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 dissemble 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.

Foreword

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
📖**NOTE**	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

1 Overview

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 upto10 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

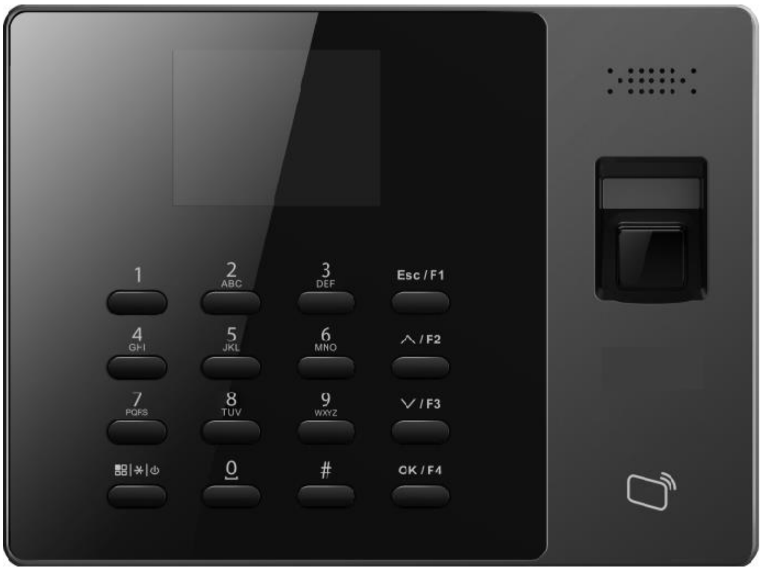


Table 1-1 Key description

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

Icon	Description
ESC/F1	● Press the key to exit or go to the previous menu. ● On the standby interface, press the button to check in.
∧/F2	● In the standby mode, press the key, BREAK OUT will be displayed on the screen. ● Up (direction key; attendance type switch).
∨/F3	● In the standby mode, press the key, BREAK IN will be displayed on the screen. ● Down (direction key; attendance type switch).
OK/F4	● Enter or confirm. ● On the standby interface, press the key to check out.
#	Delete key or shortcut key for reviewing records.
▦|✱|⏻	● 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). ● On the standby mode, press the key, and then administrators can go to the main menu by fingerprints, passwords, or cards. ● When you need to enter text, press the key, and then you can switch text input types (numbers, letters and punctuation).

Figure 1-2 Rear panel

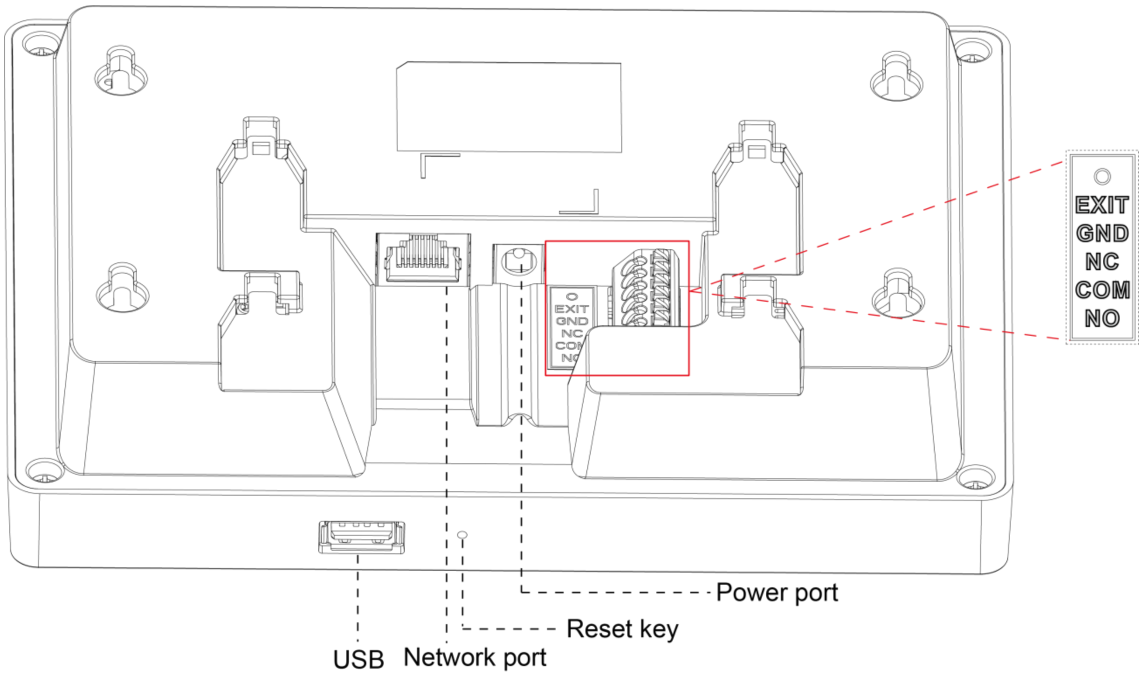


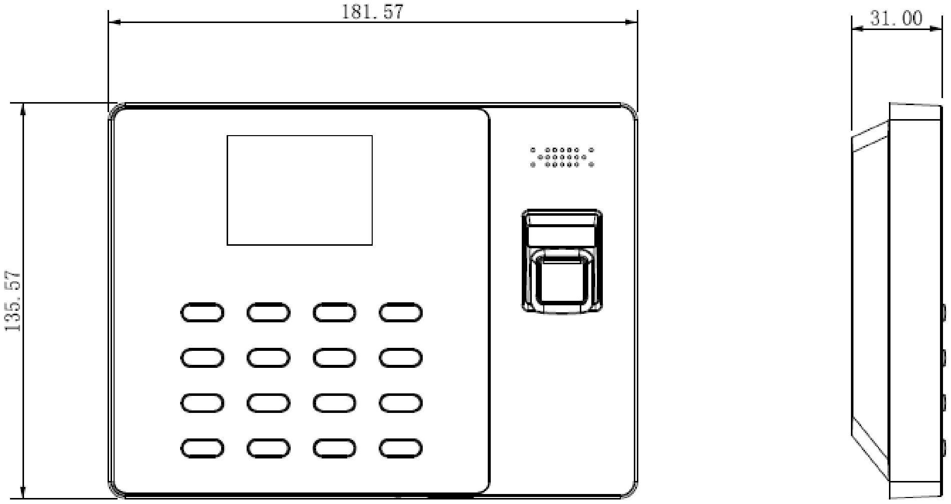
Table 1-2 Port description

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

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

1.4 Dimensions

Figure 1-3 Dimensions (mm)

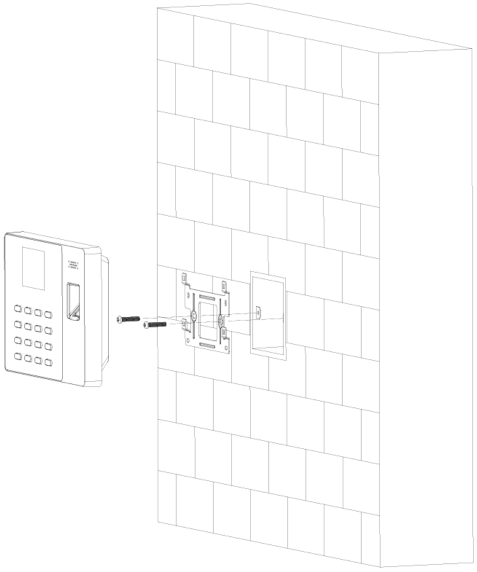


2 Installation

2.1 Installation Methods

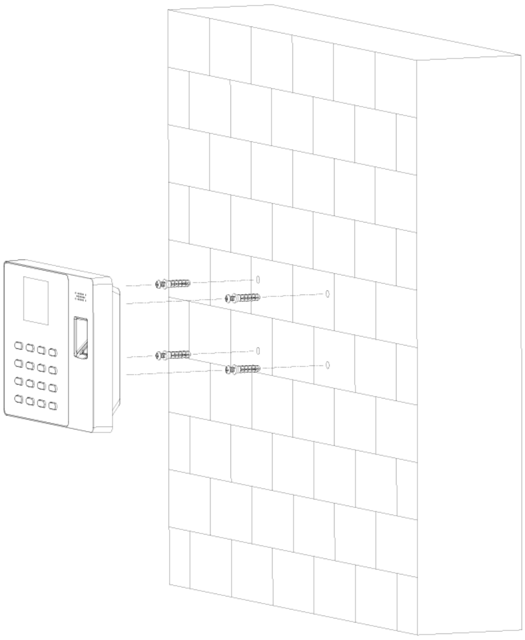
Installed through 86 electrical box

Figure 2-1 Installed through 86 electrical box



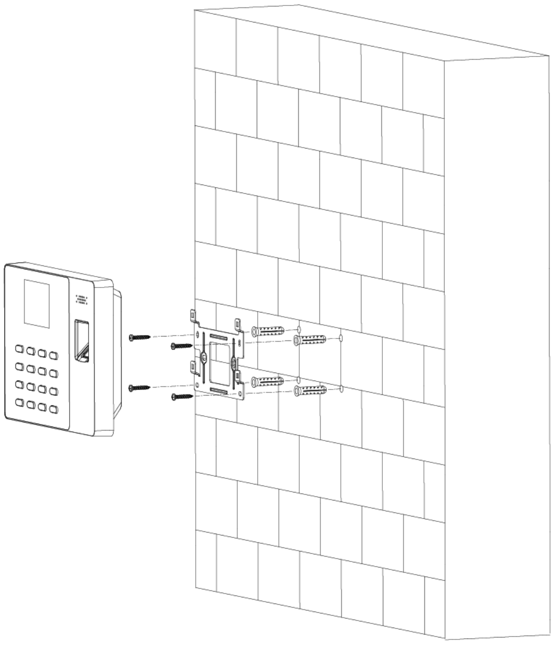
Directly installed on the wall

Figure 2-2 Directly installed on the wall



Installed through bracket

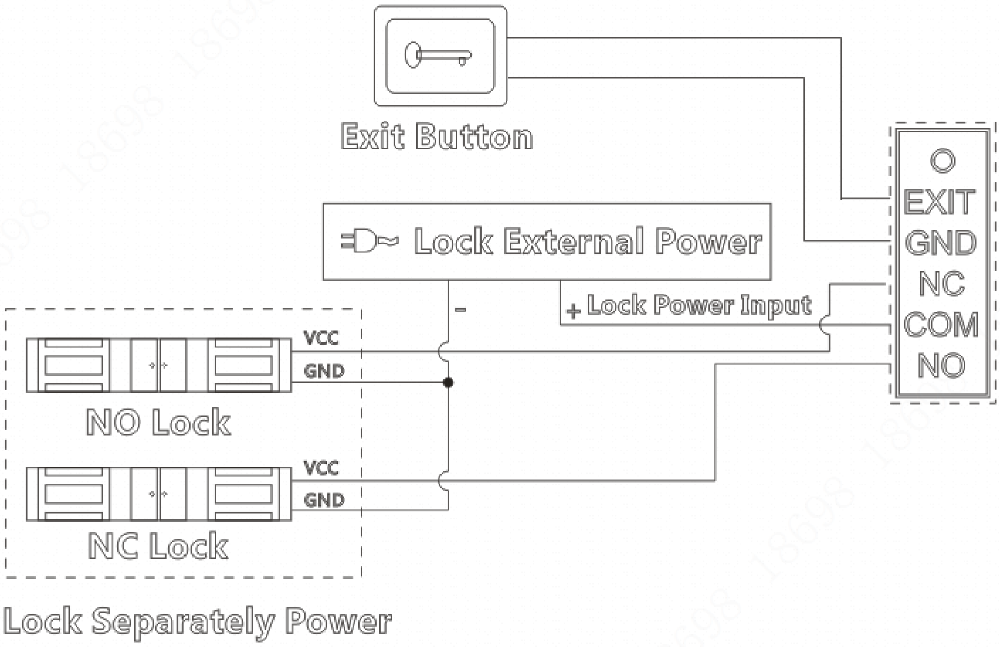
Figure 2-3 Installed through bracket



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

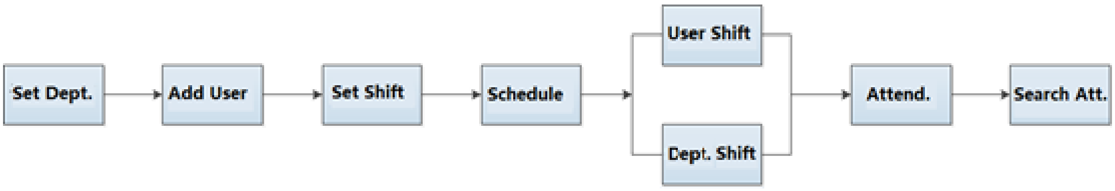


3 Operation

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

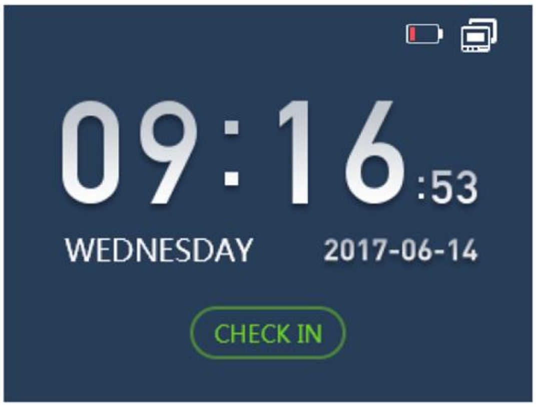


3.2 Main Menu

Standby mode

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

Figure 3-2 Standby interface

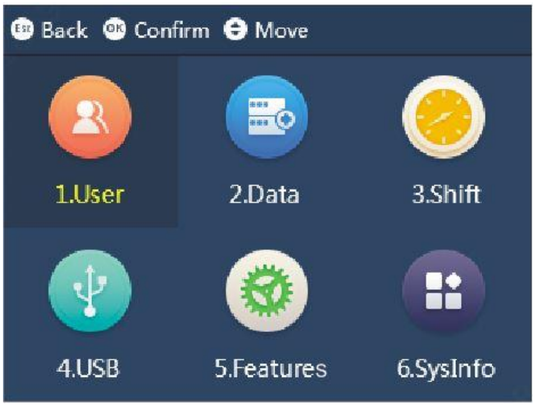


- Before administrators are created, anyone can enter the main menu and do settings. Once administrators are created, only administrators can enter the main menu.
- 🖧 indicates that the network is disconnected.
- 🖧 indicates that the network is connected.
- 🔋 🖧 indicates the battery level and network 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

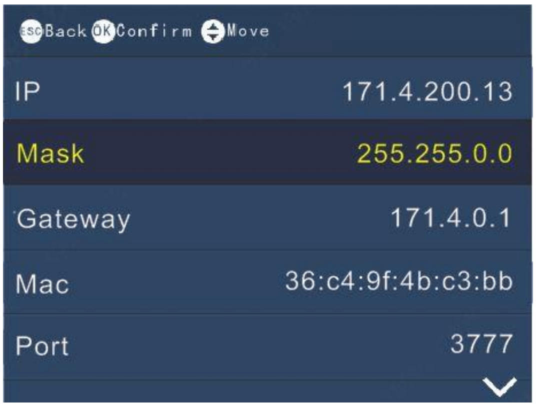


- After you have created administrators, you need to press ⊞|✱|⏻ first, and then you can go to the main menu by the following methods:
  - ◇ Press your finger tip at the fingerprint sensor;
  - ◇ Enter the administrator’s user ID and password;
  - ◇ Swipe your card at the card reader.
- You can select icon by the following two methods:
  - ◇ Press ∧/**F2** or ∨/**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



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 3-1 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.

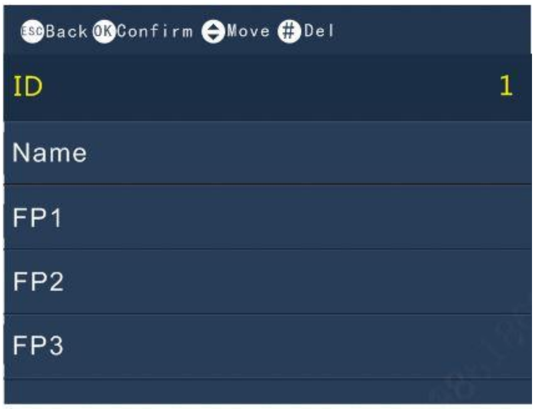
3.4 Add Users

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)



ID 1

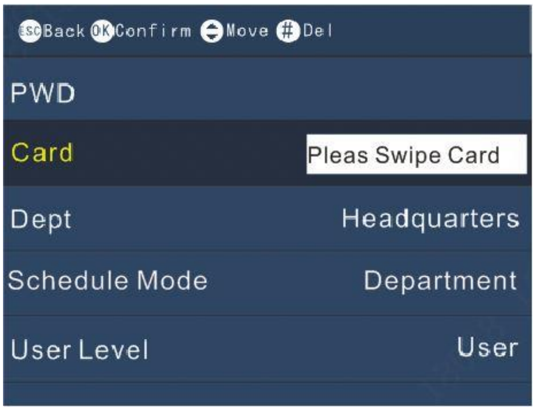
Name

FP1

FP2

FP3

Figure 3-6 Adding new user (2)



PWD

Card Pleas 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.

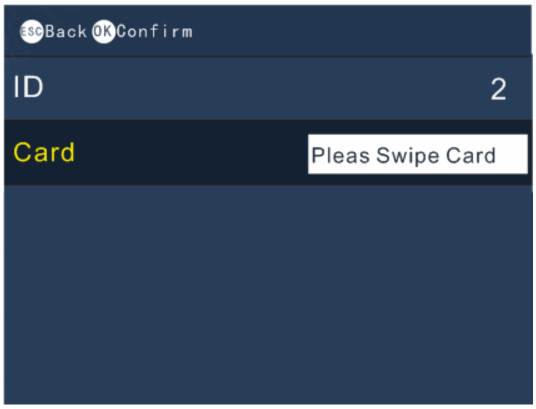
- Maximum user ID length is 8 digits (the user ID length range can be 1–99999999).
- Maximum user name length is 16 letters.
- Passwords can be numbers of 1–8 digits (Zero alone cannot be set as password and cannot be the first number of a password.).
- At most three fingerprints can be recorded for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



ID 2

Card Pleas Swipe Card

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.

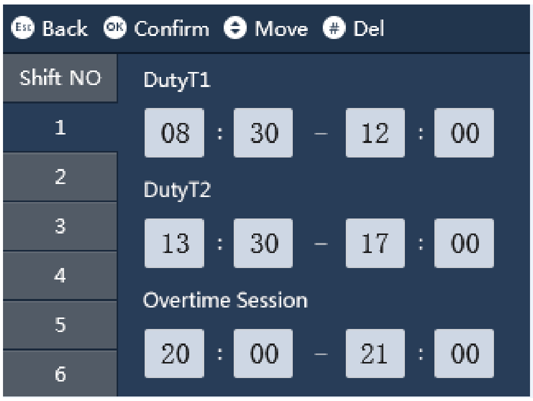
3.5 Shift

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



DutyT1
08 : 30 – 12 : 00

DutyT2
13 : 30 – 17 : 00

Overtime Session
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**.

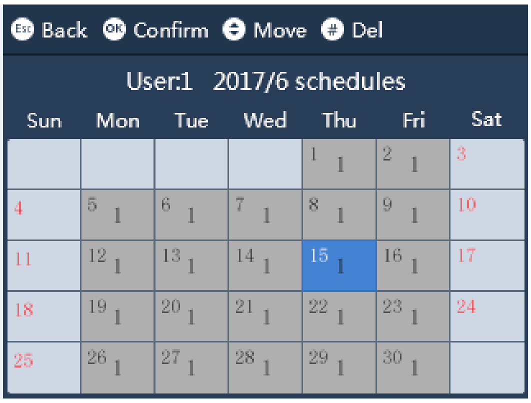
Step 3 Enter the user ID.

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

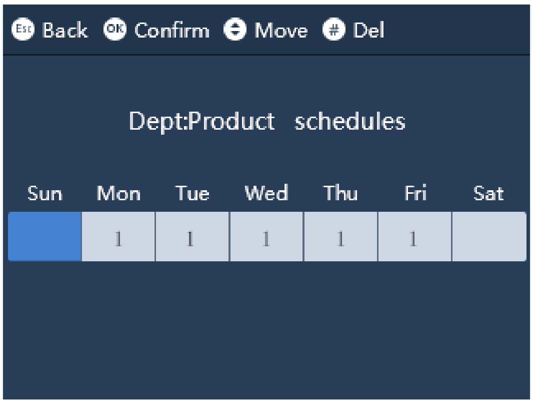
Step 1 On the main menu, select **Shift > Schedule Setting > Department**.

Step 2 Select a department.

Step 3 Press **OK/F4**.

See Figure 3-10.

Figure 3-10 Department schedule



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.

3.5.3 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.