

# Time & Attendance Terminal

User's Manual

**V1.0.0**

# Important Safeguards and Warnings

This Chapter describes the contents covering proper handling of the Time & Attendance Terminal, hazard prevention, and prevention of property damage. Read these contents carefully before using the Time & Attendance Terminal, comply with them when using, and keep it well for future reference.

## Operation Requirement

- Do not place or install the Time & Attendance Terminal in a place exposed to sunlight or near the heat source.
- Keep the Time & Attendance Terminal away from dampness, dust or soot.
- Keep the Time & Attendance Terminal installed horizontally on the stable place to prevent it from falling.
- Do not drop or splash liquid onto the Time & Attendance Terminal, and make sure there is no object filled with liquid on the Time & Attendance Terminal to prevent liquid from flowing into the Time & Attendance Terminal.
- Install the Time & Attendance Terminal in a well-ventilated place, and do not block the ventilation of the Time & Attendance Terminal.
- Operate the Time & Attendance Terminal within the rated range of power input and output.
- Do not disassemble the Time & Attendance Terminal.
- Transport, use and store the Time & Attendance Terminal under the allowed humidity and temperature conditions.

## Electrical Safety


- Improper battery use might result in fire, explosion, or inflammation.
- When replacing battery, make sure the same model is used.
- Use the recommended power cables in the region and conform to the rated power specification.
- Use the power adapter provided with the Time & Attendance Terminal; otherwise, it might result in people injury and device damage.
- The power source shall conform to the requirement of the Safety Extra Low Voltage (SELV) standard, and supply power with rated voltage which conforms to Limited power Source requirement according to IEC60950-1. Please note that the power supply requirement is subject to the device label.
- Connect the device (I-type structure) to the power socket with protective earthing.
- The appliance coupler is a disconnection device. When using the coupler, keep the angle for easy operation.

## General

This User's Manual (hereinafter referred to as "Manual") introduces the installation and basic operation of the Time & Attendance Terminal (hereinafter referred to as "terminal").

## Safety Instructions

The following categorized signal words with defined meaning might appear in the Manual.

Signal Words	Meaning
 <b>NOTE</b>	Provides additional information as the emphasis and supplement to the text.

## Privacy Protection Notice

As the device user or data controller, you might collect personal data of other such as face, fingerprints, car plate number, Email address, phone number, GPS and so on. You need to be in compliance with the local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures include but not limited to: providing clear and visible identification to inform data subject the existence of surveillance area and providing related contact.

## About the Manual

- The Manual is for reference only. If there is inconsistency between the Manual and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the Manual.
- The Manual would be updated according to the latest laws and regulations of related regions. For detailed information, see the paper manual, CD-ROM, QR code or our official website. If there is inconsistency between paper manual and the electronic version, the electronic version shall prevail.
- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the Manual. Please contact the customer service for the latest program and supplementary documentation.
- There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, please refer to our final explanation.
- Upgrade the reader software or try other mainstream reader software if the Manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and the company names in the Manual are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem

occurred when using the device.

- If there is any uncertainty or controversy, please refer to our final explanation.

18698 大华 2019-02-14

# Table of Contents

<b>Important Safeguards and Warnings .....</b>	<b>II</b>
<b>Foreword .....</b>	<b>III</b>
<b>1 Overview.....</b>	<b>1</b>
1.1 Introduction .....	1
1.2 Features .....	1
1.3 Appearance .....	1
1.4 Dimensions .....	3
<b>2 Installation.....</b>	<b>4</b>
2.1 Installation Methods .....	4
2.2 Cable Connection .....	5
<b>3 Operation.....</b>	<b>6</b>
3.1 Notice .....	6
3.2 Main Menu .....	6
3.3 Attendance Check Methods .....	7
3.4 User.....	9
3.4.1 Add New Users .....	9
3.4.2 Query & Edit User.....	10
3.4.3 Edit Department.....	11
3.4.4 Add Cards in Batch .....	11
3.5 Data.....	12
3.5.1 Query User ATT. Log .....	12
3.5.2 Export Monthly User ATT. Log/Export Monthly ATT. Report.....	13
3.6 Shift .....	13
3.6.1 Shift Setting .....	13
3.6.2 Schedule Setup .....	14
3.6.3 Late-in/Early-out Allowed.....	16
3.7 USB.....	16
3.7.1 Import/Export User Info .....	16
3.7.2 Import/Export User FP.....	16
3.7.3 Import/Export Bell Info .....	17
3.7.4 Import/Export Auto Switch Time .....	17
3.8 Feature.....	17
3.8.1 Date & Time .....	17
3.8.2 Communication.....	18
3.8.3 Features.....	18
3.8.4 System.....	21
3.8.5 Language.....	22
3.9 System .....	22
<b>4 Attendance Configuration on SmartPSS .....</b>	<b>23</b>
4.1 Creating Departments and Adding Users .....	23
4.1.1 Creating Departments .....	23

4.1.2 Adding Users .....	24
4.2 Attendance Setting.....	25
4.2.1 Attendance Time Zone.....	25
4.2.2 Attendance Shift.....	28
4.2.3 Holiday .....	29
4.2.4 Attendance Event.....	30
4.3 Shift Schedule .....	31
4.4 Viewing Real-Time Attendance Check Detail .....	33
4.5 Attendance Report .....	35
<b>Appendix 1 Fingerprint Record Description .....</b>	<b>36</b>
<b>Appendix 2 Text Input.....</b>	<b>38</b>
<b>Appendix 3 FAQ.....</b>	<b>39</b>
<b>Appendix 4 Cybersecurity Recommendations .....</b>	<b>40</b>

18698 大华 2019-02-14

# 1 Overview

## 1.1 Introduction

The terminal can be used to check attendance. The attendance check can be completed through three methods: fingerprint, password, and card.

## 1.2 Features

- High capacity standby battery works for upto 10 hours in the standby mode.
- Can be connected to the third party access control device.
- 1, 000 user information (ID, name, fingerprint, password, card number) can be recorded on terminal.
- Stores up to 100, 000 attendance record reports and 10, 000 management records.
- All users can query their own attendance records.
- Only administrators can add new users, edit user information, query, import or export attendance logs and attendance reports.
- USB disk update firmware.
- T9 text input.
- 24 groups of shift.
- 20 departments.

## 1.3 Appearance

Figure 1-1



Table 1-1 Key description

Icon	Description
0-9	Number keys for number and letter input.


Icon	Description
<b>ESC/F1</b>	<ul style="list-style-type: none"> <li>Press the key to exit or go to the previous menu.</li> <li>On the standby interface, press the button to check in.</li> </ul>
<b>^/F2</b>	<ul style="list-style-type: none"> <li>In the standby mode, press the key, BREAK OUT will be displayed on the screen.</li> <li>Up (direction key; attendance type switch).</li> </ul>
<b>∨/F3</b>	<ul style="list-style-type: none"> <li>In the standby mode, press the key, BREAK IN will be displayed on the screen.</li> <li>Down (direction key; attendance type switch).</li> </ul>
<b>OK/F4</b>	<ul style="list-style-type: none"> <li>Enter or confirm.</li> <li>On the standby interface, press the key to check out.</li> </ul>
<b>#</b>	Delete key or shortcut key for reviewing records.
	<ul style="list-style-type: none"> <li>When the terminal is off/on, press the key to turn the terminal on/off (press the key for over three seconds to turn the terminal off).</li> <li>On the standby mode, press the key, and then administrators can go to the main menu by fingerprints, passwords, or cards.</li> <li>When you need to enter text, press the key, and then you can switch text input types (numbers, letters and punctuation).</li> </ul>

Figure 1-2

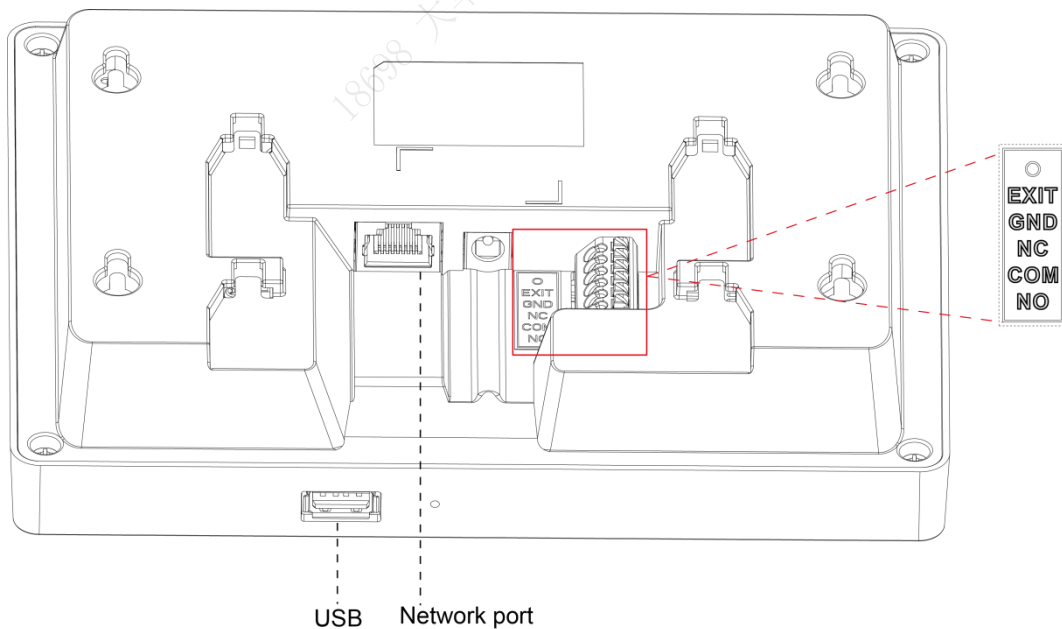


Table 1-2 Port description

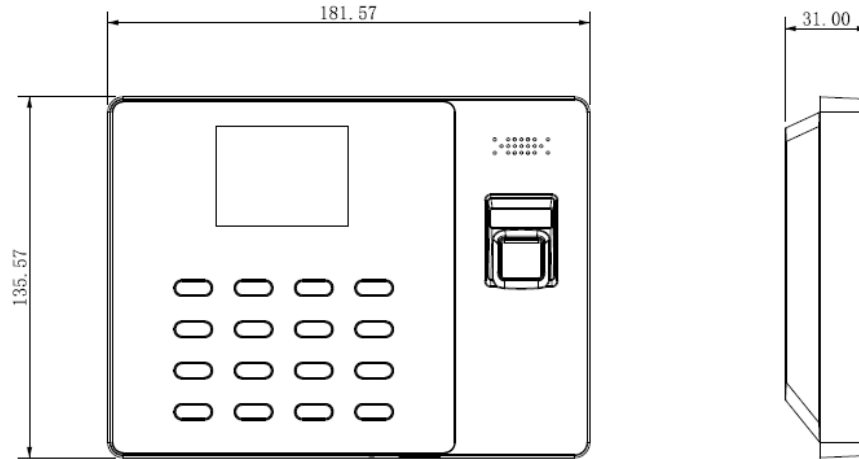
Port	Description
<b>EXIT</b>	Connected to the door exit button.
<b>GND</b>	Connected to the ground line.
<b>NC</b>	Makes the relay normally closed.
<b>COM</b>	COM port.



Port	Description
NO	Makes the relay normally on.

## 1.4 Dimensions

Figure 1-3 Dimensions (mm)

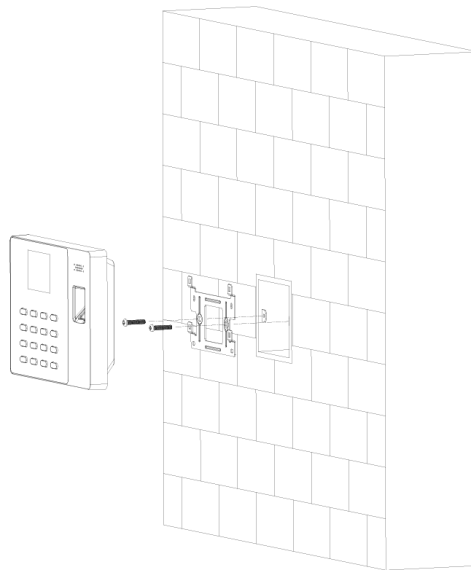


# 2 Installation

## 2.1 Installation Methods

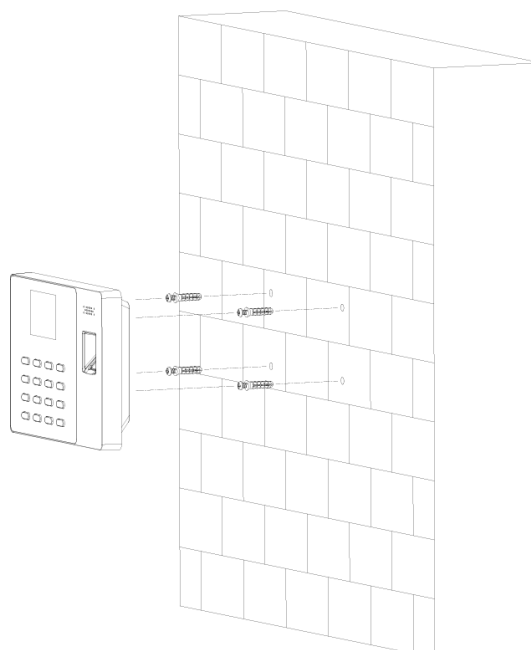
Installed through the 86 electrical box

Figure 2-1 Installed through 86 electrical box



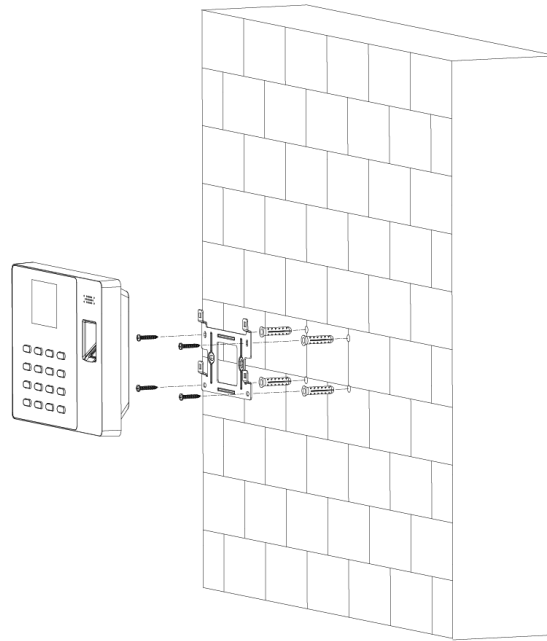
Directly installed on the wall

Figure 2-2 Directly installed on the wall



Installed through the bracket

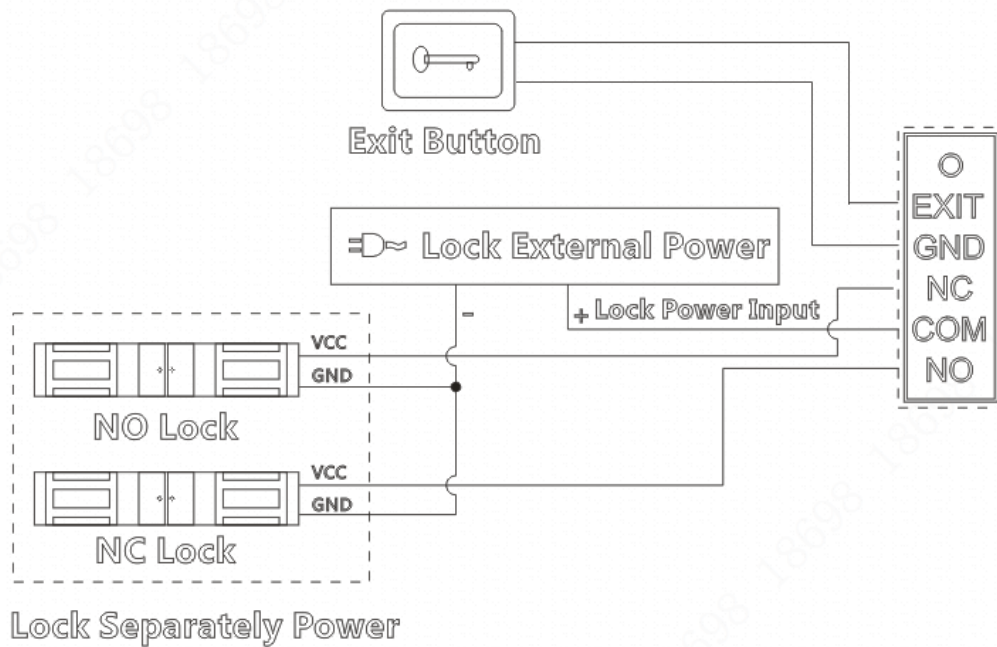
Figure 2-3 Installed through bracket



## 2.2 Cable Connection

The terminal can be connected to exit button to control the door. See Figure 2-4.

Figure 2-4 Cable connection



# 3 Operation

## 3.1 Notice


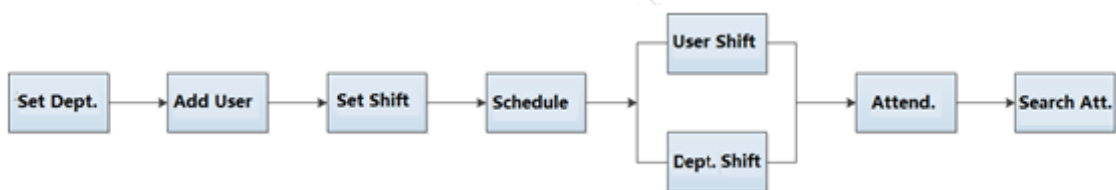
- When the terminal is connected to the power source, you need to press  to turn it on.
- Before an administrator is created, anyone can enter the main menu and do settings for the terminal. For the sake of information security, you need to create administrators first (Select **1 User > Add New User**, and then select a user ID. Select **User Level**, press **OK/F4** and then **^/F2** or **∨/F3** to select **Administrator**.).
- When you need to connect the terminal to SmartPSS (the management platform), the default ID is “admin” and the default password is also “admin”.
- Settings about shifts, schedules, and departments in the terminal are independent of those on SmartPSS.
- For standalone system framework, see Figure 3-1.

Figure 3-1 System framework

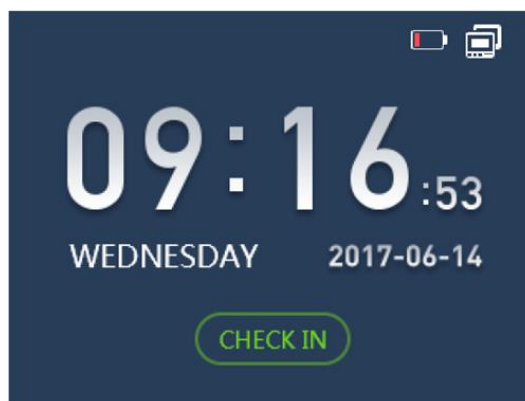


## 3.2 Main Menu




### Standby mode

Before you enter the main page, the interface below is displayed. See Figure 3-2.

Figure 3-2 Standby interface





-  indicates that the network is disconnected.
-  indicates that the network is connected.
-  indicates the battery level and network connection condition. When you turn the terminal on for the first time, the battery level is 25% (can last for about one hour). As time goes by the battery life reduces.

## Main menu


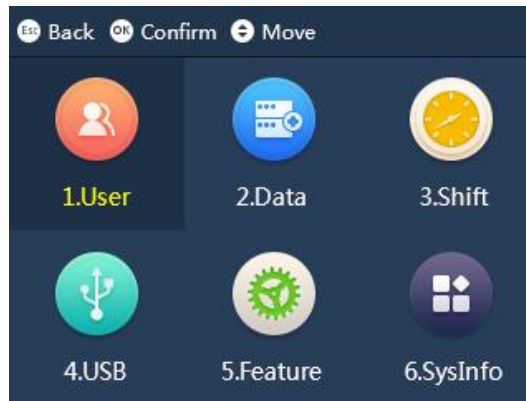

Press , and then the main menu will be displayed. See Figure 3-3.

Figure 3-3 Main menu



- After you have created administrators, you need to press  first, and then you can go to the main menu by the following methods:
  - ◇ Press your finger tip at the fingerprint sensor;
  - ◇ Enter the administrator's user ID and password;
  - ◇ Swipe your card at the card reader.
- You can select icon by the following two methods:
  - ◇ Press  $\wedge/F2$  or  $\vee/F3$ ;
  - ◇ Press number keys.

## 3.3 Attendance Check Methods

On the standby interface, you can get your attendance checked by fingerprint, password, or card.

### Fingerprint

Step 1 Press your finger tip at the fingerprint sensor.

There are six options (Check in, Break out, Break in, Check out, OT-In, and OT-Out) displayed on the screen.

Step 2 Select one of the six according to your requirement.

Step 3 Press **OK/F4**.

The attendance is checked.

## Password

Step 1 Press the user ID number on the keyboard.

Step 2 Press **OK/F4**.

Step 3 Enter the password.

Step 4 Press **OK/F4**.

There are six options (Check in, Break out, Break in, Check out, OT-In, and OT-Out) displayed on the screen.

Step 5 Select one of the six according to your requirement.

Step 6 Press **OK/F4**.

The attendance is checked.

## Card

Swipe the card at the card reader below the fingerprint sensor to get your attendance checked. Your user ID, name, card swiping time, attendance events will all be displayed on the screen. See Figure 3-4.

Figure 3-4 Swipe card



Press **^/F2** or **∨/F3** continuously, **BREAK OUT, CHECK IN, OT-OUT, OT-IN, CHECK OUT, BREAK IN** will be displayed in turn.

There are shortcut keys for check-in, check-out, break-in, and break-out.

- ◇ **Esc/F1**: Press **Esc/F1**, **CHECK IN** will be displayed on the screen, and then you can check-in by fingerprint, password, or card.
- ◇ **^/F2**: Press **^/F2**, **BREAK OUT** will be displayed on the screen, and then you can make an attendance when you need to go out during work time by fingerprint, password, or card.
- ◇ **∨/F3**: Press **∨/F3**, **BREAK IN** will be displayed on the screen, and then you can make an attendance when you return to the company during the work time by fingerprint, password, or card.

- ◇ **OK/F4:** Press **OK/F4**, **CHECK OUT** will be displayed on the screen, and then you can check out by fingerprint, password, or card.
- ◇ **OT-IN:** You can make an attendance record before you need to work overtime.
- ◇ **OT-OUT:** You can make an attendance record after you have worked overtime.

## 3.4 User

On the main menu, select **1 User**, and then you can add new users, query and edit user, edit department, and add cards in batches.

### 3.4.1 Add New Users

You can add users one by one or you can add users in batches.

#### 3.4.1.1 Add One by One

Step 1 On the main menu, select **1 User > Add New User**, and then the adding new user interface is displayed. See Figure 3-5 and Figure 3-6.

Figure 3-5 Adding new user (1)

Figure 3-6 Adding new user (2)

Step 2 Do the following operations:

- 1) Enter user ID and name;
- 2) Record user's fingerprints;
- 3) Let users set passwords;
- 4) Register a card for the new user;
- 5) Select a department;
- 6) Select a schedule mode;

7) Select a user level.

A new user is added.



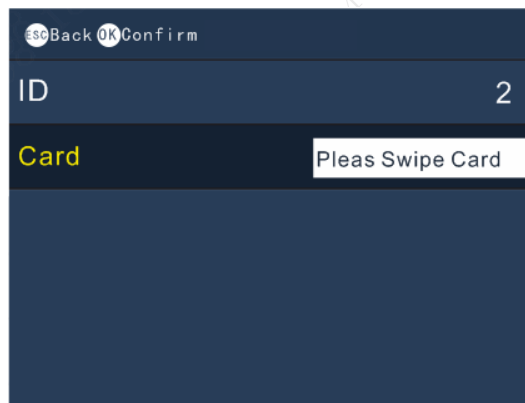
- Maximum user ID length is 8 digits (the user ID length range can be 1–99999999).
- Maximum user name length is 16 letters.
- Passwords can be numbers of 1–8 digits (Zero alone cannot be set as password and cannot be the first number of a password.).
- At most three fingerprints can be recorded for one user.

### 3.4.1.2 Add in Batches

#### Add users by swiping cards

Select **1 User > Add Cards in Batch**, swipe cards at the card reader, and then user ID, and card number will be automatically saved. You need to edit user names, add fingerprints and passwords separately. See Figure 3-7.

Figure 3-7 Swipe cards to add users



#### Add users through USB

Excel charts with special format are stored in the USB flash drive. You need to export the excel chart first, and then enter user information (including user ID, user name, password, card number, department, user level and schedule mode) into the charts, and then import the charts to the terminal. User information with the same User ID will be overwritten.

Step 1 On the main menu, select **4 USB > Import User Info**.

The prompt **New info will cover the before one** will be displayed.

Step 2 Press **Confirm-OK**.

And then user information will be imported.

### 3.4.2 Query & Edit User

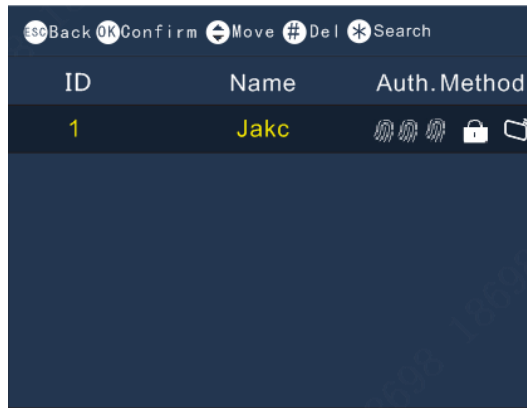
Step 1 On the main menu, select **1 User > Query & Edit User**.

Step 2 Press **OK/F4**.

See Figure 3-8.



Figure 3-8 Query & edit users



Step 3 Press  $\wedge$ /F2 or  $\vee$ /F3 to select a user.

Step 4 Press **OK/F4**.

Information of the user you selected will be displayed.

Step 5 Press **OK/4**.

And then you can edit user name, add fingerprints, register a card, modify department and schedule mode, and user level.

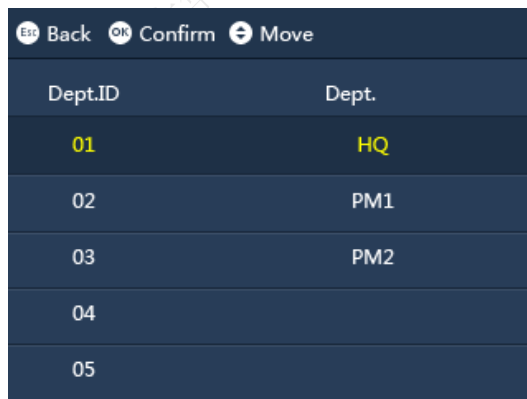
### 3.4.3 Edit Department

Step 1 On the main menu, select **1 User > Edit Dept.**

Step 2 Press **OK/F4**.

Department ID and Department name will be displayed. See Figure 3-9.

Figure 3-9 Edit department



Step 3 Press  $\wedge$ /F2 or  $\vee$ /F3 to select a user.

Step 4 Press **OK/F4**.

And then you can press letter keys to create department names.

Step 5 Press **OK/F4** to save names you entered.



- There are 20 departments in total and departments cannot be deleted.
- Department names cannot be null.

### 3.4.4 Add Cards in Batch

See “3.4.1.2 Add in Batches”.

## 3.5 Data



Before you export attendance record, make sure the USB is inserted. During exporting, do not remove the USB or operate the terminal, otherwise the exporting will fail and system malfunction will occur.

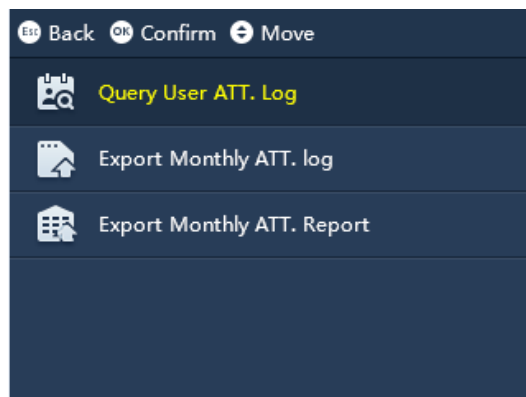
You can query and export attendance record.

### 3.5.1 Query User ATT. Log

Step 1 On the main menu, select **2 Data > Query User ATT. Log**.

See Figure 3-10.

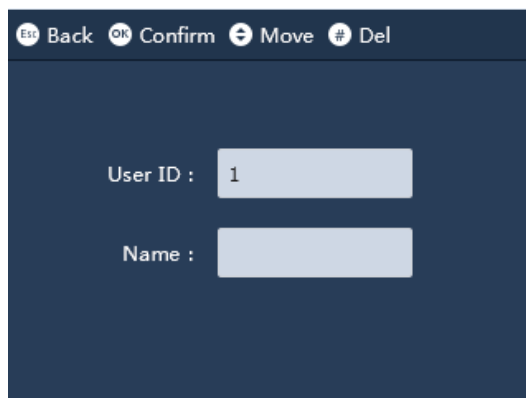
Figure 3-10 Query user ATT.Log



Step 2 Press **OK/F4**.

Step 3 Enter the **User ID** (**Name** will be displayed automatically). See Figure 3-11.

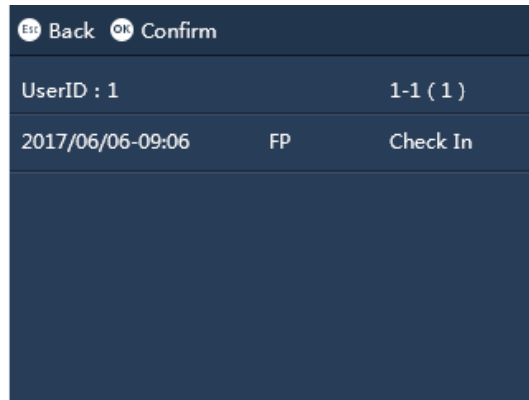
Figure 3-11 Enter user ID



Step 4 Press **OK/F4**.

Attendance record of the user will be displayed. See Figure 3-12.

Figure 3-12 Attendance record



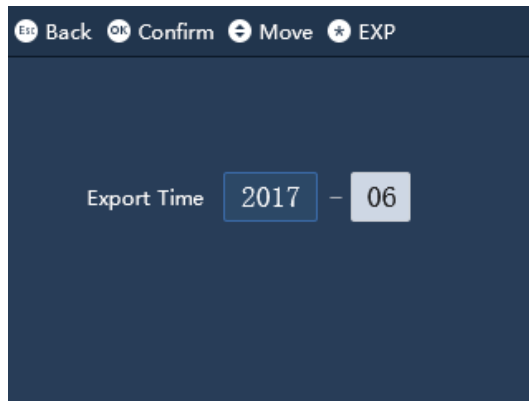
## 3.5.2 Export Monthly User ATT. Log/Export Monthly ATT. Report

Step 1 On the main menu, select **2 Data > Export Monthly ATT. Log or Export Monthly ATT. Report.**

Step 2 Press **OK/F4.**

Step 3 Select a date.  
See Figure 3-13.

Figure 3-13 Export logs/reports



Step 4 Press **OK/F4.**

Step 5 Press **☰ \* ⏻**.

The logs and reports will be exported.

## 3.6 Shift

You can set shift periods. There are 24 shifts in total.

### 3.6.1 Shift Setting

On the main menu, select **3 Shift > Shift Setting > Shift.** You can set 24 shifts at most.  
See Figure 3-14.

Figure 3-14 Shift setting

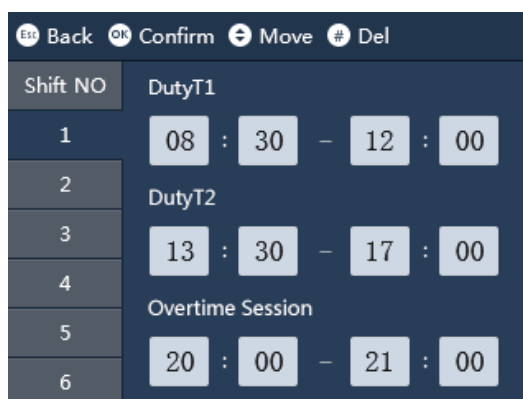


Table 3-1 Shift setting description

Duty	Description
Duty T1	You can set duration for duty time in each shift. For example 08:30–12:00.
Duty T2	You can set duration for duty time in each shift. For example 13:30–17:00.
Overtime Session	You can set overtime duration. For example 20:00–21:00.



- There are two periods in which you may need to sign in and sign out, because there is an interval between Duty T1 and Duty T2.
- If you signed in for more than once, the system takes the earliest sign in records as effective; if you signed out for more than once, the system only takes the latest sign out records as effective.
- In Overtime Session, there is no late/early leave time setup.

## Import/Export shift

Once you have done shift settings on a terminal, you can export the settings through flash drives and then import them to other terminals, thus you do not need to do settings repeatedly.

### 3.6.2 Schedule Setup

On the main menu, select **3 Shift > Schedule Setup**, and then you can set schedule in each month (only the current month and the next month) for users and set schedules in each week for departments.

#### User schedule

Step 1 On the main menu, select **Shift > Schedule Setup > User Schedule**.

Step 2 Press **OK/F4**.

Step 3 Enter the user ID.

User name and department name will be displayed automatically.

Step 4 Press **OK/F4**.

See Figure 3-15.

Figure 3-15 User schedule

User:1 2017/6 schedules						
Sun	Mon	Tue	Wed	Thu	Fri	Sat
				1 1	2 1	3
4	5 1	6 1	7 1	8 1	9 1	10
11	12 1	13 1	14 1	15 1	16 1	17
18	19 1	20 1	21 1	22 1	23 1	24
25	26 1	27 1	28 1	29 1	30 1	



- Numbers at the center of each box are shift numbers. There are 24 shifts in total.
- Numbers at the top left corner of each box are days.
- Null and 0 means off duty.
- 25 means business trip.
- 26 means leave.

## Department Schedule

**Step 1** On the main menu, select **Shift > Schedule Setup > Department**.

**Step 2** Select a department.

**Step 3** Press **OK/F4**.

See Figure 3-16.

Figure 3-16 Department schedule

Dept:Product schedules						
Sun	Mon	Tue	Wed	Thu	Fri	Sat
	1	1	1	1	1	

## Import/Export Schedule



Before you export or import schedules, make sure the USB is inserted. During exporting or importing, do not remove the USB or operate the terminal, otherwise exporting or importing will fail and system malfunction will occur.

Once you have done schedule settings on a terminal, you can export the settings through flash drives and then import them to other terminals, thus you do not need to do settings repeatedly.

### 3.6.3 Late-in/Early-out Allowed

Late-in Allowed is used to set flexible working hours. For example the permitted start working time is 8:30, and the late time is 5 minutes, then if a user gets his/her attendance checked before 8:35, he/she is not considered to be late.

Early-out Allowed is used to set flexible working hours, too. For example the permitted finishing working time is 17:30, and the early leave time is 5 minutes, then if a user gets his/her attendance checked after 17:25, he/she is not considered to have left early.

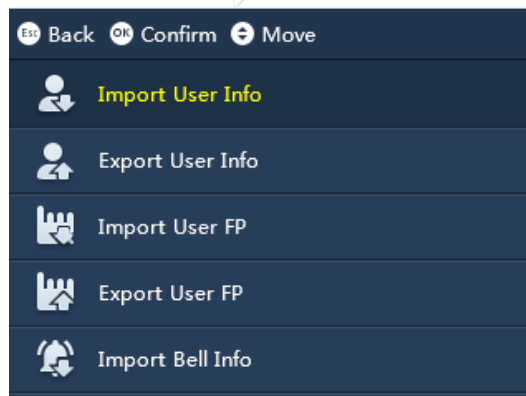


- During Duty 1 and Duty 2 period, you have only one chance to get your attendance checked late and one chance to leave early.
- If you arrive late or leave early within the time period permitted, overtime will still be counted.

## 3.7 USB

Select **4 USB**, and then you can import/export user Information, fingerprints, bell information, and auto switch time. See Figure 3-17.

Figure 3-17 USB



### 3.7.1 Import/Export User Info

Excel charts with special format are stored in the USB flash drive. You can enter user information (including user ID, user name, password, card number, department, user level and schedule mode) into the charts, and then import/export the charts to/from the terminal. User information with the same user ID will be overwritten.

### 3.7.2 Import/Export User FP

Fingerprints collected can be imported and exported to/from the terminal.

### 3.7.3 Import/Export Bell Info

Bell information can be imported and exported to/from the terminal. The bell will ring in the periods you set.

### 3.7.4 Import/Export Auto Switch Time

Auto switch time can be imported and exported to/from the terminal. Check in, Break out, Break in, Check out, OT-In, and OT-Out will be displayed on the screen during the period you set.

## 3.8 Feature

On the main menu, select **5 Feature**, and then you can do settings and configurations about date and time, network communication, features (state switch time, bell time, recheck interval, verification method, system auto test, attendance event mode, fixed mode setup, and open door keep time).

### 3.8.1 Date & Time

On the main menu, select **5 Features > Date & Time**, and then you can do settings about date, time, time zone, DST setting, and network time protocol (NTP).

#### Date Format

There are three options: YY\_MM\_DD, DD\_MM\_YY, and MM\_DD\_YY.



Y stands for year. M stands for month. D stands for day.

#### Date Setting

Set a date for the terminal. The date will be displayed on the screen.

#### Time Setting

Set time for the terminal. The time will be displayed on the screen.

#### Time Zone

Set time zone for the terminal. The time zone range is GMT-12:00 to GMT+13:00.

#### DST

You can set daylight saving time.

- If you select **By Date**, you can set start/end date and start/end time of the DST.
- If you select **By Week**, you can set start/end time, month and week of the DST.

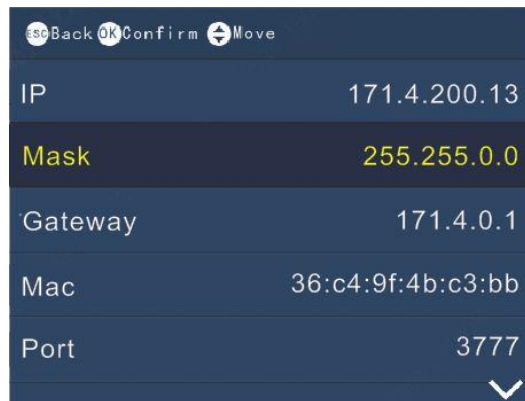
## NTP Setting

You can set IP, port, and update period (min) for the NTP server.

### 3.8.2 Communication

On the main menu, select **5 Feature > Communication**, and then you can configure IP address, mask, gateway, MAC, and port. See Figure 3-18.

Figure 3-18 Communication



The screenshot shows a configuration menu with the following settings:

Parameter	Value
IP	171.4.200.13
Mask	255.255.0.0
Gateway	171.4.0.1
Mac	36:c4:9f:4b:c3:bb
Port	3777

Table 3-2 Parameter description

Parameter	Description
IP	It is 192.168.1.108 by default.
Mask	It is 255.255.255.0 by default.
Gateway	It is 192.168.1.1 by default.
MAC	MAC address of the terminal and it cannot be modified.
Port	Port number, used to login the terminal on the SmartPSS.

### 3.8.3 Features

Select **5 Feature > Features**, and then you can set state switch time, bell time, recheck interval, verification method, system auto test, attendance event mode, fixed mode setup, and open door keep time.

#### 3.8.3.1 State Switch Time

You can set state switch time. There are 24 options and six states: Check in, Break out, Break in, Check out, OT-In, and OT-Out. See Figure 3-19.



Figure 3-19 State switch time

Esc Back OK Confirm ← Move # Del		
NO.	Time	State
1	08:00	Check In
2	17:30	Check Out
3	00:00	NULL
4	00:00	NULL
5	00:00	NULL
6	00:00	NULL

### 3.8.3.2 Bell Time

You can set bell time, ringing cycle, and ringing duration for the bell. See Figure 3-20.

Figure 3-20 Bell time

Esc Back OK Confirm			
	Time	Cycle	Duration(s)
1	00:00	Every Day	00
2	00:00	Every Day	00
3	00:00	Every Day	00
4	00:00	Every Day	00
5	00:00	Every Day	00

### 3.8.3.3 Recheck Interval

Recheck interval is used to set the interval in which you can get your attendance checked. For example, if you select 3, then you can get your attendance checked only once in every three minutes. There are ten options: 0, 1, 2, 3, 4, 5, 6, 7, 8, and 9.

### 3.8.3.4 Verification Method

There are four options: FP or PWD or Card, FP, PWD, and Card.

- If you select **FP or PWD or Card**, your attendance will be checked by fingerprint, password, or card.
- If you select **FP**, your attendance can only be checked by fingerprint.
- If you select **PWD**, your attendance can only be checked by password.
- If you select **Card**, your attendance can only be checked by card.

### 3.8.3.5 System Auto Test

There are six options: auto test, FP, display, voice, key, and USB.

### 3.8.3.6 Att.Event Mode

There are three attendance check mode: Auto/Manual, Fixed, and Forced.

#### Auto/Manual

In **Auto/Manual** mode, there are three methods:

- You can get your attendance checked directly by pressing your finger at the fingerprint sensor, by entering your user ID and password, or by swiping your card;



You need to do shift settings in advance in **3 Shift > Shift Setting > Shift**. See “3.6.1 Shift Setting”.

- You can select an attendance event by pressing **Esc/F1**, **^/F2**, **∨/F3**, and **OK/F4**, and then do fingerprint, password, or card attendance check;
- You can get your attendance recorded without doing shift settings and without selecting attendance events.

#### Fixed

In the Fixed mode, you can select a fixed attendance event for a terminal, and then users can sign in at one terminal and sign out at another terminal.

**Step 1** On the standby interface, select **5 Feature > Features > Att. Event Mode**.

**Step 2** Press **OK/F4**.

The white text box appears.

**Step 3** Press **^/F2** or **∨/F3** to select Fixed.

**Step 4** Press **OK/F4**.

**Step 5** Press **∨/F3**.

**Step 6** Press **OK/F4**.

The white text box appears.

**Step 7** Press **^/F2** or **∨/F3** to select among Check in, Break out, Break in, Check out, OT-In, and OT-Out.

#### Forced

In the Forced mode, you need to select your attendance type (1.Check in; 2.Break out; 3.Break in; 4.Check out; 5.OT-In; 6.OT-Out) after you press your finger tip at the fingerprint sensor, enter your user ID and password, or swiping your card.

**Step 1** On the standby interface, select **5 Feature > Features > Att. Event Mode**.

**Step 2** Press **OK/F4**.

The white text box appears.

**Step 3** Press **^/F2** or **∨/F3** to select Forced.

**Step 4** Press **OK/F4**.

## Fixed Mode

If you selected **Forced** in **5 Feature > Features > Att.Event Mode**, you can select a fixed attendance event, then users can sign in at one terminal and sign out at another terminal.

## Open Door Keep Time (SEC)

The terminal can be connected to access control devices to unlock doors. The time range that the doors will be open is 0–600 seconds.

### 3.8.4 System

Select **5 Feature > System**, and then you can turn on/off tone switch and broadcast volume switch, adjust volume, restore the terminal to the factory settings, restore the terminal to the factory settings with user information and logs saved, reboot the terminal, do firmware update, set device ID, and set screen sleep time (min). See Figure 3-21 and Figure 3-22.

Figure 3-21 System (1)

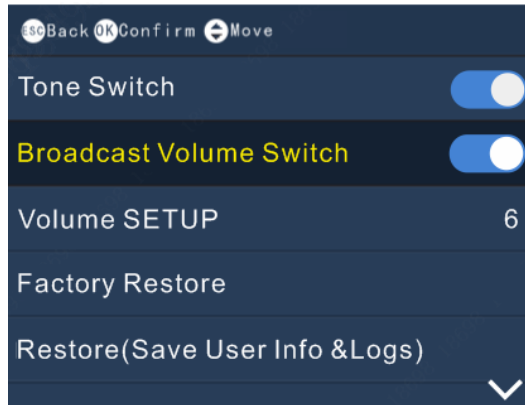
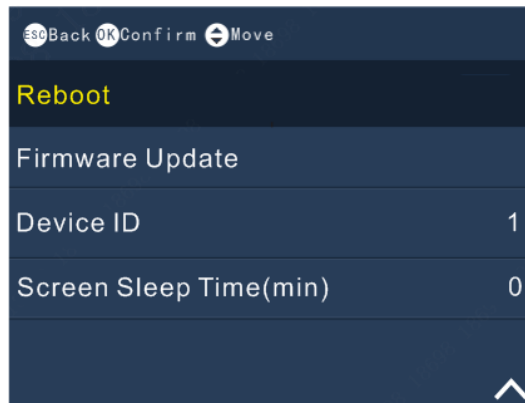


Figure 3-22 System (2)



- **Factory Restore:** you can restore the terminal to the factory settings.
- **Restore (Save User Info & Logs):** restore the terminal to the factory settings with user information and logs saved.
- **When doing firmware update,** you need to modify the file name to Update.bin.
- **The range of screen sleep time is 0–60min.**

## 3.8.5 Language

There is only one language: English.

## 3.9 System

Select **6 System**, and then you can do admin level management, view registration information and device information.

### Admin Level Management

Select **6 SysInfo > Admin Level Management**, the administrator information is displayed. You can modify the administrator level. After you have modified the user level to **user**, the user used to be the administrator will not be displayed in the Admin Level Management.



You can also modify user level by selecting **1 User > Query & Edit User**, and then selecting a user to modify the user level.

### Management

Select **6 SysInfo > Management**, and then you can view administrators' operational records (for example user information modification and system setting modification records).

### Registration Info

Select **6 SysInfo > Registration Info**, and then you can view registration information (users that can be registered, administrator number, fingerprint number, password number, card number, attendance record report number, and management records the terminal can restore). See Figure 3-23.

Figure 3-23 Registration info

Back	
User	1/1000
Administrator	0/5
FP	0/2000
PWD	1/1000
Card	1/1000
Att.record report	4/10000

### Device Info

Select **6 SysInfo > Registration Info**, and then you can view terminal version number and device ID.


# 4 Attendance Configuration on SmartPSS

You can create departments and add users; set attendance time period, shift, holiday, and attendance event; view real-time attendance information; view and download attendance statistics through the SmartPSS.

## 4.1 Creating Departments and Adding Users

You need to create departments and add users, and then you can do attendance settings for departments and users.

### 4.1.1 Creating Departments

**Step 1** Click  on the **New** interface.  
The **Attendance** interface is displayed.


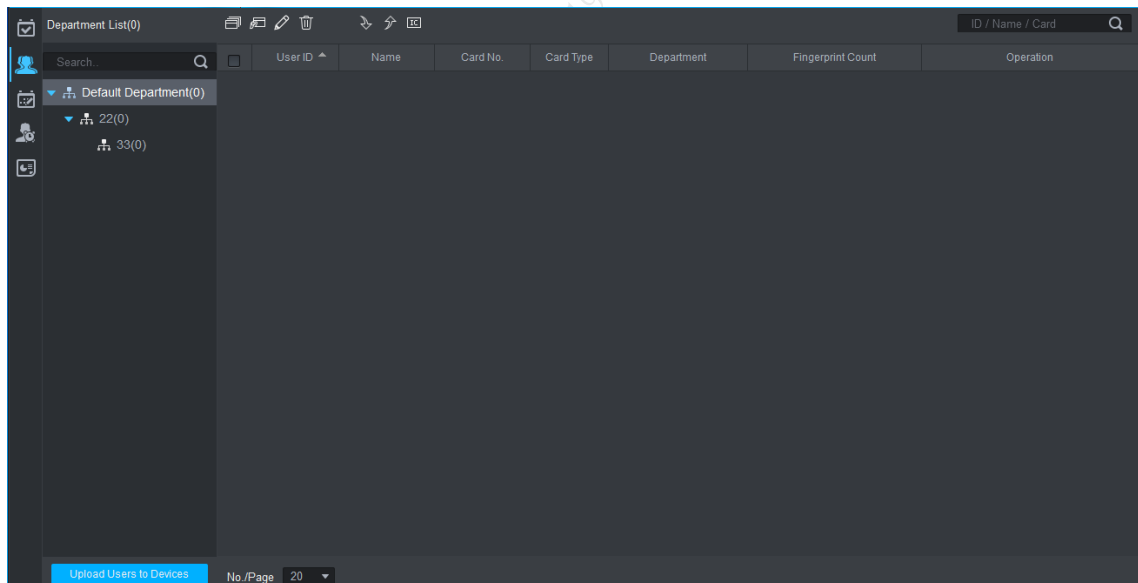
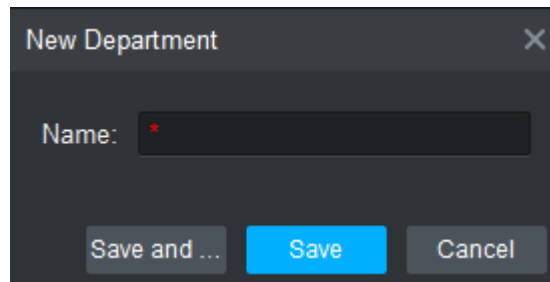
**Step 2** Click  on the Attendance interface.  
And the **User** interface is displayed. See Figure 4-1.

Figure 4-1 User



**Step 3** Click the right mouse button on the **Default Department** and then click **Add Department**.  
The **New Department** interface is displayed. See Figure 4-2.

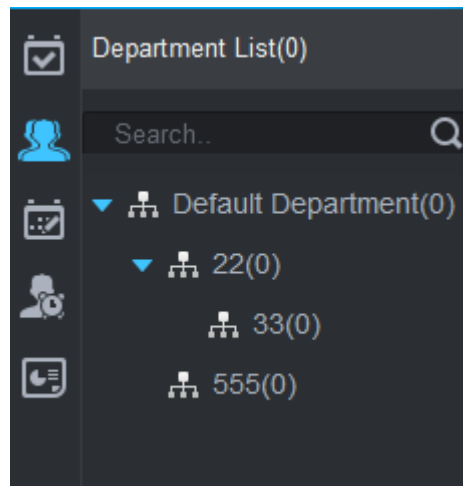
Figure 4-2 New department




Step 4 Enter department name and click **Save**.

A department is created. See Figure 4-3.

Figure 4-3 A department is created



## 4.1.2 Adding Users

Step 1 Click  on the **Attendance** interface.

The **Add User** interface is displayed. See Figure 4-4.



Figure 4-4 Add user

The screenshot shows the 'Add User' dialog box with the following fields and values:

- User ID: \*
- Name: \*
- Department: Default Department
- Card No.: Card Reader not ready!
- Card issuer: [Dropdown]
- User Type: General
- Card Password: [Text Field]
- Valid Time: 2019/4/24 0:00:00 to 2029/4/24 23:59:59 (3654 Days)
- Image Size: 0 ~ 120KB

**Step 2** Enter basic information, fingerprint info, and details, and then click **Finish**.  
A new user is added.



- You can upload users in the SmartPSS to the Time & Attendance Terminal by clicking **Upload Users to Devices** on the bottom left corner of the **User** interface.
- You can import and export users by clicking  or 

## 4.2 Attendance Setting

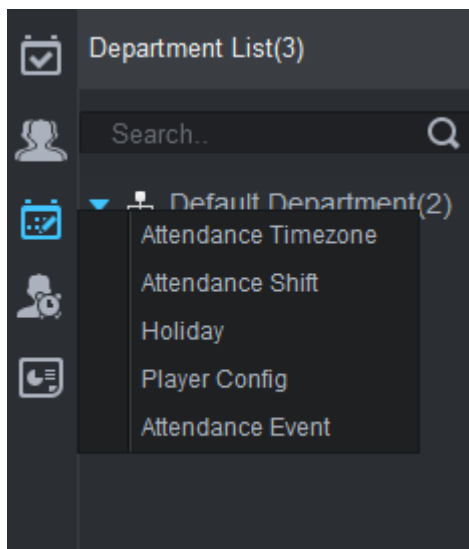
### 4.2.1 Attendance Time Zone

By setting attendance time zone, you can configure in which periods users need to get their attendance checked according to company regulations.

**Step 1** Click  on the Attendance interface.

Figure 4-5 is displayed.

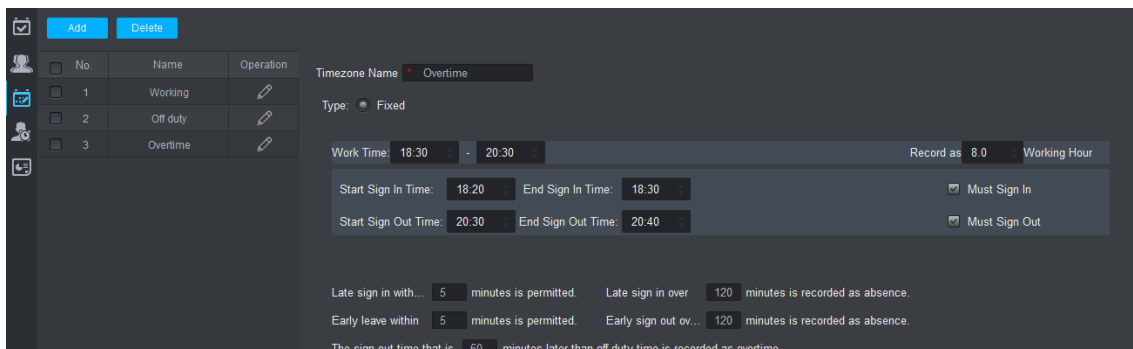
Figure 4-5 Attendance setting



**Step 2** Click **Attendance Timezone**.

The attendance timezone interface is displayed. See Figure 4-6.

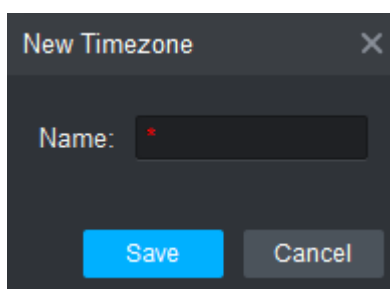
Figure 4-6 Attendance timezone



**Step 3** Click **Add** on the top left corner of the interface.

The **New Timezone** interface is displayed. See Figure 4-7.

Figure 4-7 New Timezone



**Step 4** Enter timezone name and click **Save**.

**Step 5** The timezone setting interface is displayed. See Figure 4-8.



Figure 4-8 Timezone setting

Timezone Name: Overtime

Type:  Fixed  Flexible

Work Time: 18:30 - 20:30 Record as: 8.0 Working Hour

Start Sign In Time: 18:20 End Sign In Time: 18:30  Must Sign In +

Start Sign Out Time: 20:30 End Sign Out Time: 20:40  Must Sign Out

Late sign in within... 5 minutes is permitted. Late sign in over 120 minutes is recorded as absence.

Early leave within 5 minutes is permitted. Early sign out over... 120 minutes is recorded as absence.

The sign out time that is 60 minutes later than off duty time is recorded as overtime.

Save Cancel

Table 4-1 Timezone setting description

Parameter	Description
Time Zone Name	Customize period name.
Type	<p>Select work attendance type, including fix and free.</p> <ul style="list-style-type: none"> <li>● Attendance type is set to fix attendance. For more info, please see the rest of this chart.</li> <li>● Attendance type is free attendance, and you only need to set duration and whether to limit the latest sign in time.</li> </ul>
Work Time	Set work time of this period, meantime please select day of week.
Record as X Workday	One week time is recorded as how many weekdays.
Start Sign In Time	<ul style="list-style-type: none"> <li>● If this period of attendance time zone has two separate sub periods, then you shall click  to set second work time sign in/out time.</li> <li>● If you set two work time, then both time shall have sign in/out to be valid for normal attendance.</li> </ul>
End Sign In Time	
Start Sign Out Time	
End Sign Out Time	
Late sign in within X minutes is permitted.	<p>Define late, early leave and absence.</p> <p>You can set different time ranges, the followings are example only.</p> <p>Set start time of work time has standard sign in time. Actual time later is than this time, within <math>5\text{ min} &lt; X \leq 30\text{min}</math>, will be late.</p> <p>Set start time of work time has standard sign in time. Actual time later is than this time, <math>X &gt; 30\text{min}</math>, will be absence.</p> <p>Set end time of work time has standard sign out time. Actual sign out is earlier than this time, and <math>0\text{min} &lt; X \leq 5\text{min}</math>, will be early leave.</p>
Late sign in over X minutes is recorded as absence.	
Early leave within X minutes is permitted.	

Parameter	Description
Early sign out over X minutes is recorded as absence.	Set end time of work time has standard sign out time. Actual sign out is earlier than this time, and $5\text{min} < X \leq 30\text{min}$ , will be absence.
The sign out time that is X minutes later than off duty time is recorded as overtime.	Set end time of work is standard off duty time. Actual sign out time later than this time, and over set value will be overtime.

Step 6 set timezone settings and click **Save**.

A new timezone is created.

## 4.2.2 Attendance Shift

Attendance shifts are the status of days, weeks or months. You can set status for each day within a week and a month, or you can set working status for every single day.



- There are four statuses: **Rest**, **Working**, **Off Duty**, and **Overtime**.
- There are three types of attendance shifts: **Week**, **Month**, and **Day**.

See Figure 4-9 to Figure 4-11 for attendance shift types.

Figure 4-9 Attendance shift (Week)

No.	Date	Timezone	Operation
1	Sun	Working	Enable all
2	Mon	Working	Enable all
3	Tue	Working	Enable all
4	Wed	Working	Enable all
5	Thu	Working	Enable all
6	Fri	Working	Enable all
7	Sat	Rest	Enable all

Figure 4-10 Attendance shift (Month)

No.	Date	Timezone	Operation
1	1	Working	Enable all
2	2	Working	Enable all
3	3	Working	Enable all
4	4	Working	Enable all
5	5	Working	Enable all
6	6	Working	Enable all
7	7	Working	Enable all
8	8	Working	Enable all
9	9	Working	Enable all
10	10	Working	Enable all
11	11	Working	Enable all
12	12	Working	Enable all
13	13	Working	Enable all
14	14	Working	Enable all
15	15	Working	Enable all
16	16	Working	Enable all
17	17	Working	Enable all

Figure 4-11 Attendance shift (Day)

No.	Date	Timezone	Operation
1	Day 1	Working	Enable all
2	Day 2	Working	Enable all
3	Day 3	Working	Enable all
4	Day 4	Working	Enable all
5	Day 5	Working	Enable all
6	Day 6	Working	Enable all
7	Day 7	Working	Enable all
8	Day 8	Working	Enable all
9	Day 9	Working	Enable all
10	Day 10	Working	Enable all
11	Day 11	Working	Enable all
12	Day 12	Working	Enable all
13	Day 13	Working	Enable all
14	Day 14	Working	Enable all
15	Day 15	Working	Enable all
16	Day 16	Working	Enable all
17	Day 17	Working	Enable all

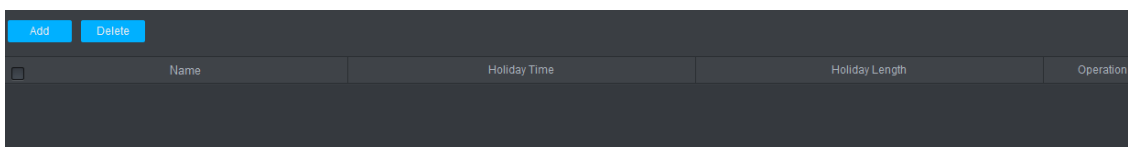
### 4.2.3 Holiday

When doing attendance shift setting, you need to set holidays so that users do not need to get their attendance checked.

Step 1 Select **Attendance Setting > Holiday**.

The **Holiday** interface is displayed. See Figure 4-12.

Figure 4-12 Holiday (1)

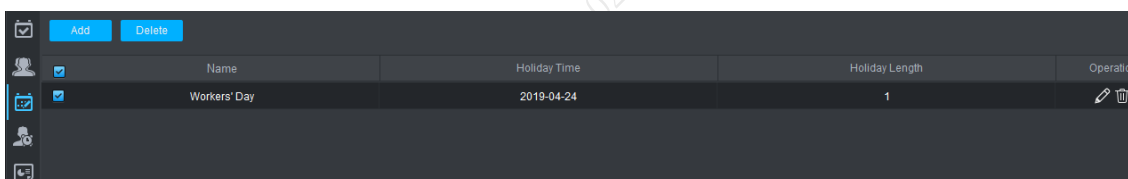


**Step 2** Click **Add** on the top left corner of the interface.  
The **Holiday** interface is displayed. See Figure 4-13.

Figure 4-13 Holiday (2)

**Step 3** Enter holiday name, select holiday time, enter holiday length, and then click **OK**.  
A holiday is added. See Figure 4-14.

Figure 4-14 A holiday is created



## 4.2.4 Attendance Event

There are seven default attendance events: Punch the Clock, Sign In, Go Out, Come back, Sign Out, Overtime work sign out, and Overtime work sign in.

**Step 1** Select **Attendance Setting > Attendance Event**.  
The **Attendance Event** interface is displayed. See Figure 4-15.

Figure 4-15 Attendance Event

<input type="checkbox"/>	Encode	Att Events	Operation
	0	Punch The Clock	
	1	Sign In	
	2	Go Out	
	3	Come Back	
	4	Sign Out	
	5	Overtime work sign out	
	6	1	

**Step 2** Click and you can edit attendance event names. See Figure 4-16.

Figure 4-16 Edit attendance event name


Dialog box titled "Edit Name" with the following fields:

- Encode: 6
- Original Name: Overtime work sign in
- Modify Name: 1

Buttons: OK, Cancel

## 4.3 Shift Schedule

You can set shift schedules and temporary shift for users.

Step 1 Click  on the Attendance interface.

The **Shift Schedule** interface is displayed. See Figure 4-17.

Figure 4-17 Shift schedule

Default Department	User ID/Name	Sun	Mon	Tue	Wed	Thu	Fri	Sat
	<input type="checkbox"/> 55 55	31	1	2	3	4	5	6
	<input type="checkbox"/> 66 66	7	8	9	10	11	12	13
		14	15	16	17	18	19	20
		21	22	23	24	25	26	27
		28	29	30	1	2	3	4
		5	6	7	8	9	10	11

Step 2 Select a department from the Default Department drop-down list.

Step 3 Select users. See Figure 4-18.

Figure 4-18 Select department and users

Default Department: [Dropdown]

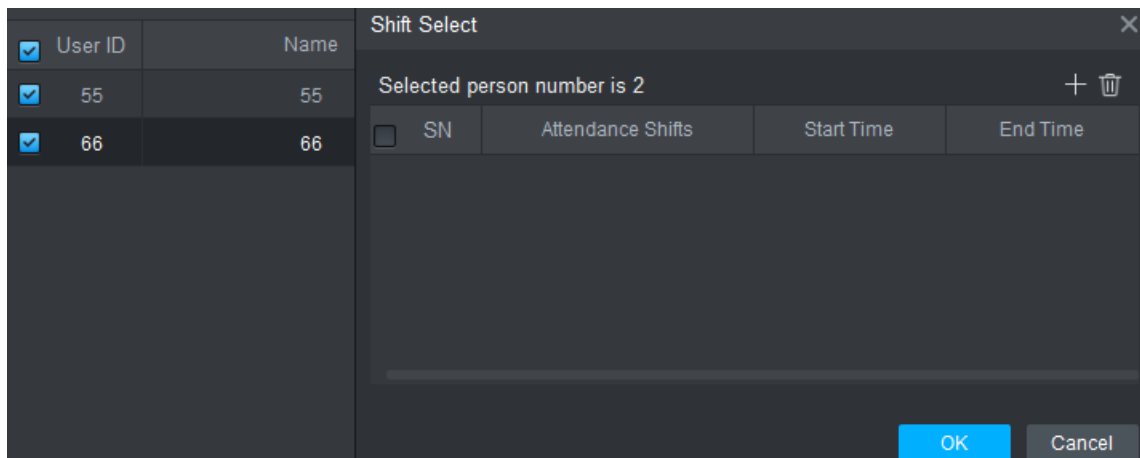
User ID/Name: [Search]


User ID	Name
<input type="checkbox"/> 55	55
<input type="checkbox"/> 66	66

**Step 4** Click  at the bottom left corner of the interface.

The **Shift Select** interface is displayed. See Figure 4-19

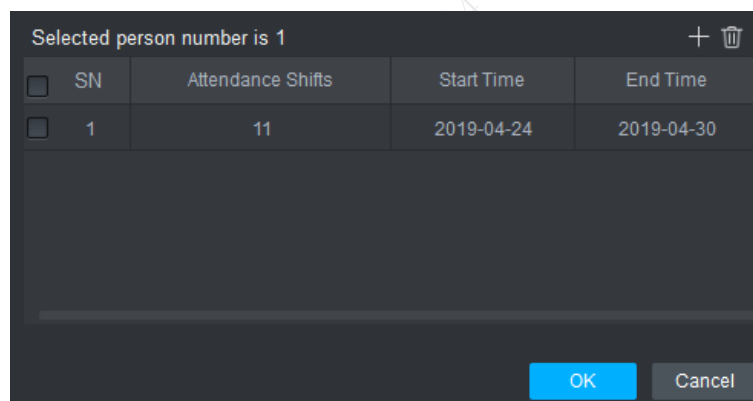
Figure 4-19 Shift select



**Step 5** Click  at the top right corner of the interface.

And then you can set attendance shift, start time, and end time for the user you have selected.

Figure 4-20 Set attendance shift



Double-click the attendance shift names, start time, and end time, and then you can select attendance shifts, set start time and end time.




**Step 6** Click **OK**.

The attendance shift of the user or users you selected will be displayed on the attendance interface. See Figure 4-21.

Figure 4-21 Attendance shift of the user (s) you selected

2019-04						
Sun	Mon	Tue	Wed	Thu	Fri	Sat
31	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23 Take Working Days Off T	24 Overtime T	25 H	26 Working	27 Working
28 Working	29 Working	30 Working	1	2	3	4
5	6	7	8	9	10	11

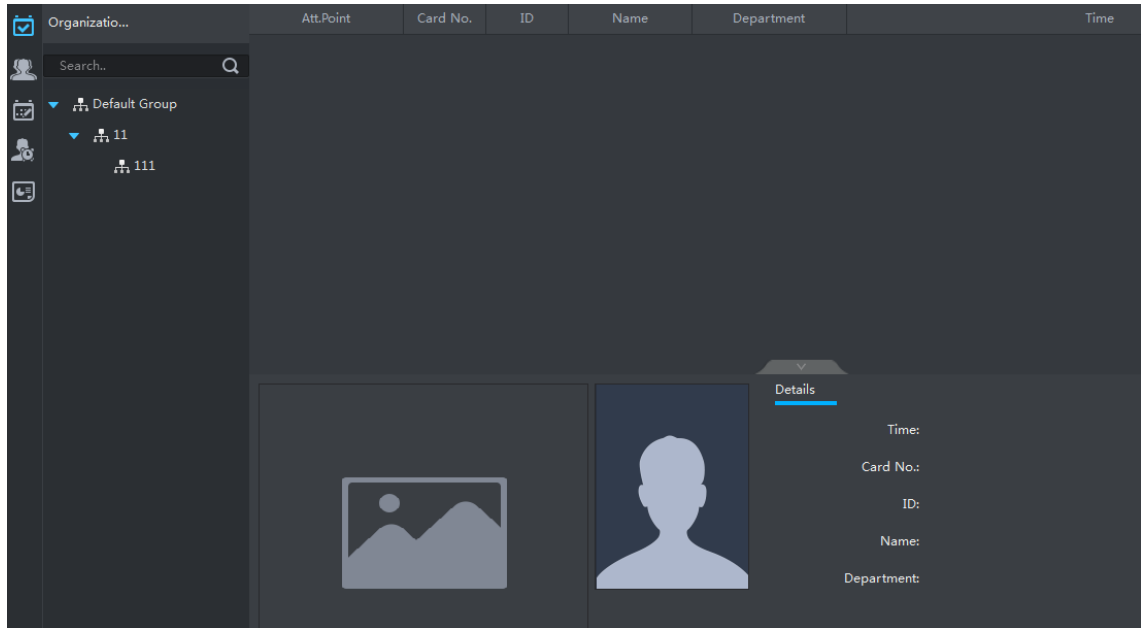


- : Select users, and then click this icon, then you can set temporary for users.
- : Select users and select a temporary shift (with blue T), and then you can delete a temporary.
- : Means the day is a holiday.

## 4.4 Viewing Real-Time Attendance Check Detail

When users are checking their attendance, their information will be displayed on the Console interface. See Figure 4-22.

Figure 4-22 View real-time attendance check detail



18698 大华 2019-02-14



## 4.5 Attendance Report

You can view the following information on the **Report** interface: attendance statistics, attendance detail, overtime, exception, break, leave, first-in last-out, and logs.


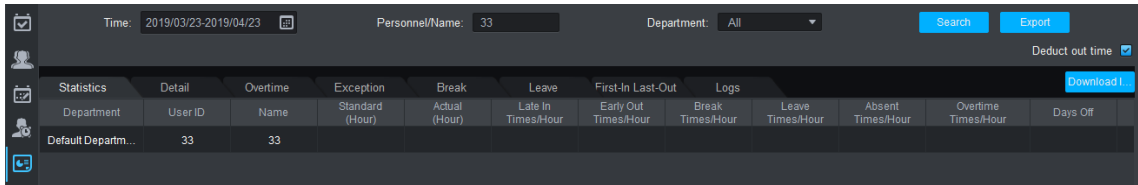
Click . The **Report** interface is displayed. See Figure 4-23.

Figure 4-23 Report



The screenshot shows the Report interface with the following data:

Department	User ID	Name	Standard (Hour)	Actual (Hour)	Late In (Times/Hour)	Early Out (Times/Hour)	Break (Times/Hour)	Leave (Times/Hour)	Absent (Times/Hour)	Overtime (Times/Hour)	Days Off
Default Departm...	33	33									

18698 大华 2019-02-14

# Appendix 1 Fingerprint Record Description

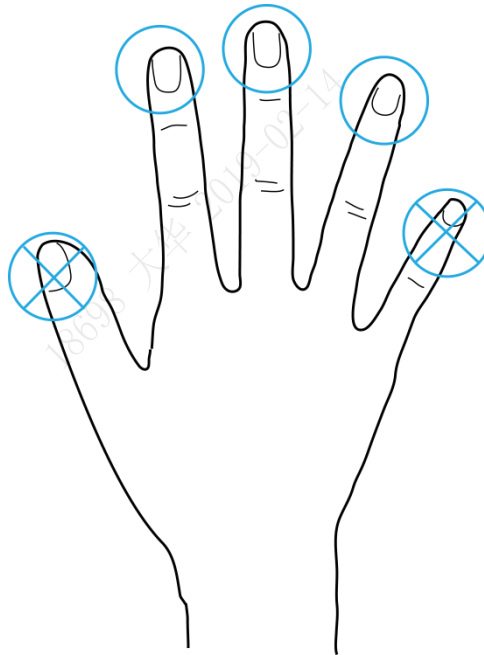
## Notice

- Make sure that your fingers are clean and dry before recording your fingerprints.
- Press your finger to the fingerprint recording area, and make your fingerprint is centered on the recording area.

## Fingers recommended

Forefingers, middle fingers, and ring fingers are recommended. Thumbs and little fingers cannot be put at the recording center easily.

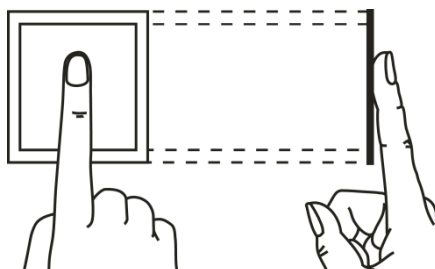
Appendix figure 1-1 Recommended fingers



## Finger pressing method

- Correct method

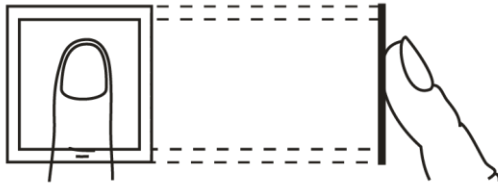
Appendix figure 1-2 Correct finger pressing



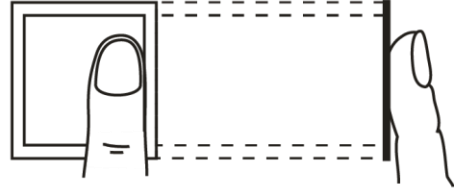
- Incorrect method

Appendix figure 1-3 Wrong finger pressing

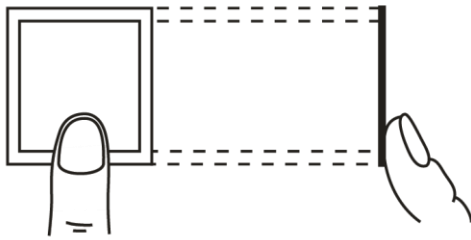
Fingertip perpendicular to the record area



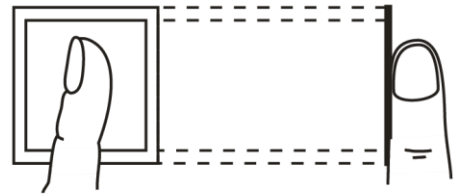
Fingertip not at the center of the record area



Fingertip not at the center of the record area






Fingertip inclination






18698 大华 2019-02-14

# Appendix 2 Text Input

You can type English letters, numbers and punctuation. You need to click    to switch.

## Number

Step 1 Press    until **123** is displayed on the screen.

Step 2 Enter numbers.  
See Appendix figure 2-1.

Appendix figure 2-1



Step 3 Press **OK/F4** to confirm.

## Letter

Step 1 Press    until **ABC** is displayed on the screen.




Step 2 Enter letters.  
See Appendix figure 2-1.

Appendix figure 2-2



Step 3 Press **OK/F4** to confirm.

## Punctuation

Step 1 Press    until **:-)** is displayed on the screen.

Step 2 Press number key.  
Punctuations will be displayed on the screen.

Step 3 Press **^/F2** or **∨/F3** to select.

Step 4 Press **OK/F4** to confirm.

## Appendix 3 FAQ

- Q: After I have got my fingerprint read by the fingerprint sensor, the system asks me to re-press my finger, and attendance check failed.  
A: Check if your fingerprints have been recorded.
- Q: The bell does not work.  
A: Check if bell setup is correct and if the broadcast volume switch is on.
- Q: I cannot update the terminal by USB flash drive.  
A: Check if the terminal has recognized the USB flash drive and check update file name.
- Q: Failed to export by USB flash drive.  
A: Use USB flash drive in FAT32 format.
- Q: I forget administrator password.  
A: Contact the manufacturer.
- Q: I want to search for user attendance record.  
A: In the standby interface, press #, and then press your finger at the fingerprint sensor, or enter the user ID and password, or swipe the card.

18698 大华 2019-02-1

# Appendix 4 Cybersecurity Recommendations

Cybersecurity is more than just a buzzword: it's something that pertains to every device that is connected to the internet. IP video surveillance is not immune to cyber risks, but taking basic steps toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations from Dahua on how to create a more secured security system.

## **Mandatory actions to be taken for basic equipment network security:**

### **1. Use Strong Passwords**

Please refer to the following suggestions to set passwords:

- The length should not be less than 8 characters;
- Include at least two types of characters; character types include upper and lower case letters, numbers and symbols;
- Do not contain the account name or the account name in reverse order;
- Do not use continuous characters, such as 123, abc, etc.;
- Do not use overlapped characters, such as 111, aaa, etc.;

### **2. Update Firmware and Client Software in Time**

- According to the standard procedure in Tech-industry, we recommend to keep your equipment (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the equipment is connected to the public network, it is recommended to enable the "auto-check for updates" function to obtain timely information of firmware updates released by the manufacturer.
- We suggest that you download and use the latest version of client software.

## **"Nice to have" recommendations to improve your equipment network security:**

### **1. Physical Protection**

We suggest that you perform physical protection to equipment, especially storage devices. For example, place the equipment in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable equipment (such as USB flash disk, serial port), etc.

### **2. Change Passwords Regularly**

We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

### **3. Set and Update Passwords Reset Information Timely**

The equipment supports password reset function. Please set up related information for password reset in time, including the end user's mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

### **4. Enable Account Lock**

The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

## **5. Change Default HTTP and Other Service Ports**

We suggest you to change default HTTP and other service ports into any set of numbers between 1024~65535, reducing the risk of outsiders being able to guess which ports you are using.

## **6. Enable HTTPS**

We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

## **7. Enable Whitelist**

We suggest you to enable whitelist function to prevent everyone, except those with specified IP addresses, from accessing the system. Therefore, please be sure to add your computer's IP address and the accompanying equipment's IP address to the whitelist.

## **8. MAC Address Binding**

We recommend you to bind the IP and MAC address of the gateway to the equipment, thus reducing the risk of ARP spoofing.

## **9. Assign Accounts and Privileges Reasonably**

According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

## **10. Disable Unnecessary Services and Choose Secure Modes**

If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.

If necessary, it is highly recommended that you use safe modes, including but not limited to the following services:

- SNMP: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
- SMTP: Choose TLS to access mailbox server.
- FTP: Choose SFTP, and set up strong passwords.
- AP hotspot: Choose WPA2-PSK encryption mode, and set up strong passwords.

## **11. Audio and Video Encrypted Transmission**

If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

Reminder: encrypted transmission will cause some loss in transmission efficiency.

## **12. Secure Auditing**

- Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
- Check equipment log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

## **13. Network Log**

Due to the limited storage capacity of the equipment, the stored log is limited. If you need to save the log for a long time, it is recommended that you enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

## **14. Construct a Safe Network Environment**

In order to better ensure the safety of equipment and reduce potential cyber risks, we recommend:

- Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.

- The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
- Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.

18698 大华 2019-02-14



# Time & Attendance Terminal

Quick Start Guide

**V1.0.0**

# Important Safeguards and Warnings

This Chapter describes the contents covering proper handling of the access standalone, hazard prevention, and prevention of property damage. Read these contents carefully before using the access standalone, comply with them when using, and keep it well for future reference.

## Operation Requirement

- Do not place or install the access standalone in a place exposed to sunlight or near the heat source.
- Keep the access standalone away from dampness, dust or soot.
- Keep the access standalone installed horizontally on the stable place to prevent it from falling.
- Do not drop or splash liquid onto the access standalone, and make sure there is no object filled with liquid on the access standalone to prevent liquid from flowing into the access standalone.
- Install the access standalone in a well-ventilated place, and do not block the ventilation of the access standalone.
- Operate the access standalone within the rated range of power input and output.
- Do not disassemble the access standalone.
- Transport, use and store the access standalone under the allowed humidity and temperature conditions.

## Electrical Safety


- Improper battery use might result in fire, explosion, or inflammation.
- When replacing battery, make sure the same model is used.
- Use the recommended power cables in the region and conform to the rated power specification.
- Use the power adapter provided with the access standalone; otherwise, it might result in people injury and device damage.
- The power source shall conform to the requirement of the Safety Extra Low Voltage (SELV) standard, and supply power with rated voltage which conforms to Limited power Source requirement according to IEC60950-1. Please note that the power supply requirement is subject to the device label.
- Connect the device (I-type structure) to the power socket with protective earthing.
- The appliance coupler is a disconnection device. When using the coupler, keep the angle for easy operation.

## General

This Quick Start Guide (hereinafter referred to as “Guide”) introduces the installation and basic operation of the Time & Attendance (Standalone) (hereinafter referred to as “standalone”).

## Safety Instructions

The following categorized signal words with defined meaning might appear in the Guide.

Signal Words	Meaning
 <b>NOTE</b>	Provides additional information as the emphasis and supplement to the text.

## Privacy Protection Notice

As the device user or data controller, you might collect personal data of other such as face, fingerprints, car plate number, Email address, phone number, GPS and so on. You need to be in compliance with the local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures include but not limited to: providing clear and visible identification to inform data subject the existence of surveillance area and providing related contact.

## About the Guide

- The Guide is for reference only. If there is inconsistency between the Guide and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the Guide.
- The Guide would be updated according to the latest laws and regulations of related regions. For detailed information, see the paper manual, CD-ROM, QR code or our official website. If there is inconsistency between paper manual and the electronic version, the electronic version shall prevail.
- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the Guide. Please contact the customer service for the latest program and supplementary documentation.
- There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, please refer to our final explanation.
- Upgrade the reader software or try other mainstream reader software if the Guide (in PDF format) cannot be opened.
- All trademarks, registered trademarks and the company names in the Guide are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurred when using the device.

- If there is any uncertainty or controversy, please refer to our final explanation.

# Table of Contents

<b>Important Safeguards and Warnings .....</b>	<b>II</b>
<b>Foreword .....</b>	<b>III</b>
<b>1 Overview.....</b>	<b>1</b>
1.1 Introduction .....	1
1.2 Features .....	1
1.3 Appearance .....	1
1.4 Dimensions .....	3
<b>2 Installation.....</b>	<b>4</b>
2.1 Installation Methods .....	4
2.2 Cable Connection .....	5
<b>3 Operation.....</b>	<b>6</b>
3.1 Notice .....	6
3.2 Main Menu .....	6
3.3 Configure Network Parameters .....	7
3.4 Add Users.....	8
3.4.1 Add One by One .....	8
3.4.2 Add in Batches.....	9
3.5 Shift .....	10
3.5.1 Shift Setting .....	10
3.5.2 Schedule Setting.....	11
3.5.3 Late-in/Early-out Allowed.....	12
3.6 Attendance .....	13
3.6.1 Auto/Manual.....	13
3.6.2 Fixed .....	13
3.6.3 Forced.....	13
3.7 Attendance Statistics.....	14
<b>Appendix 1 Cybersecurity Recommendations .....</b>	<b>15</b>

## 1.1 Introduction

The Time & Attendance (Standalone) can be used to check attendance. The attendance check can be completed through three methods: fingerprint, password, and card.

## 1.2 Features

- High capacity standby battery works for upto 10 hours in the standby mode.
- Can be connected to the third party access control device.
- 1, 000 user information (ID, name, fingerprint, password, card number) can be recorded on the time & attendance (standalone).
- Stores up to 100, 000 attendance record reports and 10, 000 management records.
- All users can query their own attendance records.
- Only administrators can add new users, edit user information, query, import or export attendance logs and attendance reports.
- USB disk update firmware.
- T9 text input.
- 24 groups of shift.
- 20 departments.

## 1.3 Appearance

Figure 1-1 Appearance



Table 1-1 Key description

Icon	Description
0-9	Number keys for number and letter input.


Icon	Description
<b>ESC/F1</b>	<ul style="list-style-type: none"> <li>Press the key to exit or go to the previous menu.</li> <li>On the standby interface, press the button to check in.</li> </ul>
<b>^/F2</b>	<ul style="list-style-type: none"> <li>In the standby mode, press the key, BREAK OUT will be displayed on the screen.</li> <li>Up (direction key; attendance type switch).</li> </ul>
<b>∨/F3</b>	<ul style="list-style-type: none"> <li>In the standby mode, press the key, BREAK IN will be displayed on the screen.</li> <li>Down (direction key; attendance type switch).</li> </ul>
<b>OK/F4</b>	<ul style="list-style-type: none"> <li>Enter or confirm.</li> <li>On the standby interface, press the key to check out.</li> </ul>
<b>#</b>	Delete key or shortcut key for reviewing records.
	<ul style="list-style-type: none"> <li>When the terminal is off/on, press the key to turn the terminal on/off (press the key for over three seconds to turn the terminal off).</li> <li>On the standby mode, press the key, and then administrators can go to the main menu by fingerprints, passwords, or cards.</li> <li>When you need to enter text, press the key, and then you can switch text input types (numbers, letters and punctuation).</li> </ul>

Figure 1-2 Rear panel

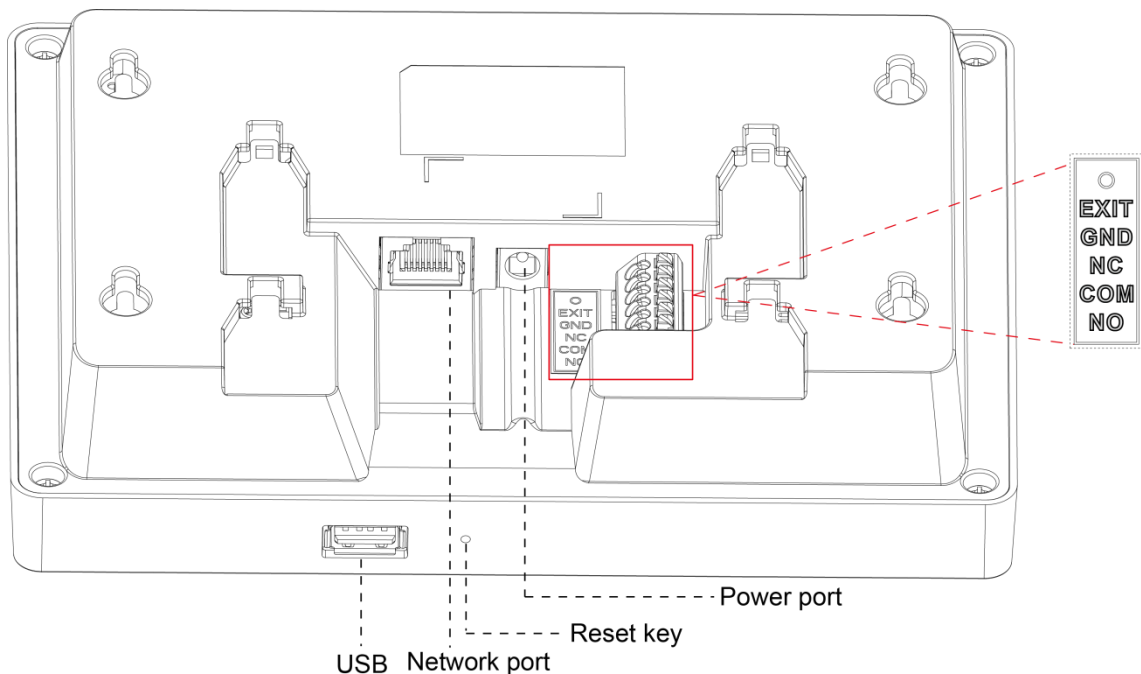


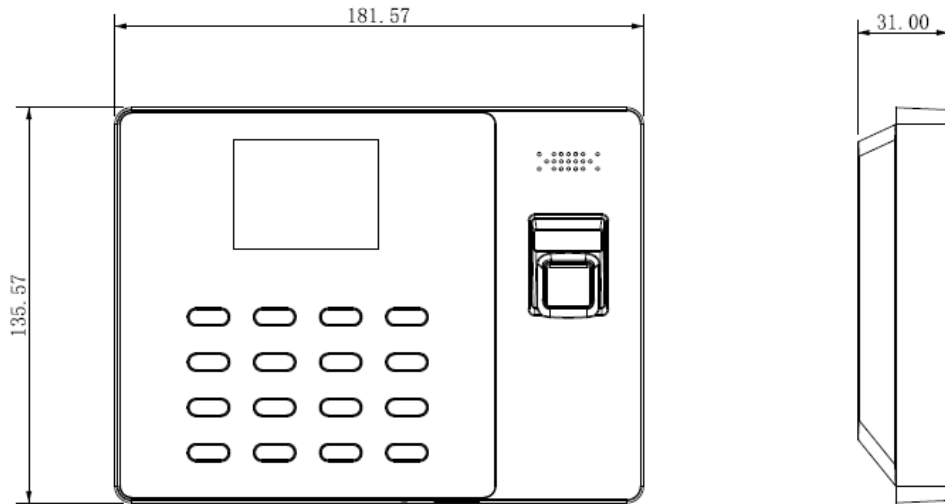
Table 1-2 Port description

Port	Description
<b>EXIT</b>	Connected to the door exit button.
<b>GND</b>	Connected to the ground line.
<b>NC</b>	Makes the relay normally closed.

Port	Description
COM	COM port.
NO	Makes the relay normally on.

## 1.4 Dimensions

Figure 1-3 Dimensions (mm)

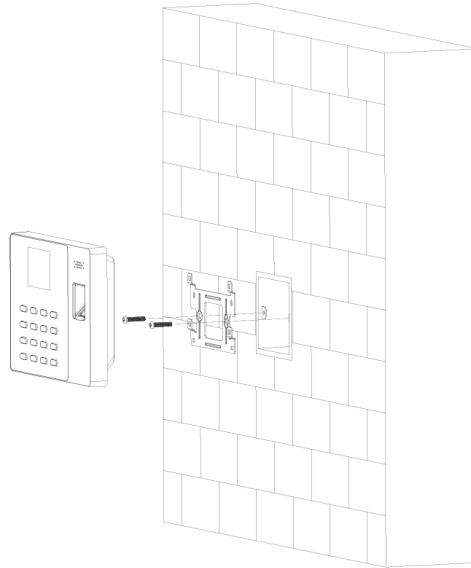




## 2.1 Installation Methods

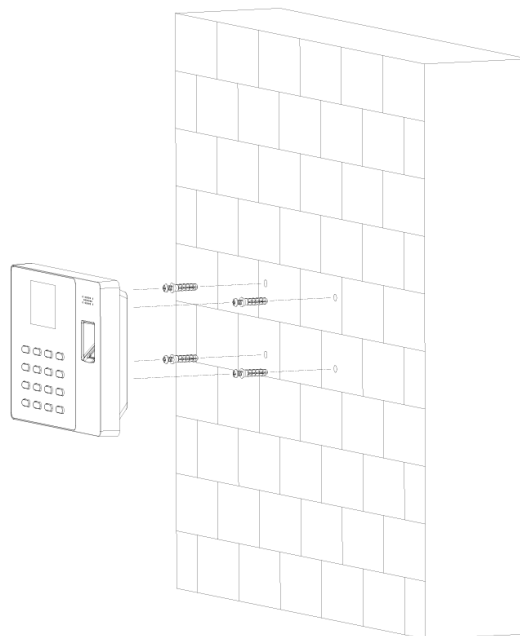
Installed through 86 electrical box

Figure 2-1 Installed through 86 electrical box



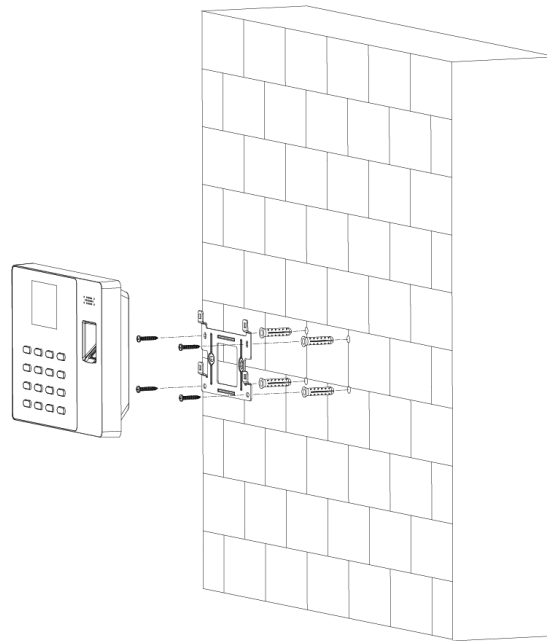
Directly installed on the wall

Figure 2-2 Directly installed on the wall



Installed through bracket

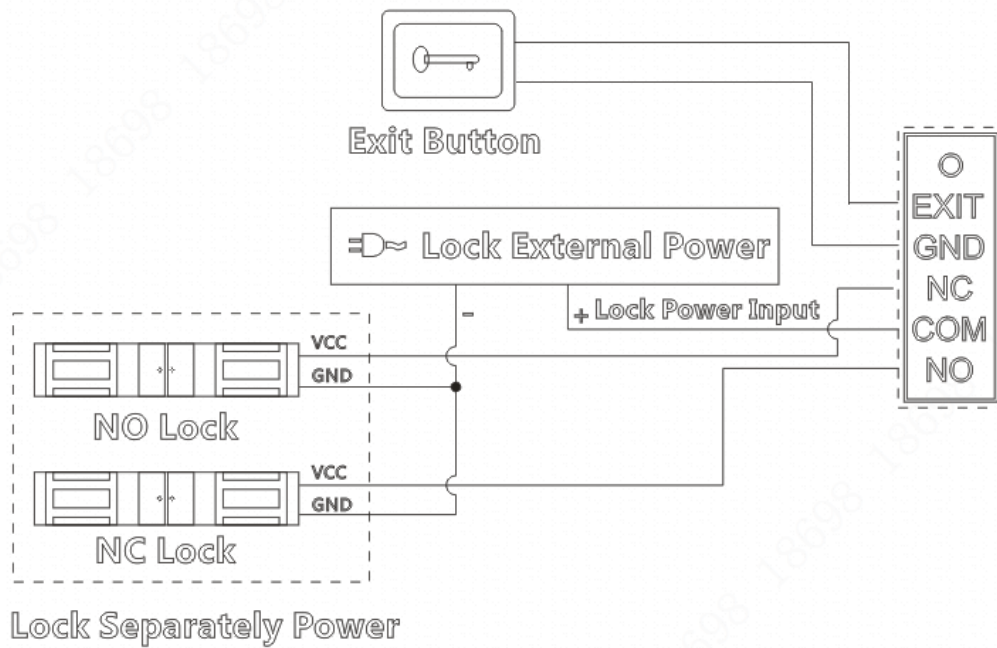
Figure 2-3 Installed through bracket



## 2.2 Cable Connection

The terminal can be connected to exit button to control the door. See Figure 2-4.

Figure 2-4 Cable connection



## 3.1 Notice


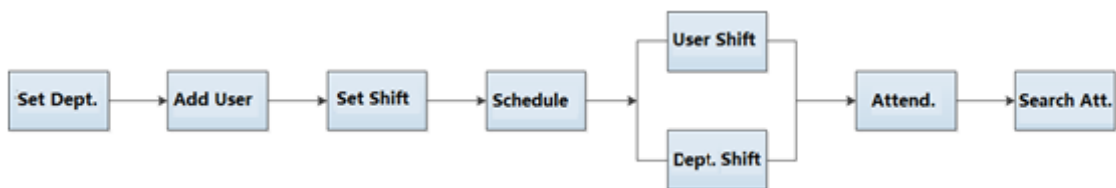
- When the terminal is connected to the power source, you need to press  to turn it on.
- Before an administrator is created, anyone can enter the main menu and do settings for the terminal. For the sake of information security, you need to create administrators first (Select **1 User > Add New User**, and then select a user ID. Select **User Level**, press **OK/F4** and then **^/F2** or **∨/F3** to select **Administrator**.).
- When you need to connect the terminal to SmartPSS (the management platform), the default ID is “admin” and the default password is also “admin”.
- Settings about shifts, schedules, and departments in the terminal are independent of those on SmartPSS.
- For standalone system framework, see Figure 3-1.

Figure 3-1

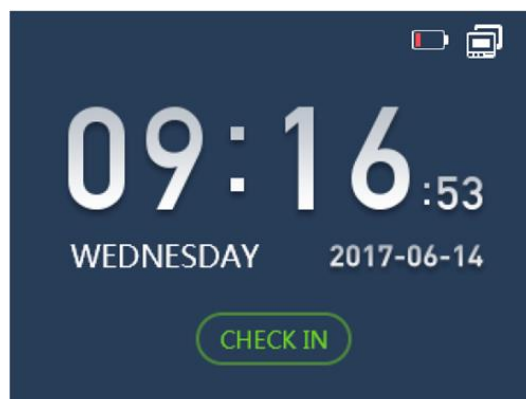


## 3.2 Main Menu




### Standby mode

Before enter the main page, the interface below is displayed. See Figure 3-2.

Figure 3-2 Standby interface





- Before administrators are created, anyone can enter the main menu and do settings. Once administrators are created, only administrators can enter the main menu.
-  indicates that the network is disconnected.
-  indicates that the network is connected.
-  indicates the battery level and network connection condition. When you turn the terminal on for the first time, the battery level is 25% (can last for about one hour). As time goes by the battery life reduces.

## Main menu


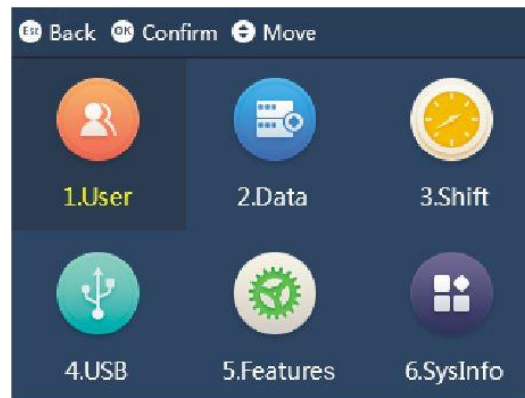

Press , and then the main menu will be displayed. See Figure 3-3.

Figure 3-3 Main menu



- After you have created administrators, you need to press  first, and then you can go to the main menu by the following methods:
  - ◇ Press your finger tip at the fingerprint sensor;
  - ◇ Enter the administrator's user ID and password;
  - ◇ Swipe your card at the card reader.
- You can select icon by the following two methods:
  - ◇ Press  $\wedge/F2$  or  $\vee/F3$ ;
  - ◇ Press number keys.

## 3.3 Configure Network Parameters

On the main menu, select **5 Feature > Communication**, and then you can configure IP address, mask, gateway, MAC, and port. See Figure 3-4.

Figure 3-4 Communication

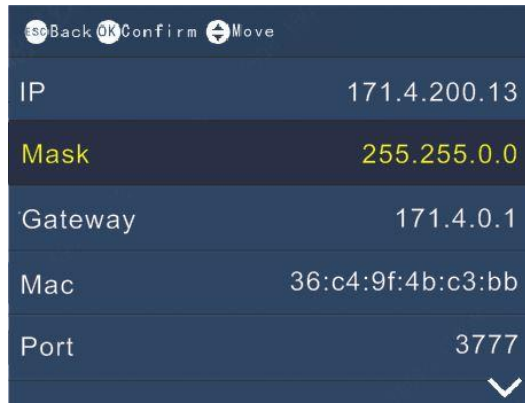


Table 3-1 Standby interface description

Parameter	Description
IP	Default value 192.168.1.108, you can configure it according to your needs.
Mask	Default value 255.255.255.0, you can configure it according to your needs.
Gateway	Default value 192.168.1.1, you can configure it according to your needs.
MAC	MAC address of the terminal and it cannot be modified.
Port	Port number, used to login the terminal on the SmartPSS.

## 3.4 Add Users

You can add users one by one or you can add users in batches.

### 3.4.1 Add One by One

Step 1 On the main menu, select **1 User > Add New User**. See Figure 3-5 and Figure 3-6.

Figure 3-5 Adding new user (1)

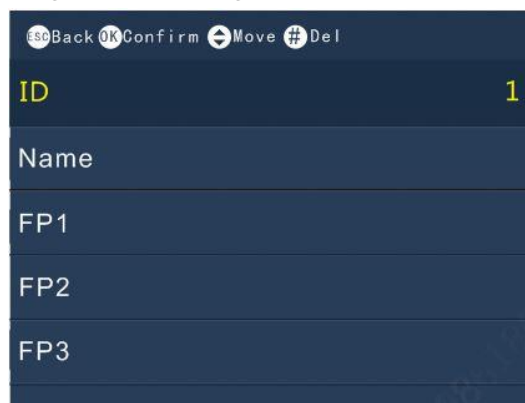
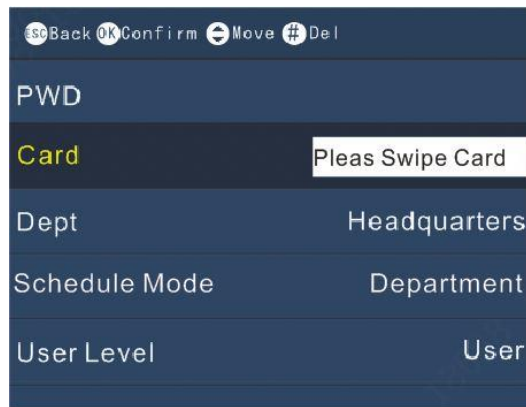


Figure 3-6 Adding new user (2)



Back Confirm Move Del	
PWD	
Card	Please Swipe Card
Dept	Headquarters
Schedule Mode	Department
User Level	User

**Step 2** Do the following operations:

- 1) Enter user ID and name;
- 2) Record user's fingerprints;
- 3) Let users set a password;
- 4) Register a card for the new user;
- 5) Select a department;
- 6) Select a schedule mode;
- 7) Select a user level.

A new user is added.



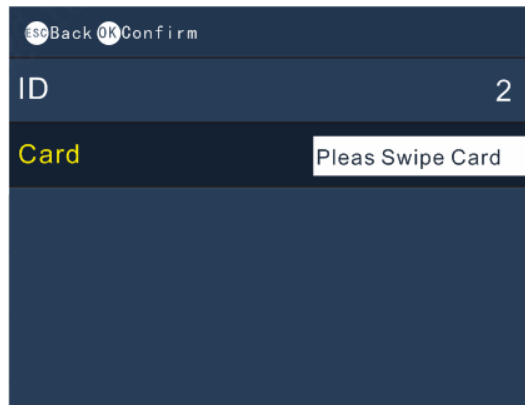
- Maximum user ID length is 8 digits (the user ID length range can be 1–99999999).
- Maximum user name length is 16 letters.
- Passwords can be numbers of 1–8 digits (Zero alone cannot be set as password and cannot be the first number of a password.).
- At most three fingerprints can be recorded for one user.

## 3.4.2 Add in Batches

### Add users by swiping cards

Select **1 User > Add Cards in Batch**, swipe cards at the card reader, and then user ID, and card number will be automatically saved. You need to edit user names, add fingerprints and passwords separately. See Figure 3-7.

Figure 3-7 Swipe cards to add users



## Add users through USB

You can export user information (including user ID, user name, password, card number, department, user level and schedule mode) from one terminal to another terminal. The exported information will be stored in an excel chart. You can edit information in the chart. When imported to other terminals, user information with the same User ID will be overwritten.

**Step 1** On the main menu, select **4 USB > Import User Info**.

The prompt **New info will cover the before one** will be displayed.

**Step 2** Press **Confirm-OK**.

And then user information will be imported.



When storage space of the USB is less than 1M, files can be exported but might be corrupted.

## 3.5 Shift

You can set shift periods. There are 24 shifts in total.

### 3.5.1 Shift Setting

On the main menu, select **3 Shift > Shift Setting > Shift**. You can set 24 shifts at most. See Figure 3-8.

Figure 3-8 Shift setting

Shift NO	DutyT1	DutyT2	Overtime Session
1	08 : 30 - 12 : 00		
2			
3	13 : 30 - 17 : 00		
4			
5			
6	20 : 00 - 21 : 00		

Table 3-2 Shift setting description

Duty	Description
Duty T1	You can set duration for duty time in each shift. For example 08:30–12:00.
Duty T2	You can set duration for duty time in each shift. For example 13:30–17:00.
Overtime Session	You can set overtime duration. For example 20:00–21:00.



- There are two periods in which you may need to sign in and sign out, because there is an interval between Duty T1 and Duty T2.
- If you signed in for more than once, the system takes the earliest sign in records as effective; if you signed out for more than once, the system only takes the latest sign out records as effective.
- In Overtime Session, there is no late/early leave time setup.

## Import/Export shift

Once you have done shift settings on a terminal, you can export the settings through flash drives and then import them to other terminals, thus you do not need to do settings repeatedly.

## 3.5.2 Schedule Setting

On the main menu, select **3 Shift > Schedule Setup**, and then you can set schedule in each month (only the current month and the next month) for users and set schedules in each week for departments.

### User Schedule

**Step 1** On the main menu, select **Shift > Schedule Setting > User Schedule**.

**Step 2** Press **OK/F4**.

**Step 3** Enter the user ID.

User name and department name will be displayed automatically.

**Step 4** Press **OK/F4**.

See Figure 3-9.

Figure 3-9 User schedule

User:1 2017/6 schedules						
Sun	Mon	Tue	Wed	Thu	Fri	Sat
				1 1	2 1	3
4	5 1	6 1	7 1	8 1	9 1	10
11	12 1	13 1	14 1	15 1	16 1	17
18	19 1	20 1	21 1	22 1	23 1	24
25	26 1	27 1	28 1	29 1	30 1	





- Numbers at the center of each box are shift numbers. There are 24 shifts in total.
- Numbers at the top left corner of each box are days.
- Null and 0 means off duty.
- 25 means business trip.
- 26 means leave.

## Department Schedule

**Step 1** On the main menu, select **Shift > Schedule Setting > Department**.

**Step 2** Select a department.

**Step 3** Press **OK/F4**.

See Figure 3-10.

Figure 3-10 Department schedule

The screenshot shows a terminal interface with a dark blue background. At the top, there are navigation buttons: 'Esc Back', 'OK Confirm', '← Move', and '# Del'. Below these is the title 'Dept:Product schedules'. Underneath is a table with columns for the days of the week: Sun, Mon, Tue, Wed, Thu, Fri, and Sat. The 'Sun' column is highlighted in blue. The 'Mon' through 'Fri' columns each contain the number '1'. The 'Sat' column is empty.

Sun	Mon	Tue	Wed	Thu	Fri	Sat
	1	1	1	1	1	

## Import/Export Schedule



- Before you export or import schedules, make sure the USB is inserted. During exporting or importing, do not remove the USB or operate the terminal, otherwise exporting or importing will fail and system malfunction will occur.
- Once you have done schedule settings on a terminal, you can export the settings through flash drives and then import them to other terminals, thus you do not need to do settings repeatedly.

### 3.5.3 Late-in/Early-out Allowed

Late-in Allowed is used to set flexible working hours. For example the permitted start working time is 8:30, and the late time is 5 minutes, then if a user gets his/her attendance checked before 8:35, he/she is not considered to be late.

Early-out Allowed is used to set flexible working hours, too. For example the permitted finishing working time is 17:30, and the early leave time is 5 minutes, then if a user gets his/her attendance checked after 17:25, he/she is not considered to have left early.



- During Duty 1 and Duty 2 period, you have only one chance to get your attendance checked late and one chance to leave early.
- If you arrive late or leave early within the time period permitted, overtime will still be counted.

## 3.6 Attendance

There are three attendance check mode: Auto/Manual, Fixed, and Forced; and three attendance check methods: fingerprint, password, and card.

### 3.6.1 Auto/Manual

In **Auto/Manual** mode, there are three methods:

- You can get your attendance checked directly by pressing your finger at the fingerprint sensor, by entering your user ID and password, or by swiping your card;



You need to do shift settings in advance in **3 Shift > Shift Setting > Shift**. See “3.5.1 Shift Setting”.

- You can select an attendance event by pressing **Esc/F1**, **^/F2**, **∨/F3**, and **OK/F4**, and then do fingerprint, password, or card attendance check;
- You can get your attendance recorded without doing shift settings and without selecting attendance events.

### 3.6.2 Fixed

In the Fixed mode, you can select a fixed attendance event for a terminal, and then users can sign in at one terminal and sign out at another terminal.

**Step 1** On the standby interface, select **5 Feature > Features > Att. Event Mode**.

**Step 2** Press **OK/F4**.

The white text box appears.

**Step 3** Press **^/F2** or **∨/F3** to select Fixed.

**Step 4** Press **OK/F4**.

**Step 5** Press **∨/F3**.

**Step 6** Press **OK/F4**.

The white text box appears.

**Step 7** Press **^/F2** or **∨/F3** to select among Check in, Break out, Break in, Check out, OT-In, and OT-Out.

### 3.6.3 Forced

In the Forced mode, you need to select your attendance type (1.Check in; 2.Break out; 3.Break in; 4.Check out; 5.OT-In; 6.OT-Out) after you press your finger tip at the fingerprint sensor, enter your user ID and password, or swiping your card.

**Step 1** On the standby interface, select **5 Feature > Features > Att. Event Mode**.

Step 2 Press **OK/F4**.

The white text box appears.

Step 3 Press **^/F2** or **∨/F3** to select Forced.

Step 4 Press **OK/F4**.



Press **^/F2** or **∨/F3** continuously, **BREAK OUT, CHECK IN, OT-OUT, OT-IN, CHECK OUT, BREAK IN** will be displayed in turn. There are shortcut keys for check-in, check-out, break-in, and break-out.

- ◇ **Esc/F1**: Press **Esc/F1**, **CHECK IN** will be displayed on the screen, and then you can check-in by fingerprint, password, or card.
- ◇ **^/F2**: Press **^/F2**, **BREAK OUT** will be displayed on the screen, and then you can make an attendance when you need to go out during work time by fingerprint, password, or card.
- ◇ **∨/F3**: Press **∨/F3**, **BREAK IN** will be displayed on the screen, and then you can make an attendance when you return to the company during the work time by fingerprint, password, or card.
- ◇ **OK/F4**: Press **OK/F4**, **CHECK OUT** will be displayed on the screen, and then you can check out by fingerprint, password, or card.
- ◇ **OT-IN**: you can make an attendance record before you need to work overtime.
- ◇ **OT-OUT**: You can make an attendance record after you have worked overtime.

## 3.7 Attendance Statistics



Before you export attendance record, make sure the USB is inserted. During exporting, do not remove the USB or operate the standalone, otherwise the exporting will fail and system malfunction will occur.

You can query and export attendance record.

On the main menu, select **2 Data > Export Monthly ATT. log/Export Monthly ATT. Report**, press **OK/F4**, select a month, and then press **OK/F4** to export logs and reports.

# Appendix 1 Cybersecurity Recommendations

Cybersecurity is more than just a buzzword: it's something that pertains to every device that is connected to the internet. IP video surveillance is not immune to cyber risks, but taking basic steps toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations from Dahua on how to create a more secured security system.

## **Mandatory actions to be taken for basic equipment network security:**

### **1. Use Strong Passwords**

Please refer to the following suggestions to set passwords:

- The length should not be less than 8 characters;
- Include at least two types of characters; character types include upper and lower case letters, numbers and symbols;
- Do not contain the account name or the account name in reverse order;
- Do not use continuous characters, such as 123, abc, etc.;
- Do not use overlapped characters, such as 111, aaa, etc.;

### **2. Update Firmware and Client Software in Time**

- According to the standard procedure in Tech-industry, we recommend to keep your equipment (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the equipment is connected to the public network, it is recommended to enable the "auto-check for updates" function to obtain timely information of firmware updates released by the manufacturer.
- We suggest that you download and use the latest version of client software.

## **"Nice to have" recommendations to improve your equipment network security:**

### **1. Physical Protection**

We suggest that you perform physical protection to equipment, especially storage devices. For example, place the equipment in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable equipment (such as USB flash disk, serial port), etc.

### **2. Change Passwords Regularly**

We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

### **3. Set and Update Passwords Reset Information Timely**

The equipment supports password reset function. Please set up related information for password reset in time, including the end user's mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

### **4. Enable Account Lock**

The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

## **5. Change Default HTTP and Other Service Ports**

We suggest you to change default HTTP and other service ports into any set of numbers between 1024~65535, reducing the risk of outsiders being able to guess which ports you are using.

## **6. Enable HTTPS**

We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

## **7. Enable Whitelist**

We suggest you to enable whitelist function to prevent everyone, except those with specified IP addresses, from accessing the system. Therefore, please be sure to add your computer's IP address and the accompanying equipment's IP address to the whitelist.

## **8. MAC Address Binding**

We recommend you to bind the IP and MAC address of the gateway to the equipment, thus reducing the risk of ARP spoofing.

## **9. Assign Accounts and Privileges Reasonably**

According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

## **10. Disable Unnecessary Services and Choose Secure Modes**

If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.

If necessary, it is highly recommended that you use safe modes, including but not limited to the following services:

- SNMP: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
- SMTP: Choose TLS to access mailbox server.
- FTP: Choose SFTP, and set up strong passwords.
- AP hotspot: Choose WPA2-PSK encryption mode, and set up strong passwords.

## **11. Audio and Video Encrypted Transmission**

If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

Reminder: encrypted transmission will cause some loss in transmission efficiency.

## **12. Secure Auditing**

- Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
- Check equipment log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

## **13. Network Log**

Due to the limited storage capacity of the equipment, the stored log is limited. If you need to save the log for a long time, it is recommended that you enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

## **14. Construct a Safe Network Environment**

In order to better ensure the safety of equipment and reduce potential cyber risks, we recommend:

- Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.

- The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
- Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.