Shifts

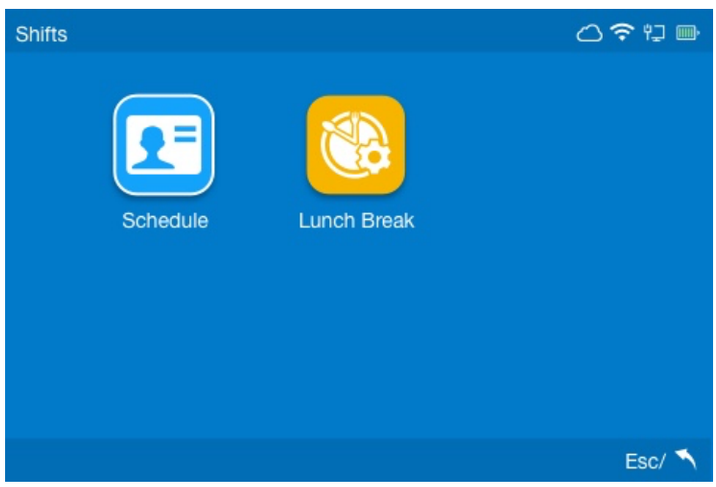


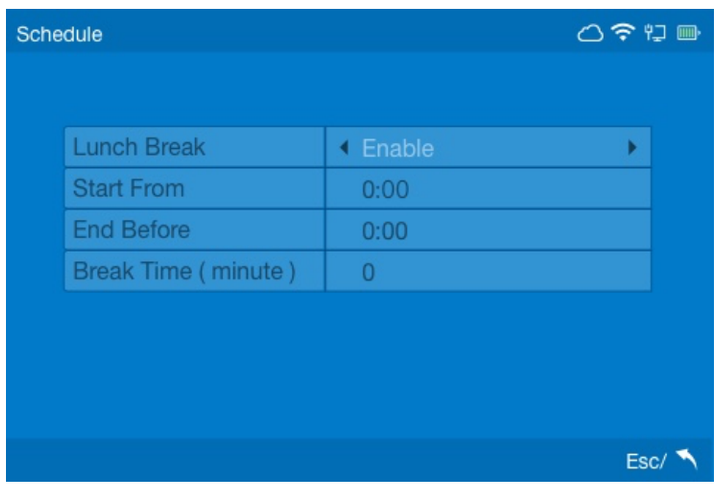




## Schedule

Click on the “Lunch Break” icon to access the device Lunch Break settings. The Lunch break is used to configure the employee attendance verification during lunch break when report shows they´re not valid attendance record.

## Lunch Break

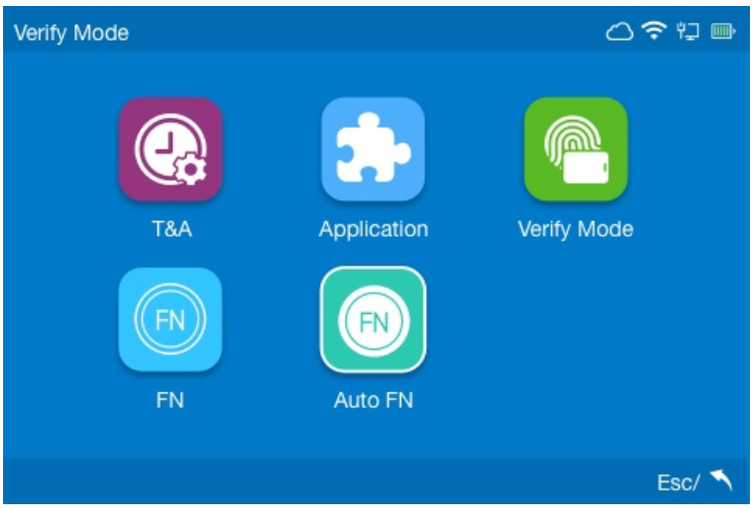


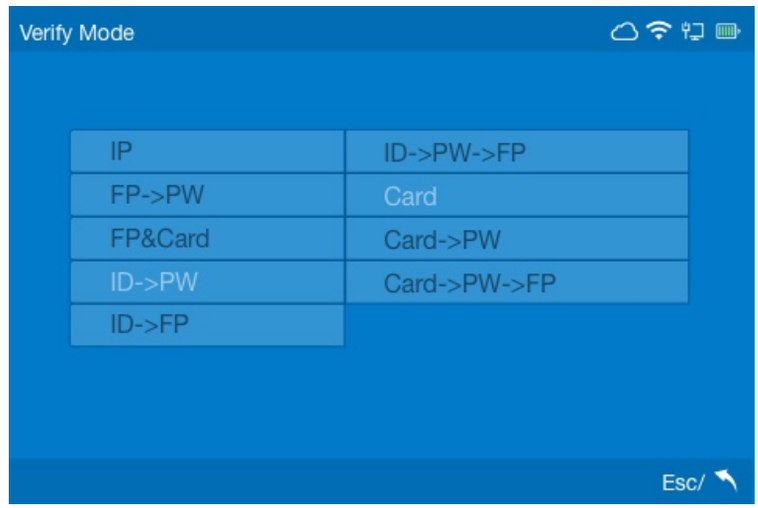




Click on the “Lunch Break” icon to enter setup Lunch Break for device. The Lunch break use to make the employee attendance verification during lunch break is not a valid attendance record.

Setup the Lunch Break start and end time. And the duration time of the lunch break

## Verify Mode



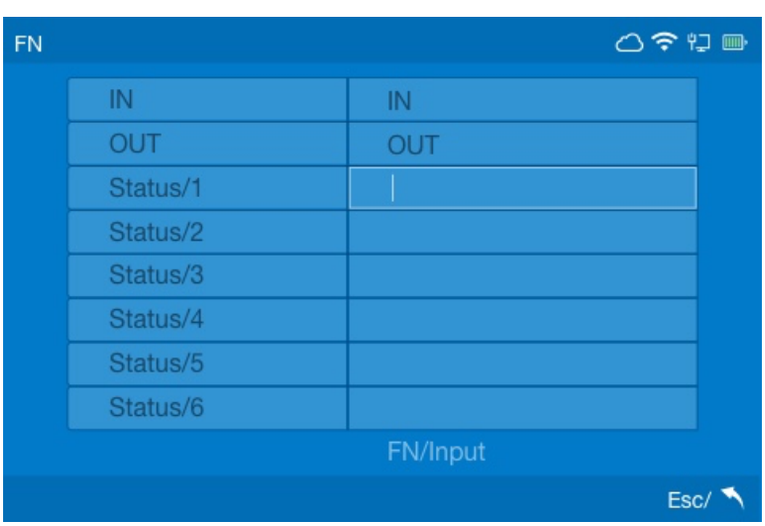




Click on the “Verify Mode” icon to setup the employee default verify mode.

FP means Fingerprint Template, PW means Password, ID means User registered number.

## FN Settings

Click the “FN” icon to enter the FN settings interface.




At this Interface it´s possible to add or modify time attendance status and its names.

## Auto FN

Click on the “Auto FN” icon to enter the Auto FN settings interface.

At this Interface it´s possible to generate specific records according to date and time.

Example: Records from 07:00 am to 10:00 am on Monday will be always considered IN.

Last page for support@anviz.com details.

In order to protec the environment, Anviz has decided to go "CD Free" campaign since June 1st 2022. We will provide QR code for you to download the electronic documents to make sure that you understand how to install and user Anviz device.

https://bit.ly/2WugbYp
Dropbox

https://bit.ly/2Vn0wh6
Google

https://bit.ly/2J9qA95
Anviz

Before using all Anviz products, please read all applicable terms, rules, policies and usage provisions found at **https://www.anviz.com/privacypolicy** and **https://www.anviz.com/anviz-biometric-data-retention-policy**. By using your Anviz, you agree to be bound by the Anviz Privacy Policy.

Anviz brand and product are trademarked and protected under law of the United States.
Unauthorized use is prohibited.
For more information visit www.anviz.com, or email marketing@anviz.com for further help.
©2021 Anviz Global Inc. All Rights Reserved.