Face Recognition Time & Attendance

User's Manual



V1.0.0

Foreword

General

This manual introduces the functions and operations of the Face Recognition Time & Attendance (hereinafter referred to as the "Time & Attendance"). Read carefully before using the device, and keep the manual safe for future reference.

Safety Instructions

The following signal words might appear in the manual.

Signal Words	Meaning
DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, reductions in performance, or unpredictable results.
TIPS	Provides methods to help you solve a problem or save time.
NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.0	First Release.	June 2022

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, fingerprints, and license plate number. You need to be in compliance with your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures which include but are not limited: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.
- All designs and software are subject to change without prior written notice. Product updates

might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.

- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of 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 company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

This section introduces content covering the proper handling of the Time & Attendance, hazard prevention, and prevention of property damage. Read carefully before using the Time & Attendance, and comply with the guidelines when using it.

Transportation Requirement



Transport, use and store the Time & Attendance under allowed humidity and temperature conditions.

Storage Requirement



Store the Time & Attendance under allowed humidity and temperature conditions.

Installation Requirements

 **WARNING**

- Do not connect the power adapter to the Time & Attendance while the adapter is powered on.
- Strictly comply with the local electric safety code and standards. Make sure the ambient voltage is stable and meets the power supply requirements of the Time & Attendance.
- Do not connect the Time & Attendance to two or more kinds of power supplies, to avoid damage to the Time & Attendance.
- Improper use of the battery might result in a fire or explosion.



- Personnel working at heights must take all necessary measures to ensure personal safety including wearing a helmet and safety belts.
- Do not place the Time & Attendance in a place exposed to sunlight or near heat sources.
- Keep the Time & Attendance away from dampness, dust, and soot.
- Install the Time & Attendance on a stable surface to prevent it from falling.
- Install the Time & Attendance in a well-ventilated place, and do not block its ventilation.
- Use an adapter or cabinet power supply provided by the manufacturer.
- Use the power cords that are recommended for the region and conform to the rated power specifications.
- The power supply must conform to the requirements of ES1 in IEC 62368-1 standard and be no higher than PS2. Please note that the power supply requirements are subject to the Time & Attendance label.
- The Time & Attendance is a class I electrical appliance. Make sure that the power supply of the Time & Attendance is connected to a power socket with protective earthing.

Operation Requirements



- Check whether the power supply is correct before use.

- Do not unplug the power cord on the side of the Time & Attendance while the adapter is powered on.
- Operate the Time & Attendance within the rated range of power input and output.
- Use the Time & Attendance under allowed humidity and temperature conditions.
- Do not drop or splash liquid onto the Time & Attendance, and make sure that there is no object filled with liquid on the Time & Attendance to prevent liquid from flowing into it.
- Do not disassemble the Time & Attendance without professional instruction.
- This product is professional equipment.

Table of Contents

Foreword I

Important Safeguards and Warnings III

1 Overview 1

1.1 Introduction 1

1.2 Features 1

1.3 Application 1

2 Local Operations 3

2.1 Basic Configuration Procedure 3

2.2 Common Icons 3

2.3 Standby Screen 3

2.4 Initialization 4

2.5 Logging In 4

2.6 Network Communication 5

2.6.1 Active Register 5

2.6.2 Configuring Wi-Fi 6

2.7 User Management 6

2.7.1 Adding New Users 6

2.7.2 Viewing User Information 8

2.8 Attendance Management 8

2.8.1 Configuring Attendance Checking Modes 8

2.8.2 Configuring Shifts 9

2.8.3 (Optional) Configuring Holiday Plans 10

2.8.4 (Optional) Configuring Departments 11

2.8.5 Configuring Work Schedules 11

2.8.6 (Optional) Configuring Verification Interval Time 12

2.8.7 (Optional) Configuring Attendance Modes 13

2.9 System 15

2.9.1 Configuring Time 15

2.9.2 Configuring Face Parameters 16

2.9.3 Setting Volume 18

2.9.4 Screen Settings 18

2.9.5 Restoring Factory Defaults 18

2.9.6 Restart the Device 18

2.9.7 Configuring the Language 18

2.10 USB Management 19

2.10.1 Exporting to USB 19
2.10.2 Importing From USB 19
2.10.3 Updating System 20
2.11 Configuring Features 20
2.12 Viewing Attendance Logs 21
2.13 System Information 21
2.13.1 Viewing Data Capacity 22
2.13.2 Viewing Device Version 22
3 Web Operations 23
3.1 Initialization 23
3.2 Logging In 23
3.3 Resetting the Password 24
3.4 Data Capacity 25
3.5 Configuring Video and Image 26
3.5.1 Configuring Video 26
3.5.1.1 Configuring Channel 1 26
3.5.1.2 Configuring Channel 2 30
3.5.2 Setting Volume 32
3.6 Configuring Face Detection 32
3.7 Configuring Network 35
3.7.1 Configuring Port 35
3.7.2 Configuring Automatic Registration 36
3.8 Safety Management 36
3.8.1 Configuring IP Authority 36
3.8.1.1 Network Access 37
3.8.1.2 Prohibit PING 38
3.8.1.3 Anti Half Connection 38
3.8.2 Configuring System 38
3.8.2.1 Creating Server Certificate 40
3.8.2.2 Downloading Root Certificate 40
3.9 User Management 43
3.9.1 Adding Users 43
3.9.2 Adding ONVIF Users 44
3.9.3 Viewing Online Users 45
3.10 Maintenance 45
3.11 Configuration Management 46
3.11.1 Exporting/Importing Configuration Files 46
3.11.2 Restoring Factory Defaults 46

3.12 Upgrading System 47
3.12.1 File Update 47
3.12.2 Online Update 47
3.13 Viewing Version Information 47
3.14 Viewing Logs 47
3.14.1 System Logs 47
3.14.2 Admin Logs 48
3.14.3 Attendance Logs 48
4 Smart PSS Lite Configuration 49
4.1 Installing and Logging In 49
4.2 Adding Devices 49
4.2.1 Adding Individually 49
4.2.2 Adding in Batches 50
4.3 User Management 51
4.3.1 Configuring Card Type 51
4.3.2 Adding Users 52
4.3.2.1 Adding Individually 52
4.3.2.2 Adding in Batches 53
4.3.3 Assigning Attendance Permissions 54
Appendix 1 Important Points of Face Registration 57
Appendix 2 Cybersecurity Recommendations 60

1 Overview

1.1 Introduction

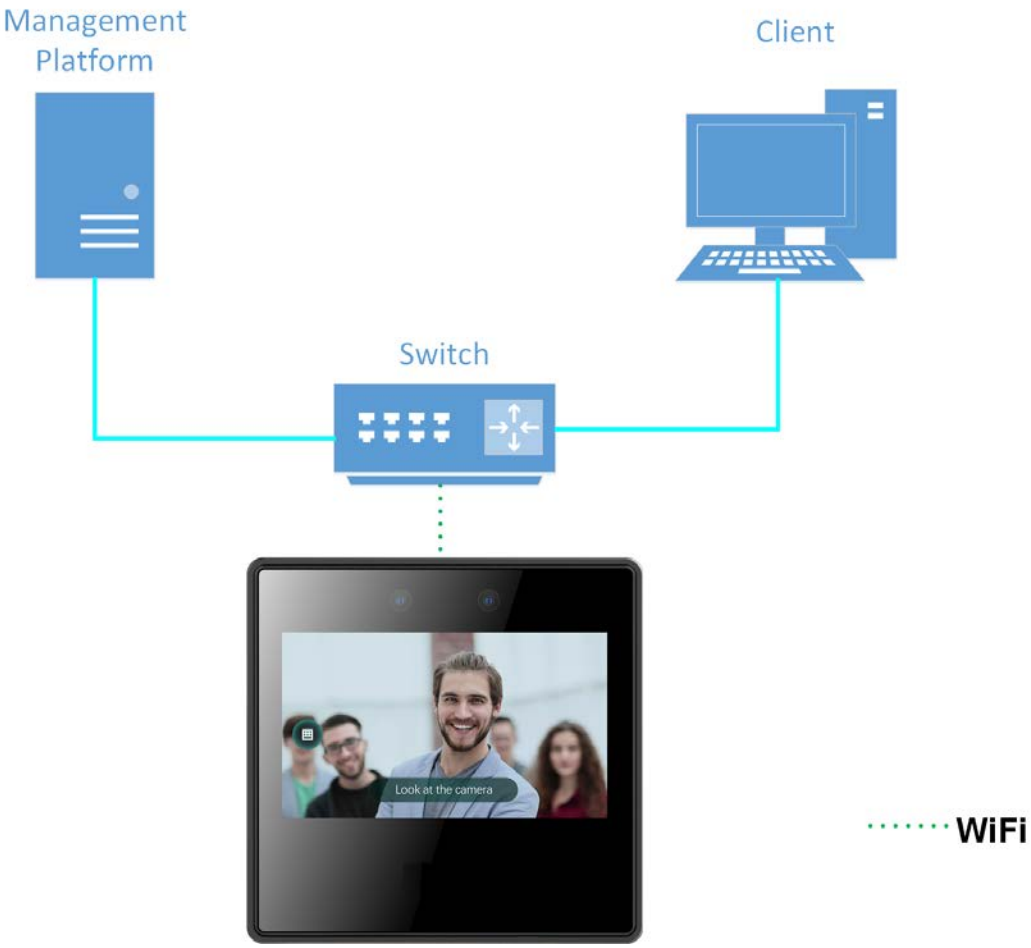
1.2 Features

- The housing is built of PC and ABS material, making it ideal for use indoors.
- 4.3 inch glass touch screen with a resolution of 480 × 272.
- 2-MP wide-angle dual-lens camera with IR illumination and DWDR.
- Supports mask detection.
- Verification Methods including face and password unlock.
- Recognizes faces 0.3 m to 1.5 m away (0.98 ft-4.92 ft), and detects persons between the height of 1.1 m and 2.0 m (3.61 ft-6.56 ft) when the camera is installed at 1.4 m (4.5 ft).
- Supports 2,000 users, 2,000 faces, 2,000 passwords, 50 administrators, and 300,000 records.
- Liveness detection has a face recognition accuracy rate of 99.9% and the 1:N comparison time is 0.2 s per person.
- Up to 128 periods and 128 holiday plans are configurable.
- Wi-Fi connection, auto registration, P2P registration, and DHCP.
- Supports customization of voice prompts.
- Online update and update through USB.
- Works while offline, and communicates with the management platform when connected to a network.
- Supports watchdog to protect the system from software and hardware failures.
- Supports SDK.
- Connects to SmartPSS Lite.

1.3 Application

It is widely used in parks, communities, business centers and factories, and ideal for places such as office buildings, government buildings, schools and stadiums.

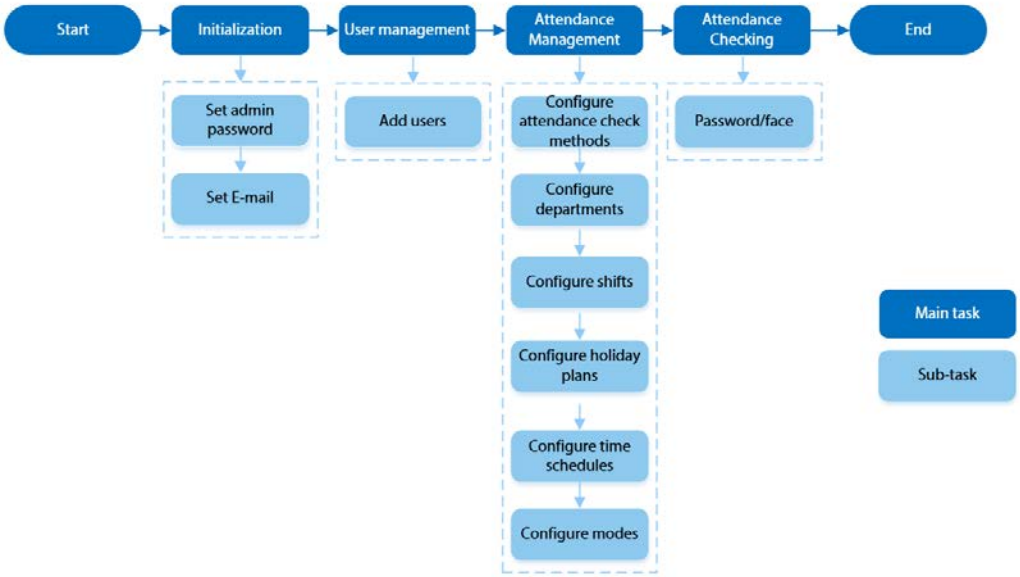
Figure 1-1 Networking



2 Local Operations

2.1 Basic Configuration Procedure

Figure 2-1 Basic configuration procedure



2.2 Common Icons

Table 2-1 Description of icons

Icon	Description
	Main menu icon.
	Confirm icon.
	Turn to the first page of the list.
	Turn to the last page of the list.
or	Turn to the previous page of the list.
or	Turn to the next page of the list.
	Return to the previous menu.
	Turned on.
	Turned off.
	Delete
	Search

2.3 Standby Screen

You can unlock the door through faces, passwords, and QR code. You can also make calls through

the intercom function.

- If there is no operation in 30 seconds, the Time & Attendance will go to the standby mode.
- This manual is for reference only. Slight differences might be found between the standby screen in this manual and the actual device.

Figure 2-2 Homepage

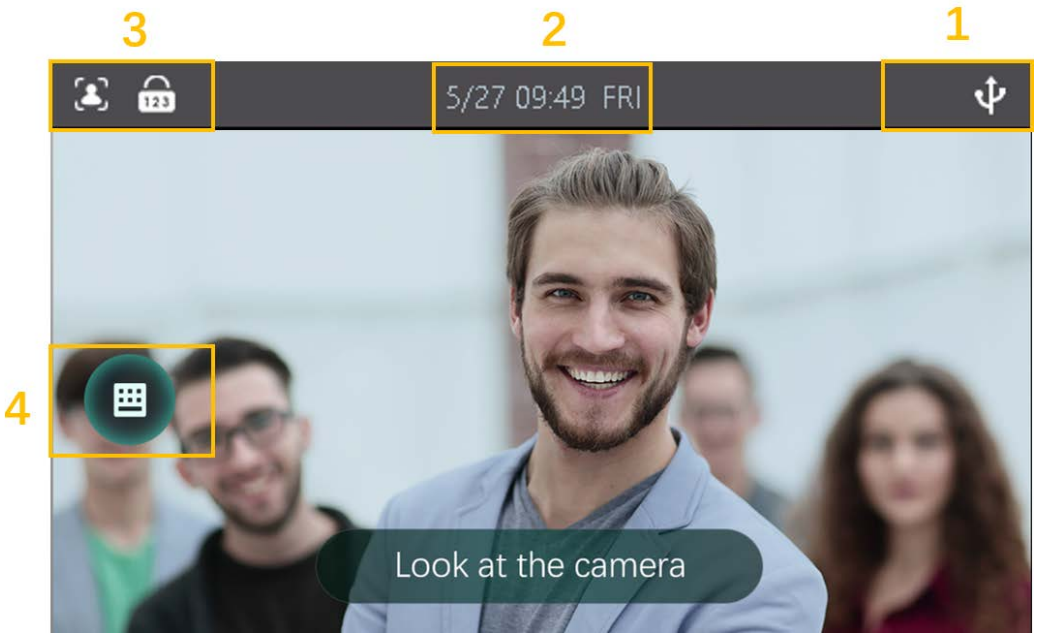


Table 2-2 Home screen description

No.	Name	Description
1	Status display	Displays status of Wi-Fi, network and USB, and more.
2	Date and time	Displays the current date and time.
3	Verification methods	Displays available verification methods.
4	Password	Enter user ID and password to punch in or punch out.

2.4 Initialization

For the first-time use or after restoring factory defaults, you need to select a language on Time & Attendance, and then set the password and email address for the admin account. You can use the admin account to log in to the main menu of the Time & Attendance and the webpage.

- If you forget the administrator password, send a reset request to your registered e-mail address.
- The password must consist of 8 to 32 non-blank characters and contain at least two types of characters among upper case, lower case, number, and special character (excluding ' " ; : &).

2.5 Logging In

Log in to the main menu to configure the Time & Attendance. Only admin account and administrator

account can enter the main menu of the Time & Attendance. For the first-time use, use the admin account to enter the main menu screen and then you can create the other administrator accounts.

- admin account: Can log in to the main menu screen of the Time & Attendance, but has no door access permission.
- Administration account: Can log in to the main menu of the Time & Attendance and has door access permissions.

Step 1 Press and hold the standby screen for 3 seconds.

Step 2 select a verification method to enter the main menu.

- Face: Enter the main menu by face recognition.
- PWD: Enter the user ID and password of the administrator account.
- admin: Enter the admin password to enter the main menu.

2.6 Network Communication

Configure the network, serial port and Wiegand port to connect the Time & Attendance to the network.

The serial port and the wiegand port might differ depending on models of Time & Attendance.

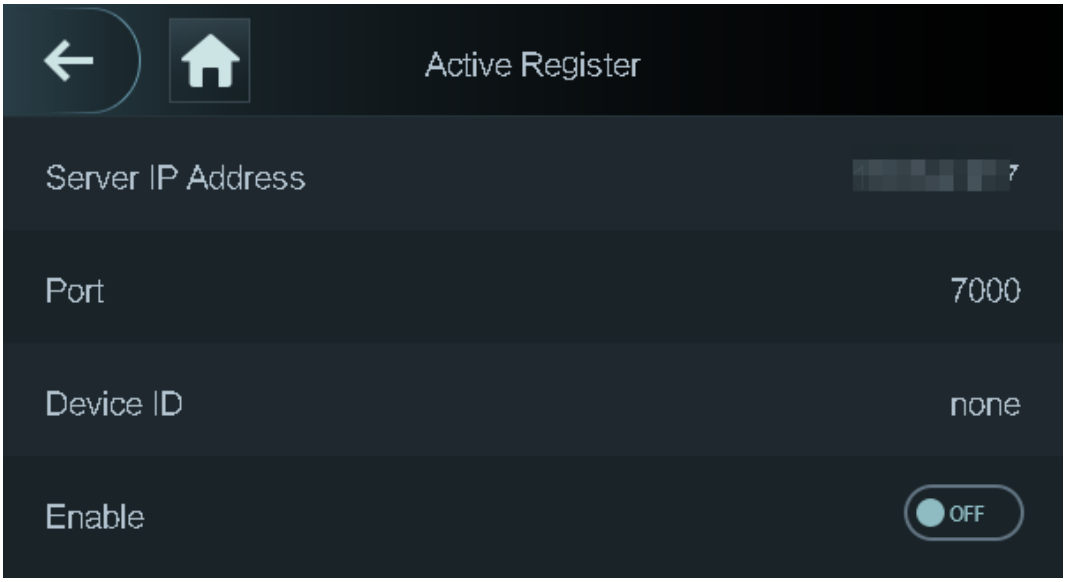
2.6.1 Active Register

You can turn on the automatic registration function to access the Time & Attendance through the management platform.

The management platform can clear all personnel configurations and initialize the Time & Attendance. To avoid data loss, keep the management platform permissions properly.

Step 1 On the **Main Menu**, select **Connection** > **Network** > **Active Register**.

Figure 2-3 Auto register



Step 2 Turn on the automatic registration function and set the parameters.

Table 2-3 Auto registration

Parameter	Description
Server Address	The IP address of the management platform.
Port	The port No. of the management platform.
Device ID	Enter the device ID (user defined). When you add the Time & Attendance to the management platform, the device ID on the management platform must conform to the defined device ID on the Time & Attendance.

Step 3 Enable the active register function.

2.6.2 Configuring Wi-Fi

You can connect the Time & Attendance to the network through Wi-Fi network.

Wi-Fi function is only available for certain models of the Time & Attendance.

Step 1 On the **Main Menu**, select **Connection** > **Network** > **WiFi**.

Step 2 Turn on Wi-Fi.

Step 3 Tap to search available wireless networks.

Step 4 Select a wireless network and enter the password.

If no Wi-Fi is searched, tap **SSID** to enter the name of Wi-Fi.

Step 5 Tap

2.7 User Management

You can add new users, view user/admin list and edit user information.

The pictures in this manual are for reference only, and might differ from the actual product.

2.7.1 Adding New Users

Step 1 On the **Main Menu**, select **User** > **New User**.

Step 2 Configure the parameters on the interface.

Figure 2-4 New user (1)



Figure 2-5 New user (2)

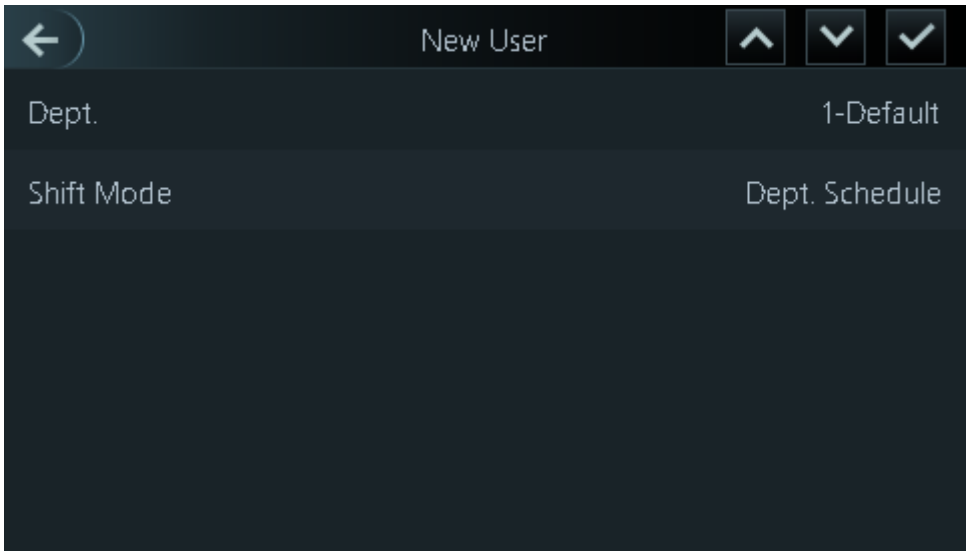


Table 2-4 Description of new user parameters

Parameter	Description
User ID	Enter user IDs. The IDs can be numbers, letters, and their combinations, and the maximum length of the ID is 32 characters. Each ID is unique.
Name	Enter name with at most 32 characters (including numbers, symbols, and letters).
Face	Make sure that your face is centered on the image capturing frame, and an image of the face will be captured and analyzed automatically.
PWD	Enter the user password. The maximum length of the password is 8 digits.
User Level	You can select a user level for new users. • **User**: Users only have door access permission. • **Admin**: Administrators can unlock the door and configure the Time & Attendance.

Parameter	Description
Valid Date	Set a date on which the access permissions of the person will be expired.
Dept.	Set departments.
Shift Mode	Select shift modes.

Step 3 Tap .

2.7.2 Viewing User Information

You can view user/admin list and edit user information.

Step 1 On the **Main Menu**, select **User** > **User List**, or select **User** > **Admin List**.

Step 2 View all added users and admin accounts.

- : Unlock through password.
- : Unlock through face recognition.

Related Operations

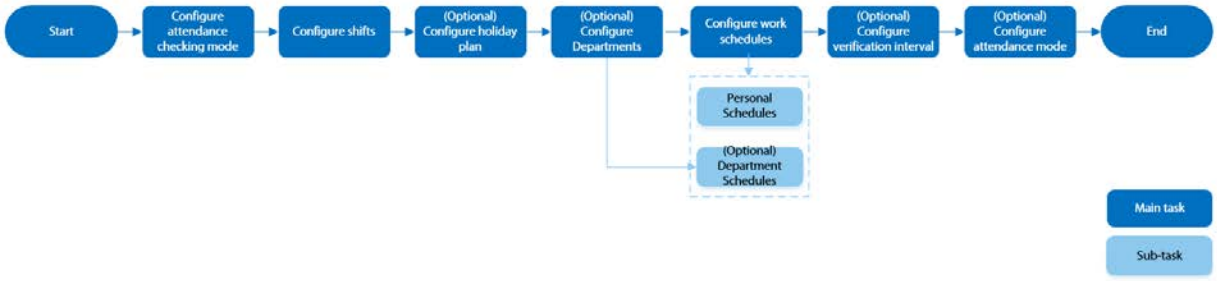
On the **User** screen, you can manage the added users.

- Search for users: Tap and then enter the username.
- Edit users: Tap the user to edit user information.
- Delete users
  - Delete individually: Select a user, and then tap .
  - Delete in batches:
    - On the **User List** screen, tap to delete all users.
    - On the **Admin List** screen, tap to delete all admin users.

2.8 Attendance Management

The Time Attendance supports attendance management both on the local device or on the Smart PSS Lite. This section only takes configuring attendance on the local device as an example.

Figure 2-6 Configuration flow chart of time attendance



2.8.1 Configuring Attendance Checking Modes

Use face or password, or their combinations to punch in/out.

Step 1 Select **Attendance** > **Atten Type**.

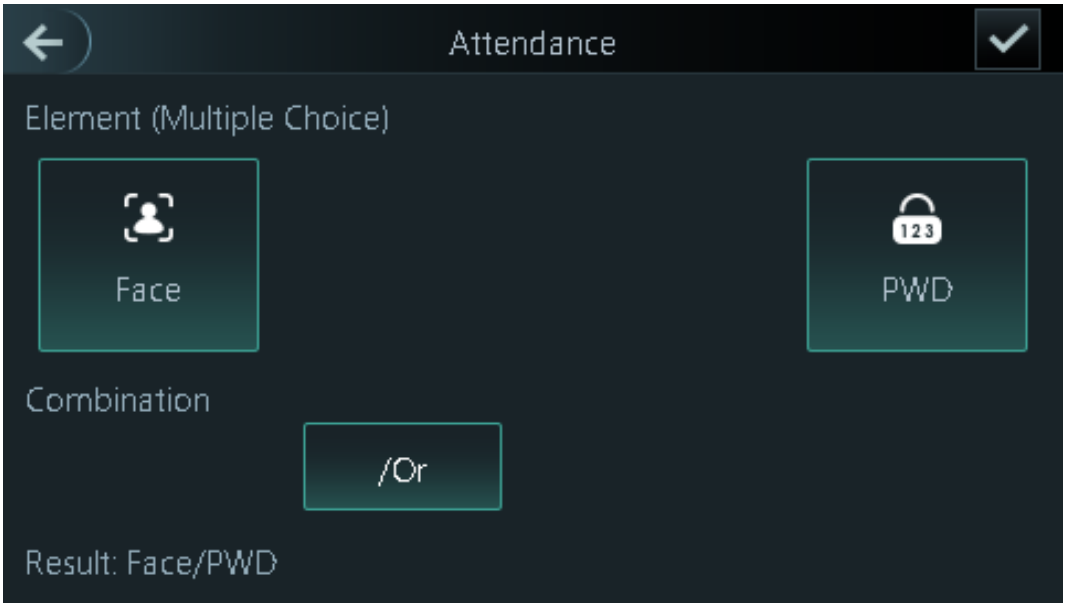
Step 2 Select the attendance checking methods.

To cancel your selection, tap the selected method again.

Step 3 Tap +**And** or **/Or** to configure combinations.

- **+And**: Verify all the selected methods to punch in/out.
- **/Or**: Verify one of the selected unlocking methods to punch in/out.

Figure 2-7 Element (multiple choice)



Step 4 Tap ☑ to save changes.

2.8.2 Configuring Shifts

Configure shifts to define time attendance rules. Employee need to come to work at the scheduled shift start time, and leave at the scheduled shift end time except when they work overtime.

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

Step 2 Select the number of the shift.

Tap ⌄ to view more shifts. You can configure up to 24 shifts.

Step 3 Configure the parameters of the shift.

Figure 2-8 Element (multiple choice)

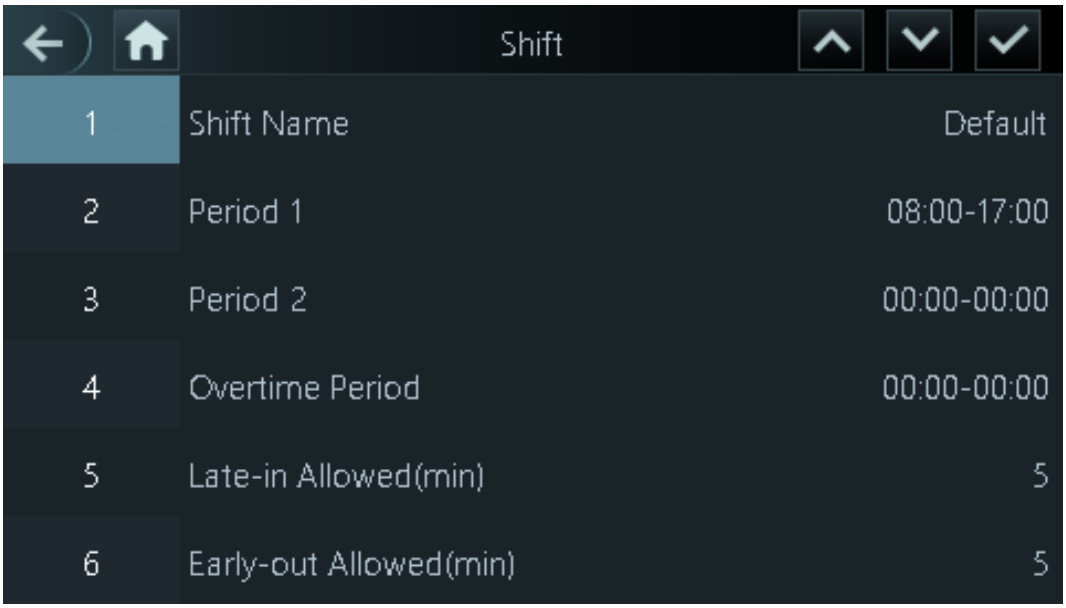


Table 2-5 Shift parameters description

Parameter	Description
Shift Name	Enter the name of the shift.
Period 1	Set the time attendance periods. If you set 08:00 —17:00, you need to punch in before 08:00 or earlier, and punch out at 17:00 or later, otherwise the abnormal attendance is abnormal. You can set two periods at the same time, the two periods cannot overlap. People must punch in and punch out in the both defined periods, and make sure their attendance is normal.
Period 2	
Overtime Period	People who punch in/out in the defined overtime period works beyond normal working hours.
Late-in Allowed(min)	The late-in and early-out allowed time is used mainly to give the employee a little flexibility to come a little late or leave a little early from work. For example, if the normal punch-in time is 8:00, and the late-in allowed time is set to 5 minutes, the employee who arrives at 8: 06 AM will be marked late by 1 minute.
Early-out Allowed(min)	

All attendance times are precise down to the second level, for example, if the punch-time is set to 8:05 AM, the employee who punches in at 8:05:59 AM will be marked normal attendance. If the employee who arrives at 8: 06 AM, they will be marked late by 1 minute.

Step 4 Tap ☑.

2.8.3 (Optional) Configuring Holiday Plans

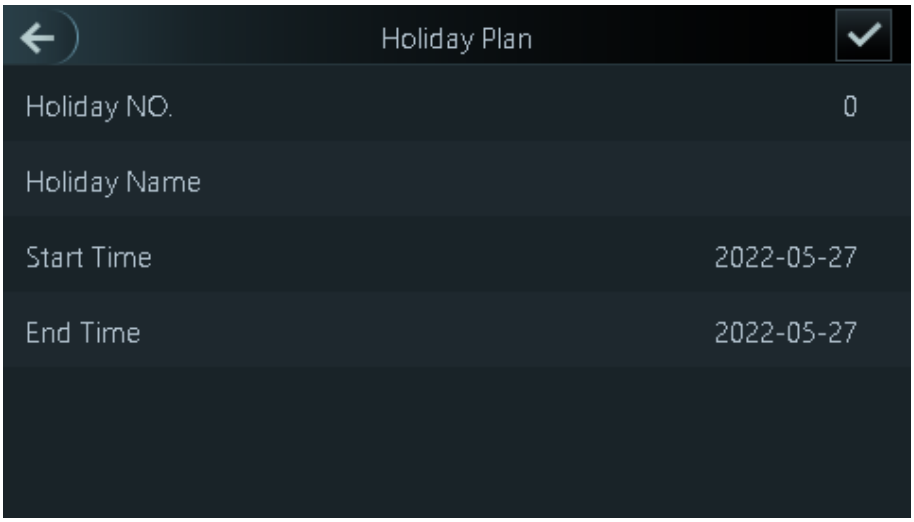
Configure holiday plans during which the time attendance will not tracked.

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

Step 2 Click + to add holiday plans.

Step 3 Configure the parameters.

Figure 2-9 Holiday Plan



Step 4 Tap ☑.

2.8.4 (Optional) Configuring Departments

Define departments.

Step 1 Select **Attendance** > **Dep. Set**.

Step 2 Select a department, and then rename it.

There are existing 20 default departments. We recommend you rename them.

Figure 2-10 Element (multiple choice)



Step 3 Tap ☑.

2.8.5 Configuring Work Schedules

A work schedule generally refers to the days per month and the hours per day that an employee is expected to be at their job. You can create different types of work schedules based on different individuals or departments, and then employees must follow the established work schedules.

Step 1 Select **Attendance** > **Schedule** > **Personal Schedule** > **Dept Schedule**.

Step 2 Set works schedules for individuals.

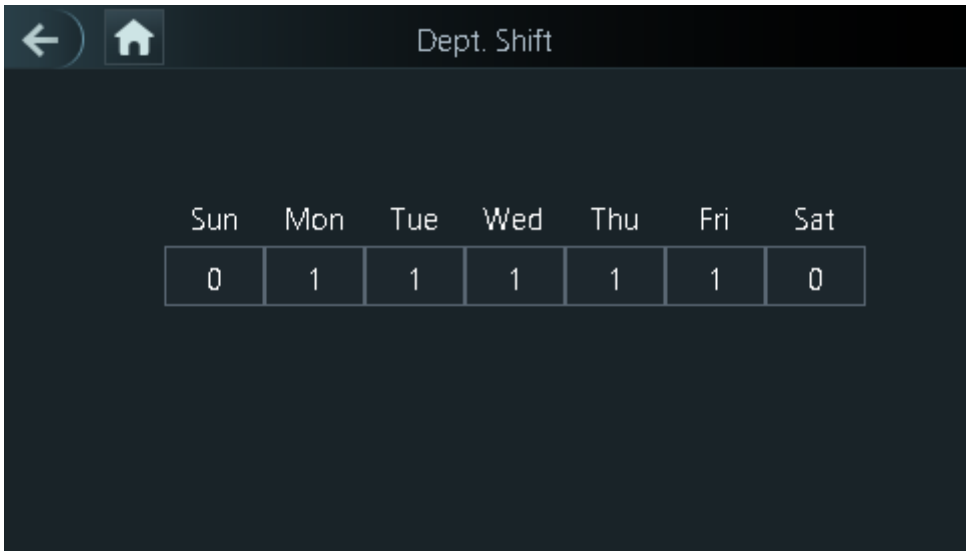
1. Tap **Personal Schedule**
2. enter the user ID, and then tap ☑.
3. On the calendar, select the date, and then configure shifts.
   You can only set work schedules for the current month and the next month.
   - 0 indicates break.
   - 1 to 24 indicates the number of the pre-defined shifts. For how to configure shifts, see "2.8.2 Configuring Shifts".
   - 25 indicates the business trip.
   - 26 indicates the leave of absence.
4. Tap ☑.

Step 3 Set works schedules for the department.

1. Tap **Dept Schedule**.
2. Tap a department, set shifts for a week.

- 0 indicates break.
- 1 to 24 indicates the number of the pre-defined shifts. For how to configure shifts, see "2.8.2 Configuring Shifts".
- 25 indicates the business trip.
- 26 indicates the leave of absence.

Figure 2-11 Department shifts



The defined work schedule is in one-week cycle and will be applied to all employees in the department.

Step 4 Tap ☑.

2.8.6 (Optional) Configuring Verification Interval Time

the employee repeats punch-in/out within a set time, the earliest punch-in/out will be recorded.

Step 1 Select **Attendance** > **Schedule** > **Verification Interval Time(s)**.

Step 2 enter the time interval, and then tap ☑.

2.8.7 (Optional) Configuring Attendance Modes

When you punch in or punch out, you can set the attendance modes to define the time attendance status.

Step 1 On the main menu, tap **Attendance** and then tap to move to the next page and then turn on **Local /Remote**.

You can set the attendance mode only after the **Local /Remote** function is turned on, and time local attendance records will be uploaded to Smart PSS Lite.

Step 2 On the main menu screen, select **Attendance** > **Mode Set**.

Figure 2-12 Attendance mode

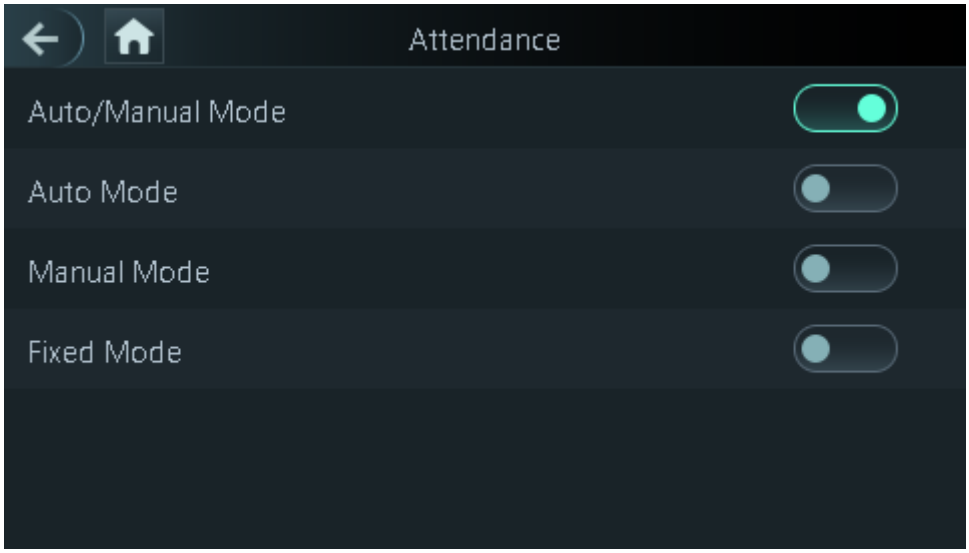


Table 2-6 Attendance mode

Parameter	Description
Auto/Manual Mode	After you punch in/out, you can manfully select the attendance status or the screen displays the time attendance status automatically.
Auto Mode	The screen displays attendance status automatically after you punch in/out.
Manual Mode	Punch in/out and then tap **Attendance status** to manfully select the attendance status.
Fixed Mode	When you punch in/out, the screen will displays the pre-configured attendance status all the time.

Step 3 Select an attendance mode.

Step 4 Configure the parameters for the attendance mode.

Figure 2-13 Auto Mode/manual mode

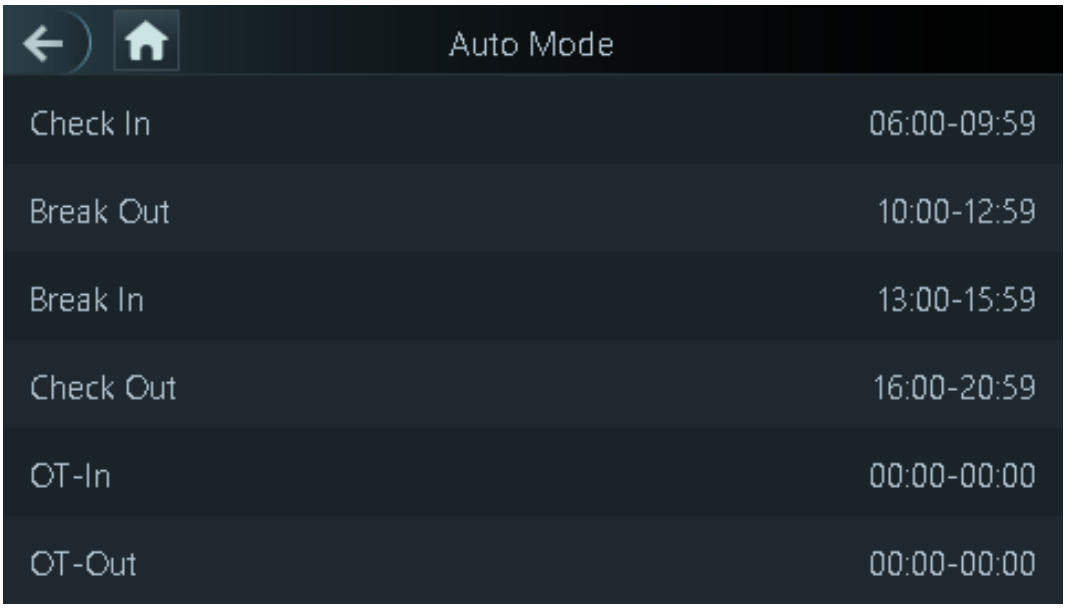


Figure 2-14 Fixed mode

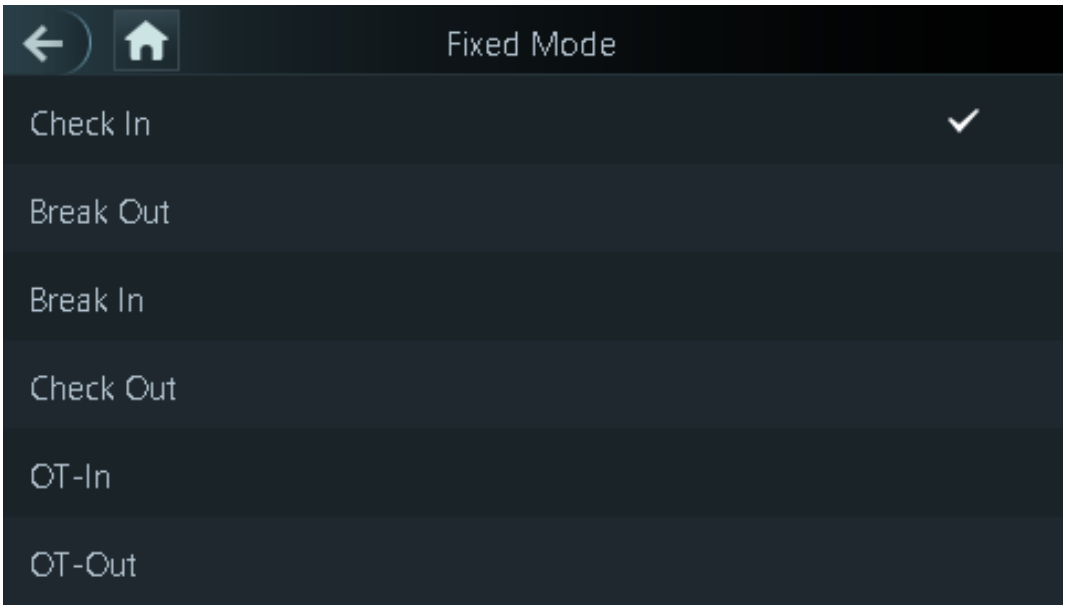


Table 2-7 Attendance mode parameters

Parameters	Description
Check In	Punch in when your normal workday starts.
Break Out	Punch out when your leave of absence ends.
Break In	Punch in when your leave of absence starts.
Check Out	Punch out when your normal workday starts.
OT-In	Punch-in when your overtime working hours starts.
OT-Out	Punch out when your overtime working hours ends.

2.9 System

2.9.1 Configuring Time

Configure system time, such as date, time, and NTP.

Step 1 On the **Main Menu**, select **System** > **Time**.

Step 2 Configure system time.

Figure 2-15 Time



Table 2-8 Description of time parameters

Parameter	Description
24-hour System	The time is displayed in 24-hour format.
Date Setting	Set up the date.
Time	Set up the time.
Date Format	Select a date format.
DST Setting	1. Tap **DST Setting** 2. Enable DST. 3. Select **Date** or **Week** from the **DST** Type list. 4. Enter start time and end time. 5. tap ✓.

Parameter	Description
NTP Check	A network time protocol (NTP) server is a machine dedicated as the time sync server for all client computers. If your computer is set to sync with a time server on the network, your clock will show the same time as the server. When the administrator changes the time (for daylight savings), all client machines on the network will also update. 1. Tap **NTP Check**. 2. Turn on the NTP check function and configure parameters. • **Server IP Address**: Enter the IP address of the NTP server, and the Time & Attendance will automatically sync time with NTP server. • **Port**: Enter the port of the NTP server. • **Interval (min)**: Enter the time synchronization interval.
Time Zone	Select the time zone.

2.9.2 Configuring Face Parameters

Step 1 On the main menu, select **System** > **Face Parameter**.

Step 2 Configure the face parameters, and then tap ☑.

Figure 2-16 Face parameter (01)

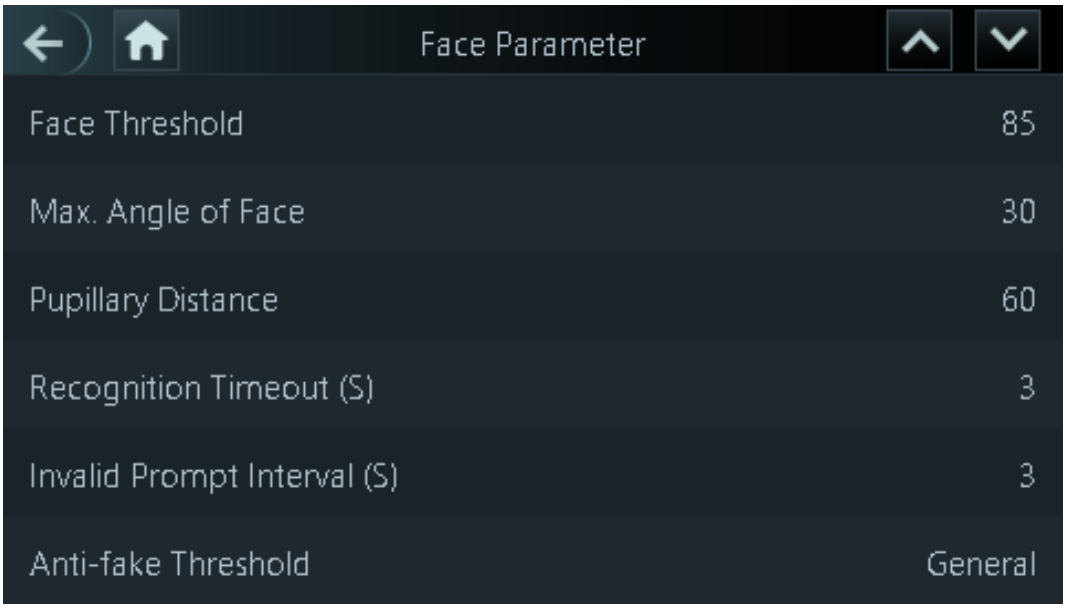


Figure 2-17 Face parameter (02)



Table 2-9 Description of face parameters

Name	Description
Face Threshold	Adjust the face recognition accuracy. Higher threshold means higher accuracy.
Max. Angle of Face	Set the maximum face pose angle for face detection. Larger value means larger face angle range. If the face pose angle is out of the defined range, the face detection box will not appear.
Pupillary Distance	Face images require desired pixels between the eyes (called pupillary distance) for successful recognition. The default pixel is 45. The pixel changes according to the face size and the distance between faces and the lens. If an adult is 1.5 meters away from the lens, the pupillary distance can be 50 px-70 px.
Recognition Timeout (S)	If a person with access permission has their face successfully recognized, the Time & Attendance will prompt face recognition success. You can enter the prompt interval time.
Invalid Face Prompt Interval (S)	If a person without access permission attempts to unlock the door for several times in the defined interval, the Time & Attendance will prompt face recognition failure. You can enter the prompt interval time.
Anti-fake Threshold	Avoid false face recognition by using a photo, video, mask or a different substitute for an authorized person's face. ● Close: Turns off this function. ● General: Normal level of anti-spoofing detection means higher door access rate for people with face masks. ● High: Higher level of anti-spoofing detection means higher accuracy and security. ● Extremely High: Extremely high level of anti-spoofing detection means extremely high accuracy and security.
BeautyEnable	Beautify captured face images.

Name	Description
Mask Parameters	• Mask mode: ◇ **No detect**: Mask is not detected during face recognition. ◇ **Mask reminder**: Mask is detected during face recognition. If the person is not wearing a mask, the system will remind them to wear masks, and access is allowed. ◇ **Mask intercept**: Mask is detected during face recognition. If a person is not wearing a mask, the system will remind them to wear masks, and access is denied. • Mask Recognition Threshold: Higher threshold means higher mask detection accuracy.
Multi-face Recognition	Supports detecting 4 face images at the same time, and the unlock combinations mode become invalid. The door is unlocked after any one of them gain access.

2.9.3 Setting Volume

You can adjust the volume of the speaker and microphone.

Step 1 On the **Main Menu**, select **System** > **Volume**.

Step 2 Tap + or − to adjust the volume.

2.9.4 Screen Settings

Configure screen off time and logout time.

Step 1 On the **Main Menu**, select **System** > **Screen settings**.

Step 2 Tap **Logout Time** or **Screen Off Timeout**, and then tap + or − to adjust the time.

2.9.5 Restoring Factory Defaults

Step 1 On the **Main Menu**, select **System** > **Restore Factory**.

Step 2 Restore factory defaults if necessary.

- **Restore Factory**: Resets all configurations and data.
- **Restore Factory (Save user & log)**: Resets configurations except for user information and logs.

2.9.6 Restart the Device

On the **Main Menu**, select **System** > **Reboot**, and the Time & Attendance will be restarted.

2.9.7 Configuring the Language

Change the language on the Time & Attendance.

On the **Main Menu**, select **System** > **Language**, select the language for the Time & Attendance.

2.10 USB Management

You can use a USB to update the Time & Attendance, and export or import user information through USB.

- Make sure that a USB is inserted to the Time & Attendance before you export data or update the system. To avoid failure, do not pull out the USB or perform any operation of the Time & Attendance during the process.
- You have to use a USB to export the information from the Time & Attendance to other devices. Face images are not allowed to be imported through USB.

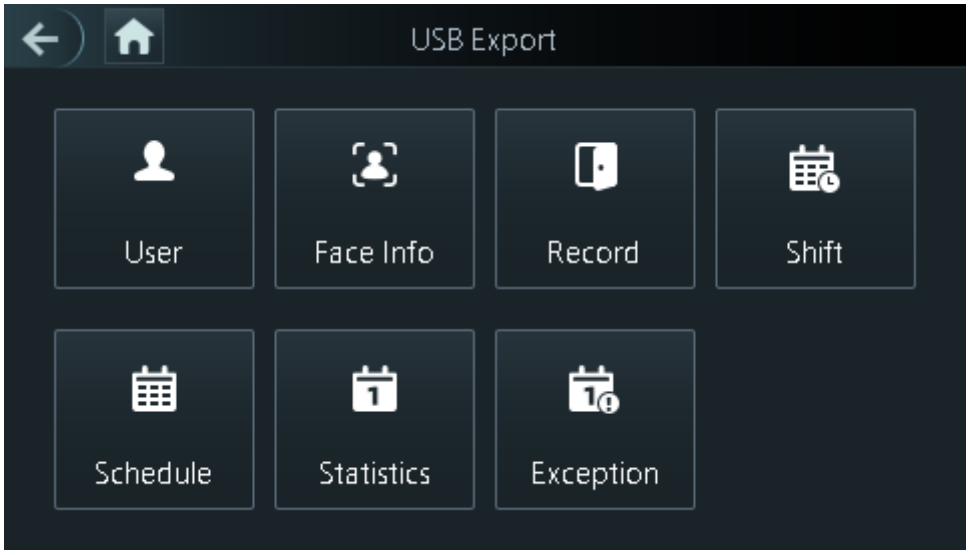
2.10.1 Exporting to USB

You can export data from the Time & Attendance to a USB. The exported data is encrypted and cannot be edited.

Step 1 On the **Main Menu**, select **USB** > **USB Export**.

Step 2 Select the data type you want to export, and then tap **OK**.

Figure 2-18 USB export



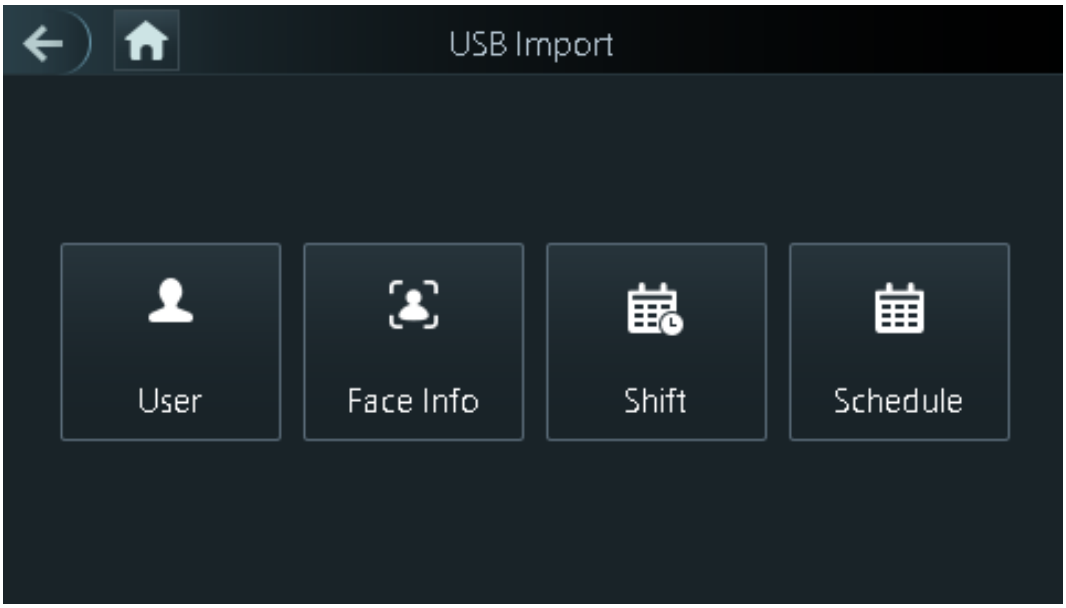
2.10.2 Importing From USB

You can import data from USB to the Time & Attendance.

Step 1 On the **Main Menu**, select **USB** > **USB Import**.

Step 2 Select the data type that you want to export, and then tap **OK**.

Figure 2-19 USB import



2.10.3 Updating System

Use a USB to update the system of the Time & Attendance.

Step 1 Rename the update file to "update.bin", put it in the root directory of the USB, and then insert the USB to the Time & Attendance.

Step 2 On the **Main Menu**, select **USB** > **USB Update**.

Step 3 Tap **OK**.

The Time & Attendance will restart when the updating completes.

2.11 Configuring Features

On the **Main Menu** screen, select **Features**.

Figure 2-20 Features

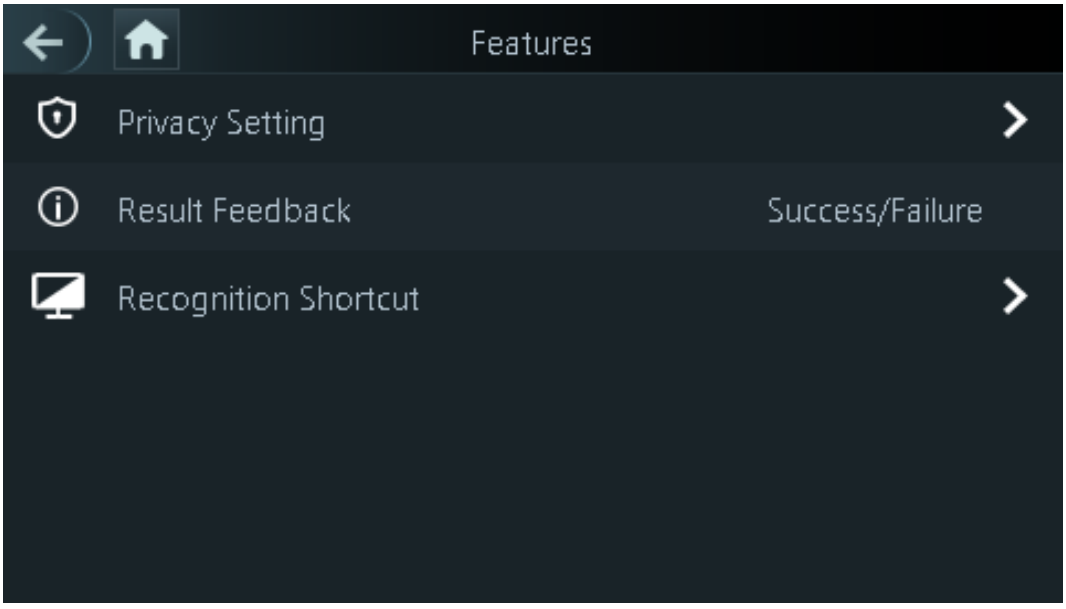


Table 2-10 Description of features

Parameter	Description
Private Setting	● PWD Reset Enable: You can enable this function to reset password. The PWD Reset function is enabled by default. ● HTTPS: Hypertext Transfer Protocol Secure (HTTPS) is a protocol for secure communication over a computer network. When HTTPS is enabled, HTTPS will be used to access CGI commands; otherwise HTTP will be used.  When HTTPS is enabled, the Time & Attendance will restart automatically. ● CGI: Common Gateway Interface (CGI) offers a standard protocol for web servers to execute programs similarly to console applications running on a server that dynamically generates web pages. The CG I is enabled by default. ● SSH: Secure Shell (SSH) is a cryptographic network protocol for operating network services securely over an unsecured network. ● Capture Photos: Face images will be captured automatically when people unlock the door. The function is enabled by default. ● Clear Captured Photos: Delete all automatically captured photos.
Result Feedback	● Success/Failure: Only displays success or failure on the standby screen. ● Only Name: Displays user ID, name and authorization time after access granted; displays not authorized message and authorization time after access denied. ● Photo&Name: Displays user's registered face image, user ID, name and authorization time after access granted; displays not authorized message and authorization time after access denied. ● Photos&Name: Displays the captured face image and a registered face image of a user, user ID, name and authorization time after access granted; displays not authorized message and authorization time after access denied.
Recognition shortcut	Password: when it is turn on, the icon of the password unlock method is displayed on the standby screen.

2.12 Viewing Attendance Logs

View or search time attendance logs. On the main menu, tap **Record Search> Attendance Records**.

2.13 System Information

You can view data capacity and device version.

2.13.1 Viewing Data Capacity

On the **Main Menu**, select **System Info** > **Data Capacity**, you can view storage capacity of each data type.

2.13.2 Viewing Device Version

On the **Main Menu**, select **System Info** > **Data Capacity**, you can view the device version, such as serial No., software version and more.

3 Web Operations

On the webpage, you can also configure and update the Time & Attendance.

Web configurations differ depending on models of the Time & Attendance.

3.1 Initialization

Initialize the Time & Attendance when you log in to the webpage for the first time or after the Time & Attendance is restored to the factory defaults.

Prerequisites

Make sure that the computer used to log in to the webpage is on the same LAN as the Time & Attendance.

Set a password and an email address before logging in to the webpage for the first time.

Step 1 Open a browser, go to the IP address (the default address is 192.168.1.108) of the Time & Attendance.

We recommend you use the latest version of Chrome or Firefox.

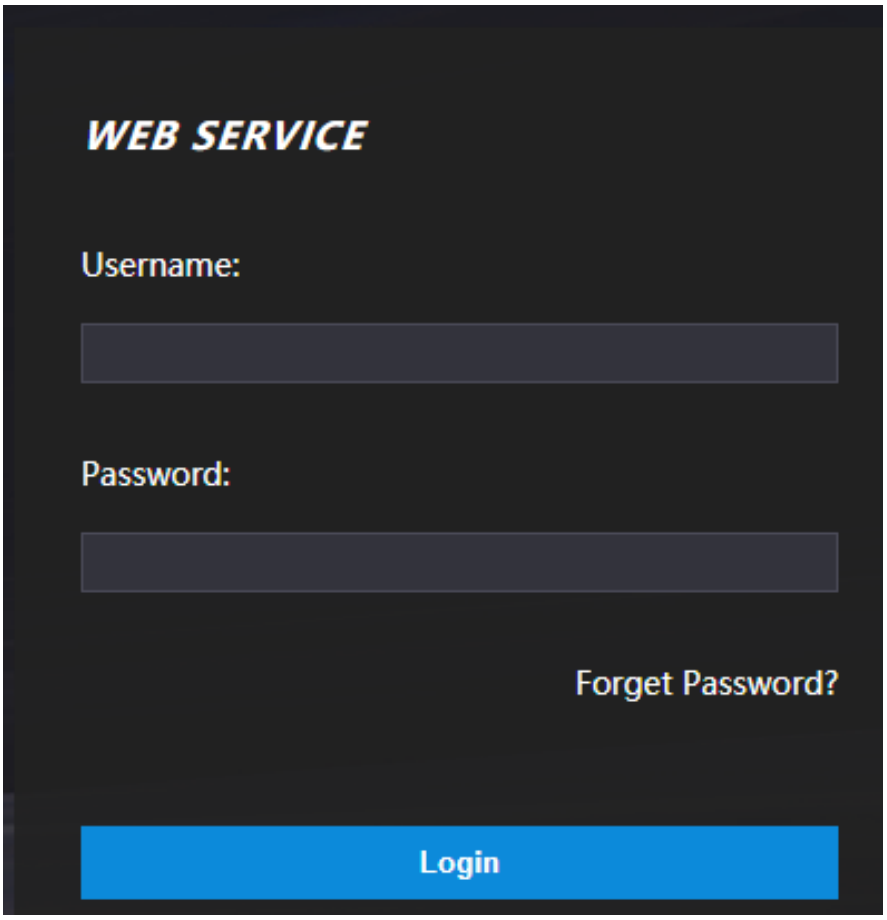
Step 2 Set the password and email address according to the screen instructions.

- The password must consist of 8 to 32 non-blank characters and contain at least two types of the following characters: upper case, lower case, numbers, and special characters (excluding ' " ; : &). Set a high-security password by following the password strength prompt.
- Keep the password safe after initialization and change the password regularly to improve security.

3.2 Logging In

Step 1 Open a browser, enter the IP address of the Time & Attendance in the **Address** bar, and press the Enter key.

Figure 3-1 Login



Step 2 Enter the user name and password.

- The default administrator name is admin, and the password is the one you set up during initialization. We recommend you change the administrator password regularly to increase security.
- If you forget the administrator login password, you can click **Forget password?** For details, see "3.3 Resetting the Password".

Step 3 Click **Login**.

3.3 Resetting the Password

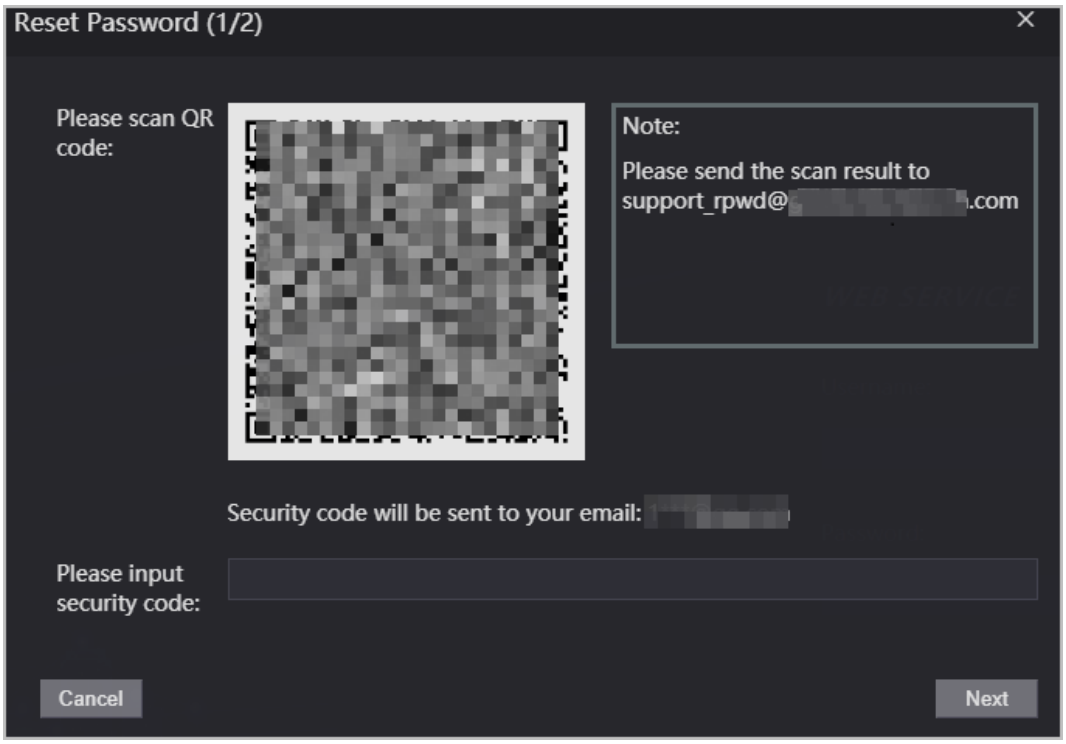
Reset the password through the linked e-mail when you forget the admin password.

Step 1 On the login page, click **Forgot password**.

Step 2 Read the on-screen prompt carefully, and then click **OK**.

Step 3 Scan the QR code, and you will get the security code.

Figure 3-2 Reset password



- Up to two security codes will be generated when the same QR code is scanned. If the security code becomes invalid, refresh the QR code and scan again.
- After you scan the QR code, you will receive a security code in your linked e-mail address. Use the security code within 24 hours after you receive it. Otherwise, it will become invalid.
- If the wrong security code is entered in a row, the administrator account will be frozen for 5 minutes.

Step 4 Enter the security code.

Step 5 Click **Next**.

Step 6 Reset and confirm the new password.

The password should consist of 8 to 32 non-blank characters and contain at least two of the following types of characters: upper case, lower case, number, and special character (excluding ' " ; : &).

Step 7 Click **OK**.

3.4 Data Capacity

You can see how many users, cards and face images that the Time & Attendance can store.

Log in to the webpage and select **Data Capacity**.

3.5 Configuring Video and Image

Configure video and image parameters, such as stream and brightness.

We recommend you use the default parameters in this section.

3.5.1 Configuring Video

On the home page, select **Video Setting**, and then configure the video stream, status, image and exposure.

- Video Standard: Select **NTSC**.
- Channel Id: Channel 1 is for configurations of visible light image. Channel 2 is for configurations of infrared light image.
- Default: Restore to defaults settings.
- Capture: Take a snapshot of the current image.

PAL video standard is 25 fps and the NTSC video standard is 30 fps.

3.5.1.1 Configuring Channel 1

Step 1 Select **Video Setting** > **Video Setting**.

Step 2 Select **1** from the **Channel No.** list.

Step 3 Configure the date rate.

Figure 3-3 Date rate

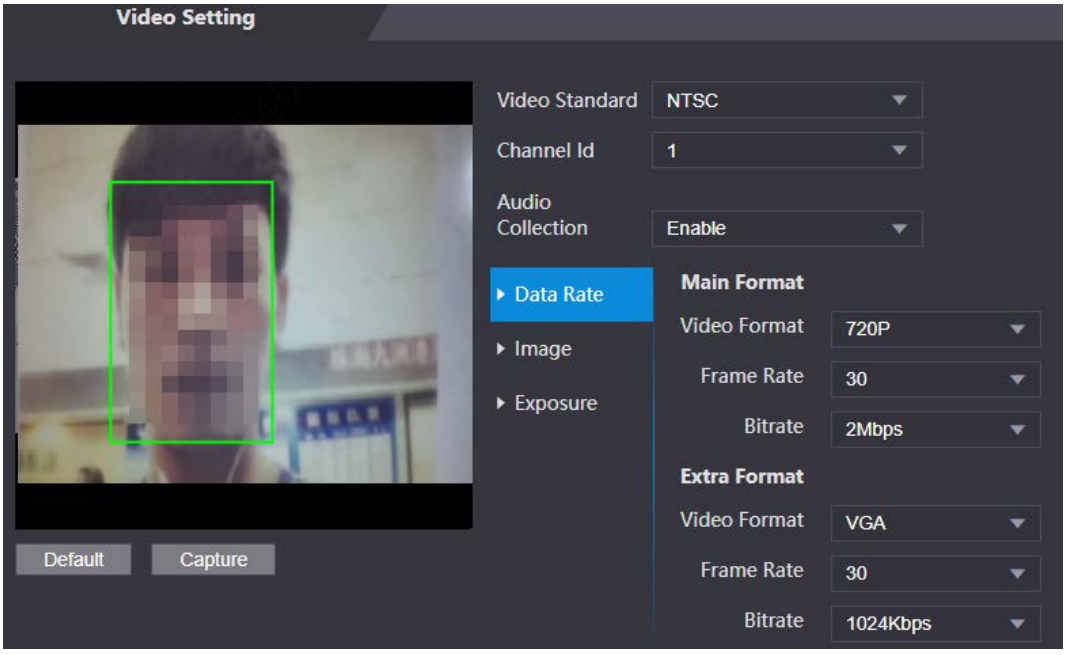


Table 3-1 Date rate description

Parameter		Description
Main Format	Video Format	When the Time & Attendance functions as the a VTO and connects the VTH, the acquired stream limit of VTH is 720p.When resolution is changed to 1080p, the call and monitor function might be affected.
	Frame Rate	The number of frames (or images) per second. The frame rate range is 1–25 fps.
	Bitrate	It indicates the amount of data transmitted over an internet connection in a given amount of time. Select a proper bandwidth based on your network speed.
Sub Stream	Video Format	The sub-stream supports D1, VGA and QVGA.
	Frame Rate	The number of frames (or images) per second. The frame rate range is 1–25 fps.
	Bitrate	It indicates the amount of data transmitted over an internet connection in a given amount of time.

Step 4 Configure the image.

Figure 3-4 Image

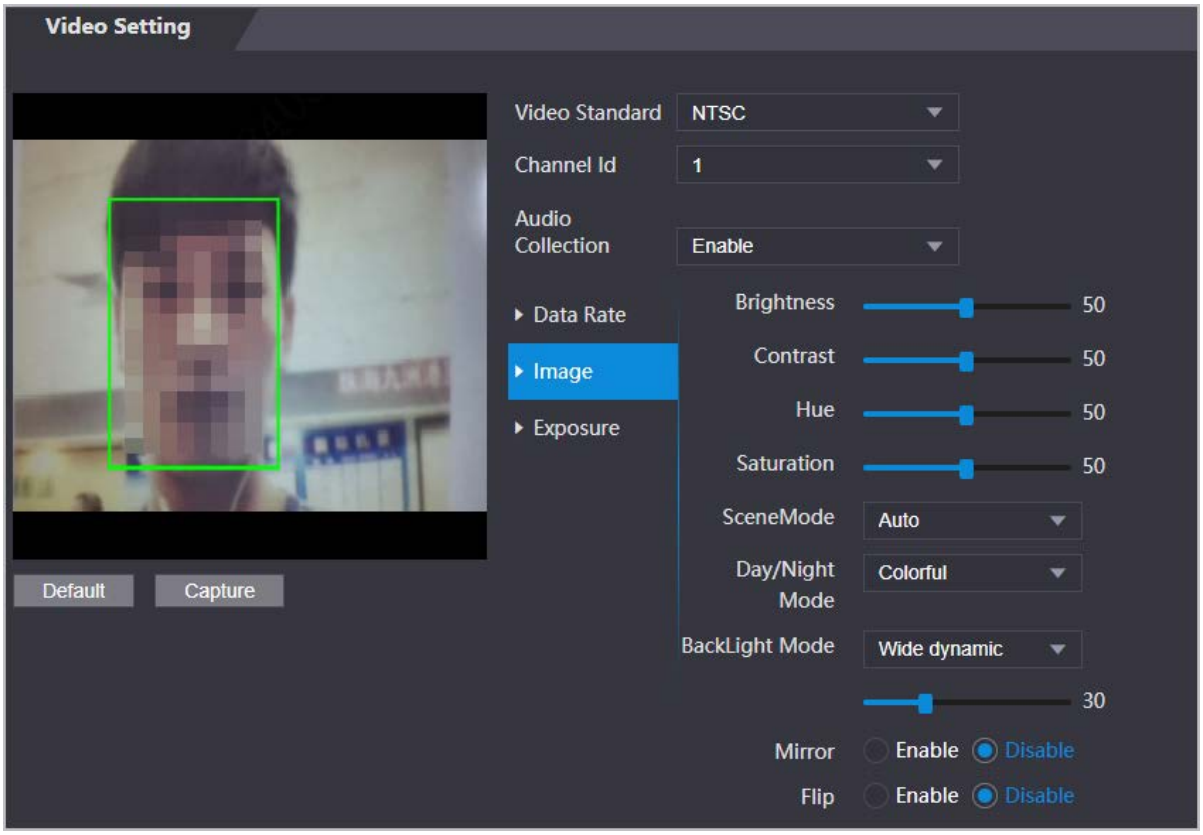


Table 3-2 Image description

Parameter	Description
Contrast	Contrast is the difference in the luminance or color that makes an object distinguishable. The larger the contrast value is, the greater the color contrast will be.
Hue	Refers to the strength or saturation of a color. It describes the color intensity, or how pure it is.
Saturation	Color saturation indicates the intensity of color in an image. As the saturation increases, the appear stronger, for example being more red or more blue. The saturation value does not change image brightness.
Scene Mode	The image hue is different in different scene mode. ● **Close**: Scene mode function is turned off. ● **Auto**: The system automatically adjusts the scene mode based on the photographic sensitivity. ● **Sunny**: In this mode, image hue will be reduced. ● **Night**: In this mode, image hue will be increased.
Day/Night	Day/Night mode affects light compensation in different situations. ● **Auto**: The system automatically adjusts the day/night mode based on the photographic sensitivity. ● **Colorful**: In this mode, images are colorful. ● **Black and white**: In this mode, images are in black and white.
Backlight Mode	● **Close**: Backlight compensation is turned off. ● **Backlight**: Backlight compensation automatically brings more light to darker areas of an image when bright light shining from behind obscures it. ● **Wide dynamic**: The system dims bright areas and compensates for dark areas to create a balance to improve the overall image quality. ● **Inhibition**: Highlight compensation (HLC) is a technology used in CCTV/IP security cameras to deal with images that are exposed to lights like headlights or spotlights. The image sensor of the camera detects strong lights in the video and reduces exposure in these spots to enhance the overall quality of the image.
Mirror	When the function is turned on, images will be displayed with the left and right side reversed.
Flip	When this function is turned on, images can be flipped over.

Step 5 Configure the exposure parameters.

Figure 3-5 Exposure

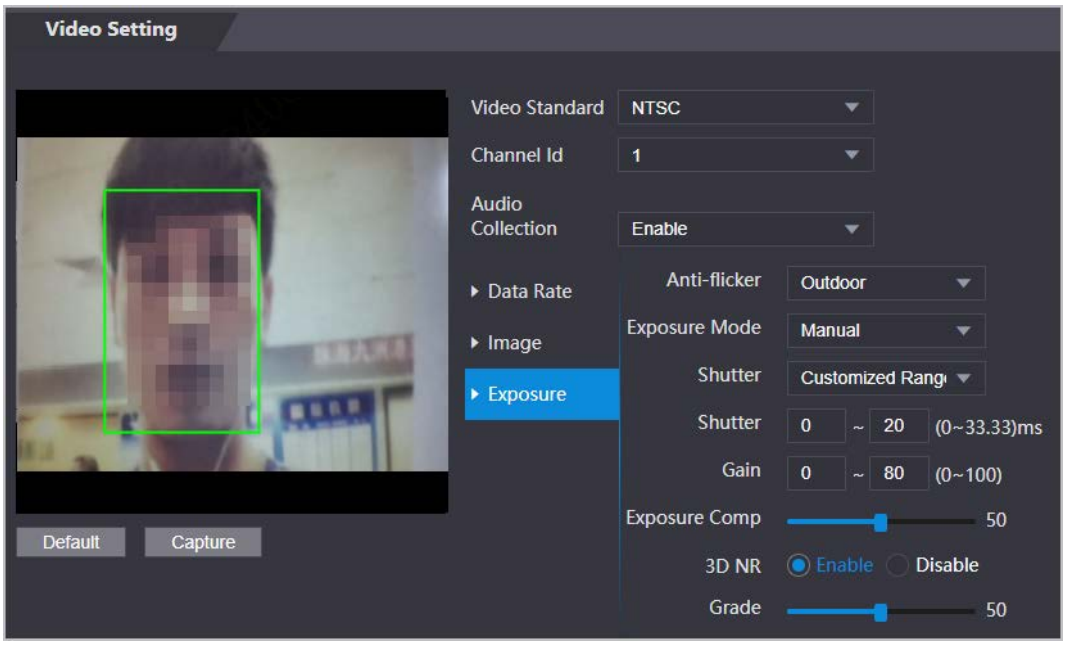


Table 3-3 Exposure parameter description

Parameter	Description
Anti-flicker	Set anti-flicker to reduce flicker and decrease or reduce uneven colors or exposure. • **50Hz**: When the mains power supply is 50 Hz, the exposure is automatically adjusted to prevent the appearance of horizontal lines. • **60Hz**: When the mains power supply is 60 Hz, the exposure is automatically adjusted to reduce the appearance of horizontal lines. • **Outdoor**: When **Outdoor** is selected, the exposure mode can be switched.
Exposure Mode	You can set the exposure to adjust image brightness. • **Auto**: The Time & Attendance automatically adjusts the brightness of images. • **Shutter Priority**: The Access Terminal will adjust image brightness according to shutter exposure range. If the image brightness is not enough and the shutter value has reached its upper or lower limit, the Time & Attendance will adjust the gain value automatically for ideal brightness level. • **Manual**: You can configure gain and shutter value manually to adjust image brightness. ◇ When you select **Outdoor** from the **Anti-flicker** list, you can select **Shutter Priority** as the exposure mode. ◇ Exposure mode might differ depending on different models of Time & Attendance.

Parameter	Description
Shutter	Shutter is a component that allows light to pass for a determined period. The higher the shutter speed, the shorter the exposure time, and the darker the image.
Gain	When the gain value range is set, video quality will be improved.
Exposure Compensation	You can make a photo brighter or darker by adjusting exposure compensation value.
3D NR	When 3D Noise Reduction (RD) is turned on, video noise can be reduced to ensure high definition videos. You can set its grade when this function is turned on.
Grade	

3.5.1.2 Configuring Channel 2

Step 1 Select **Video Setting** > **Video Setting**.

Step 2 Select 2 from the **Channel No.**.

Step 3 Configure the video status.

We recommend you turn on the WDR function when the face is in back-lighting.

Figure 3-6 Image

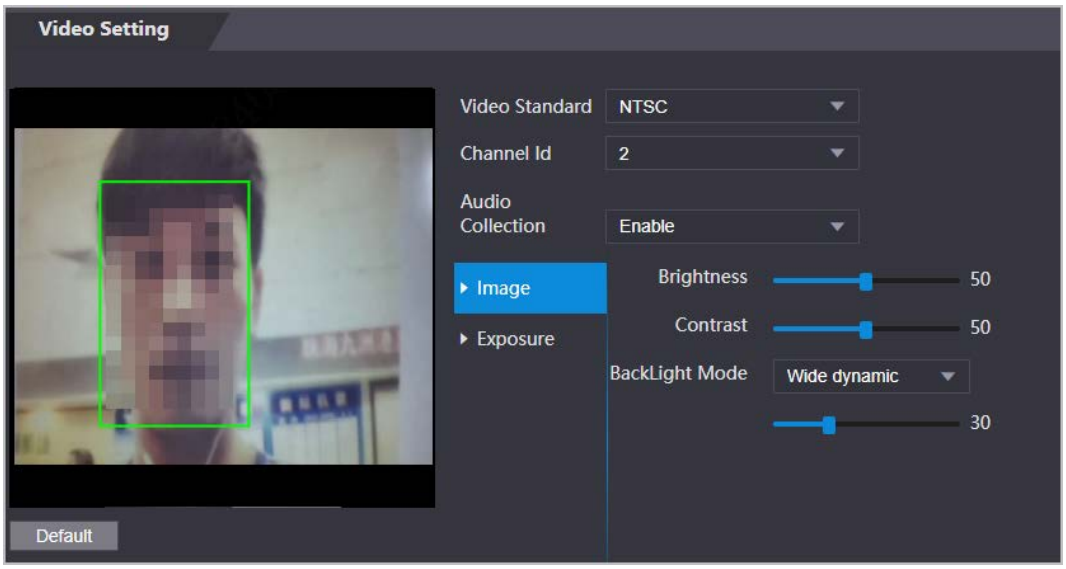


Table 3-4 Image description

Parameter	Description
Brightness	Brightness is the relative lightness or darkness of a particular color. The larger the value is, the brighter the image will be.
Contrast	Contrast is the difference in the luminance or color that makes an object distinguishable. The larger the contrast value is, the greater the color contrast will be.

Parameter	Description
Backlight Mode	• **Close**: Back-light compensation is turned off. • **Backlight**: Black-light compensation automatically brings more light to darker areas of an image when bright light shining from behind obscures it. • **Wide dynamic**: The system dims bright areas and compensates for dark areas to ensure to create a balance to improve the overall image quality. • **Inhibition**: Highlight compensation (HLC) is a technology used in CCTV/IP security cameras to deal with images that are exposed to lights like headlights or spotlights. The image sensor of the camera detects strong lights in the video and reduce exposure in these spots to enhance the overall quality of the image.

Step 4 Configure the exposure parameters.

Figure 3-7 Exposure parameter

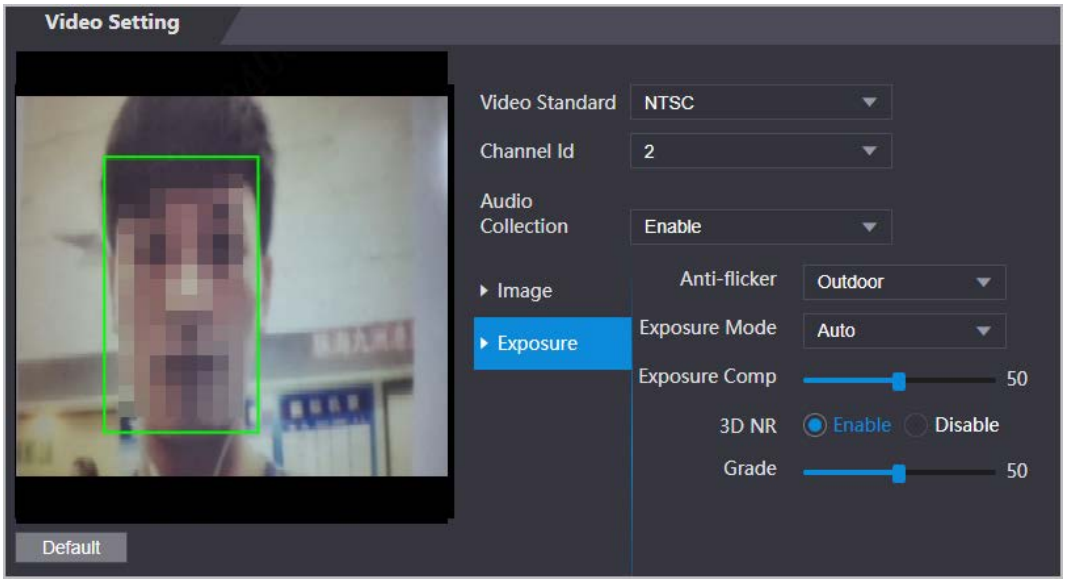


Table 3-5 Exposure parameter description

Parameter	Description
Anti-flicker	Set anti-flicker to reduce flicker and decrease or eliminate uneven colors or exposure. • **50Hz**: When the mains power supply is 50 Hz, the exposure is automatically adjusted to prevent the appearance of horizontal lines. • **60 Hz**: When the mains power supply is 60 Hz, the exposure is automatically adjusted to reduce the appearance of horizontal lines. • **Outdoor**: When **Outdoor** is selected, the exposure mode can be switched.

Parameter	Description
Exposure Mode	You can set the exposure to adjust image brightness. ● **Auto**: The Time & Attendance automatically adjusts the brightness of images. ● **Shutter Priority**: The Access Terminal will adjust image brightness according to shutter exposure range. If the image brightness is not enough and the shutter value has reached its upper or lower limit, the Time & Attendance will adjust the gain value automatically for ideal brightness level. ● **Manual**: You can configure gain and shutter value manually to adjust image brightness. ◇ When you select **Outdoor** from the **Anti-flicker** list, you can select **Shutter Priority** as the exposure mode. ◇ Exposure model might differ depending on different models of Time & Attendance.
Shutter	Shutter is a device that allows light to pass for a determined period. The higher the shutter speed, the shorter the exposure time, and the darker the image.
Gain	When the gain value range is set, video quality will be improved.
Exposure Compensation	You can make a photo brighter or darker by adjusting exposure compensation value.
3D NR	When 3D Noise Reduction (RD) is turned on, video noise can be reduced to ensure high definition videos. You can set its grade when this function is turned on.
Grade	

3.5.2 Setting Volume

You can adjust the volume of the speaker.

Step 1 Log in to the webpage.

Step 2 Select **Video Setting** > **Volume Setting**.

Step 3 Drag the slider the adjust the volume.

Step 4 Click **OK**.

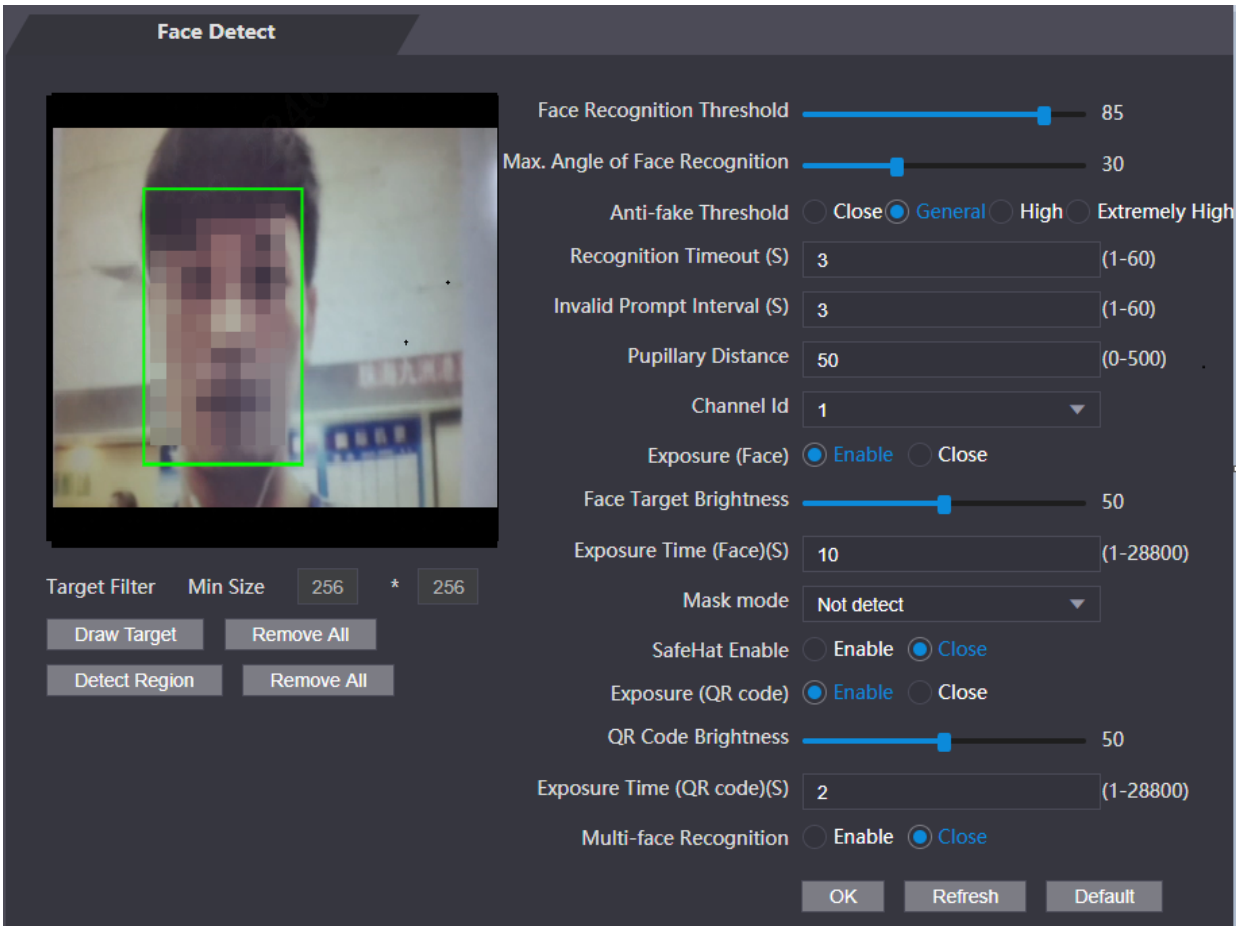
3.6 Configuring Face Detection

You can configure human face related parameters on this interface to increase the accuracy of the face recognition.

Step 1 Log in to the webpage.

Step 2 Select **Face Detect**.

Figure 3-8 Face detect



Step 3 Configure the parameters.

Table 3-6 Description of face detection parameters

Parameter	Description
Face Threshold	Adjust the face recognition accuracy. Higher threshold means higher accuracy.
Max. Angle of Face	Set the maximum face pose angle for face detection. Larger value means larger face angle range. If the face pose angle is out of the defined range, the face detection box will not appear.
Anti-fake Threshold	Avoid false face recognition by using a photo, video, mask or a different substitute for an authorized person's face. ● Close: Turns off this function. ● General: Normal level of anti-spoofing detection means higher door access rate for people with face masks. ● High: Higher level of anti-spoofing detection means higher accuracy and security. ● Extremely High: Extremely high level of anti-spoofing detection means extremely high accuracy and security.
Recognition Timeout (S)	If a person with access permission has their face successfully recognized, the Time & Attendance will prompt face recognition success. You can enter the prompt interval time.

Parameter	Description
Invalid Face Prompt Interval (S)	If a person without access permission attempts to unlock the door for several times in the defined interval, the Time & Attendance will prompt face recognition failure. You can enter the prompt interval time.
Pupillary Distance	Face images require desired pixels between the eyes (called pupillary distance) for successful recognition. The default pixel is 45. The pixel changes according to the face size and the distance between faces and the lens. If an adult is 1.5 meters away from the lens, the pupillary distance can be 50 px-70 px.
Channel Id	1 is for the white light camera and 2 is for the IR light camera.
Exposure (Face)	After face exposure is enabled, human faces will be clearer when the Time & Attendance is installed outdoors.
Face Target Brightness	The default value is 50. Adjust the brightness as needed.
Exposure Time	After a face is detected, the Time & Attendance will give out light to illuminate the face, and the Time & Attendance will not give out light again until the interval you set has passed.
Mask Mode	• **No detect**: Mask is not detected during face recognition. • **Mask reminder**: Mask is detected during face recognition. If the person does not wear a mask, the system will give them a reminder to wear masks, and access is allowed. • **Mask intercept**: Mask is detected during face recognition. If a person is not wearing a mask, the system will give them a reminder to wear masks, and access is denied.
Exposure (QR code)	When the Time & Attendance is installed outdoors, the QR code will be clearer based on the defined QR code brightness when you scan it.
QR code Brightness	
Exposure Time (QR code) (S)	After a QR code is scanned, the Time & Attendance will give out light to illuminate the QR code, and the Time & Attendance will not give out light again until the defined exposure time has passed.
Multi-face Recognition	Supports detecting 4 face images at the same time, and the unlock combinations mode become invalid. The door is unlocked after any one of them gain access.

Step 4 Draw the face detection area.

1. Click **Detect Region**,
2. Right-click to draw the detection area, and then release the left button of the mouse to complete drawing.
   The face in the defined area will be detected.

Step 5 Draw the target size.

1) Click **Draw target**
2) Right-click to draw the face recognition box to define the minimum size of detected face.

Only when the size of the face is larger than the defined size, the face can be detected by the Time & Attendance.

Step 6 Click **OK**.

3.7 Configuring Network

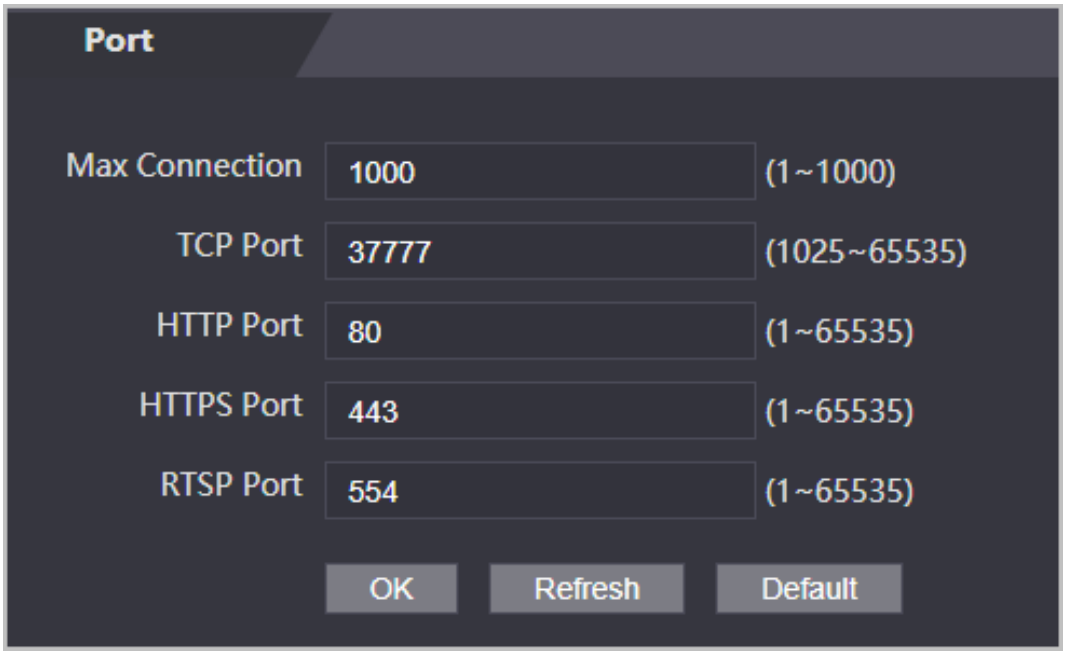
3.7.1 Configuring Port

You can limit access to the Time & Attendance at the same through web, desktop client and phone.

Step 1 Select **Network Setting** > **Port**.

Step 2 Configure port numbers.

Figure 3-9 Configure ports



Except **Max Connection** and **RTSP Port**, you need to restart the Time & Attendance to make the configurations effective after you change other parameters.

Table 3-7 Description of ports

Parameter	Description
Max Connection	You can set the maximum number of clients (such as web, desktop client and phone) that can access the Time & Attendance at the same time.
TCP Port	Default value is 37777.
HTTP Port	Default value is 80. If you want to change the port number, add the new port number after the IP address when you log in to the webpage.
HTTPS Port	Default value is 443.
RTSP Port	Default value is 554.

Step 3 Click **OK**.

3.7.2 Configuring Automatic Registration

The Time & Attendance reports its address to the designated server so that you can get access to the Time & Attendance through the management platform.

Step 1 On the home page, select **Network Setting** > **Register**.

Step 2 Enable the automatic registration function and configure the parameters.

Figure 3-10 Register

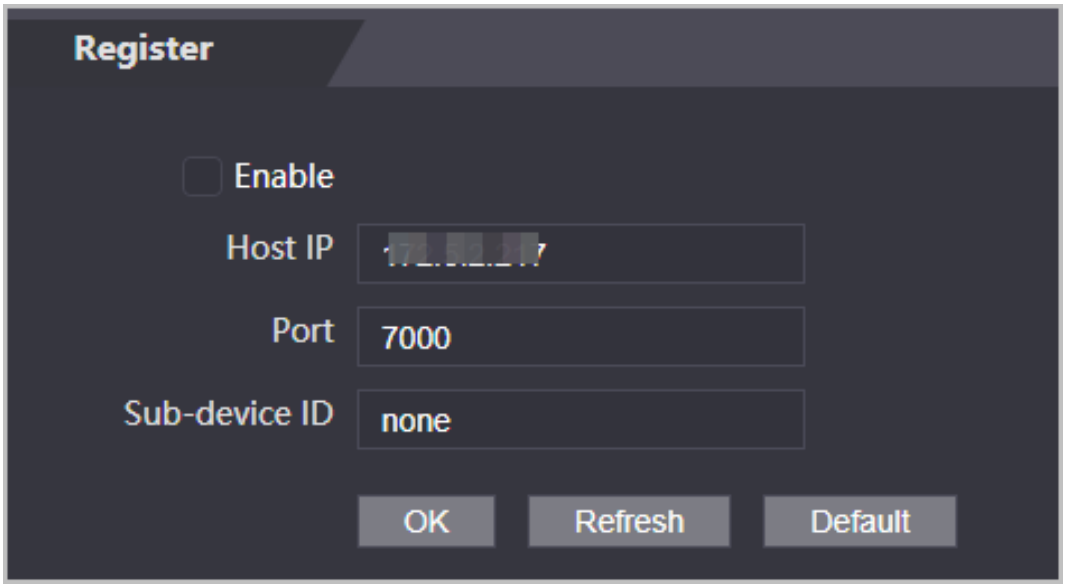


Table 3-8 Automatic registration description

Parameter	Description
Host IP	The IP address or the domain name of the server.
Port	The port of the server used for automatic registration.
Sub-Device ID	Enter the sub-device ID (user defined). When you add the Time & Attendance to the management platform, the sub-device ID on the management platform must conform to the defined sub-device ID on the Time & Attendance.

Step 3 Click **Apply**.

3.8 Safety Management

3.8.1 Configuring IP Authority

Step 1 Log in to the webpage.

Step 2 Click **Safety Mgmt.** > **IP Authority**.

Step 3 Select a cybersecurity mode from the **Type** list.

- **Network Access**: Set allowlist and blocklist to control access to the Time & Attendance.
- **Prohibit PING**: Enable **PING prohibited** function, and the Time & Attendance will not respond to the Ping request.

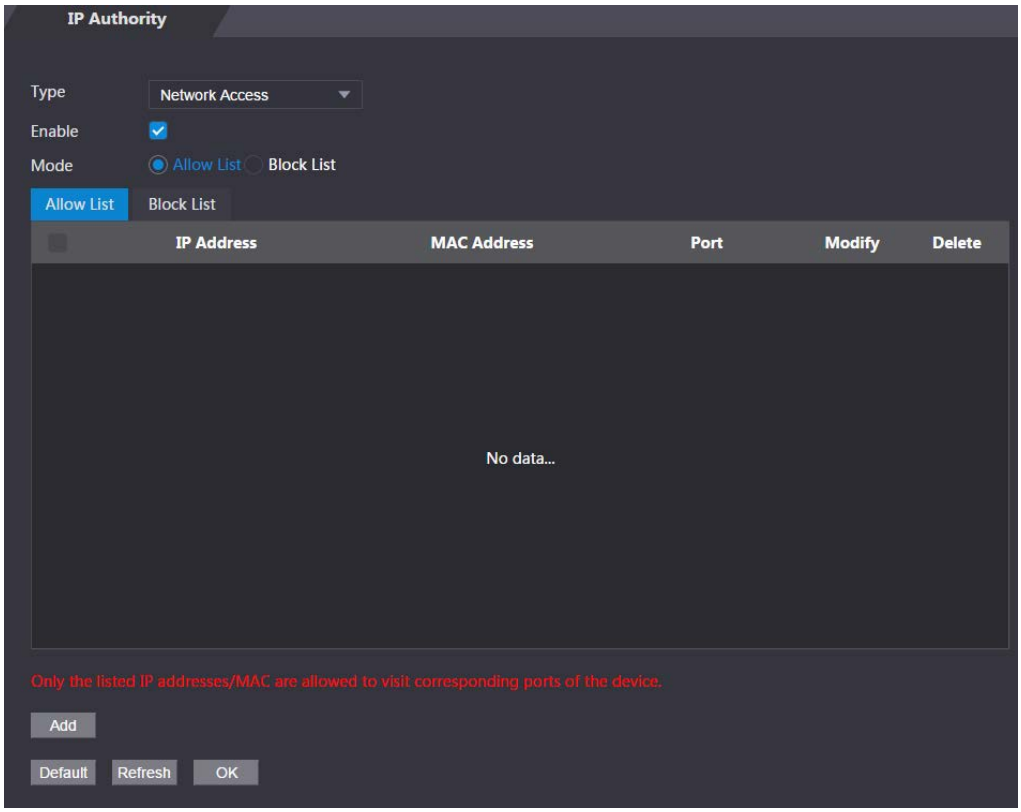
- **Anti Half Connection**: Enable **Anti Half Connection** function, and the Time & Attendance can still function properly under half connection attack.

3.8.1.1 Network Access

Step 1 Select **Network Access** from the **Type** list.

Step 2 Select the **Enable** check box.

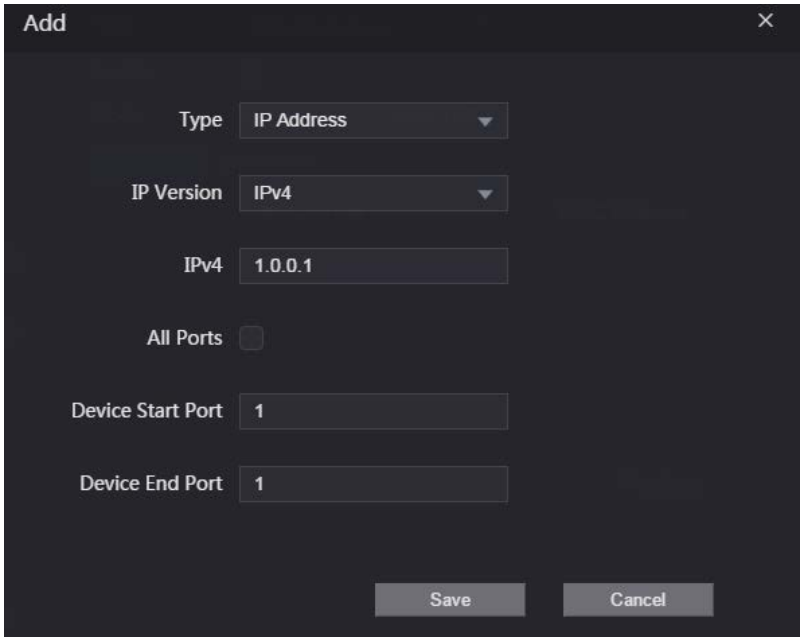
Figure 3-11 Network access



Step 3 Select **Allow List** or **Block List**.

Step 4 Click **Add**.

Figure 3-12 Add IP



Step 5 Configure parameters.

Table 3-9 Description of adding IP parameters

Parameter	Description
Type	Select the address type from the **Type** list.
IP Version	IPv4 by default.
All Ports	Select **All Ports** check box, and your settings will apply to all ports.
Device Start Port	If you clear **All Ports** check box, set the device start port and device end port.
Device End Port	

Step 6 Click **Save**, and the **IP Authority** interface is displayed.

Step 7 Click **OK**.

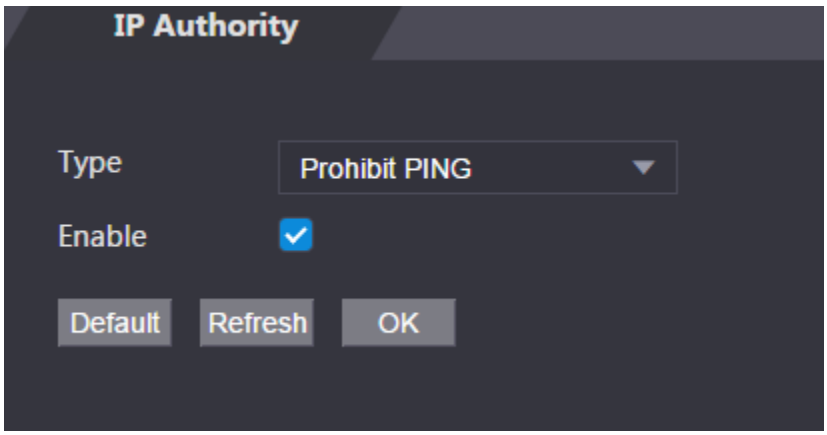
- Click to edit the allowlist or blocklist.
- Click to delete the allowlist or blocklist

3.8.1.2 Prohibit PING

Step 1 Select **Prohibit PING** from the **Type** list.

Step 2 Select the **Enable** check box.

Figure 3-13 Prohibit PING



Step 3 Click **OK**.

3.8.1.3 Anti Half Connection

Step 1 Select the **Anti Half Connection** from the **Type** list.

Step 2 Select the **Enable** check box.

Step 3 Click **OK**.

3.8.2 Configuring System

Step 1 Log in to the web interface.

Step 2 Select **Safety Mgmt.** > **System Service**.

Step 3 Enable or disable the system services as needed.

Figure 3-14 System service

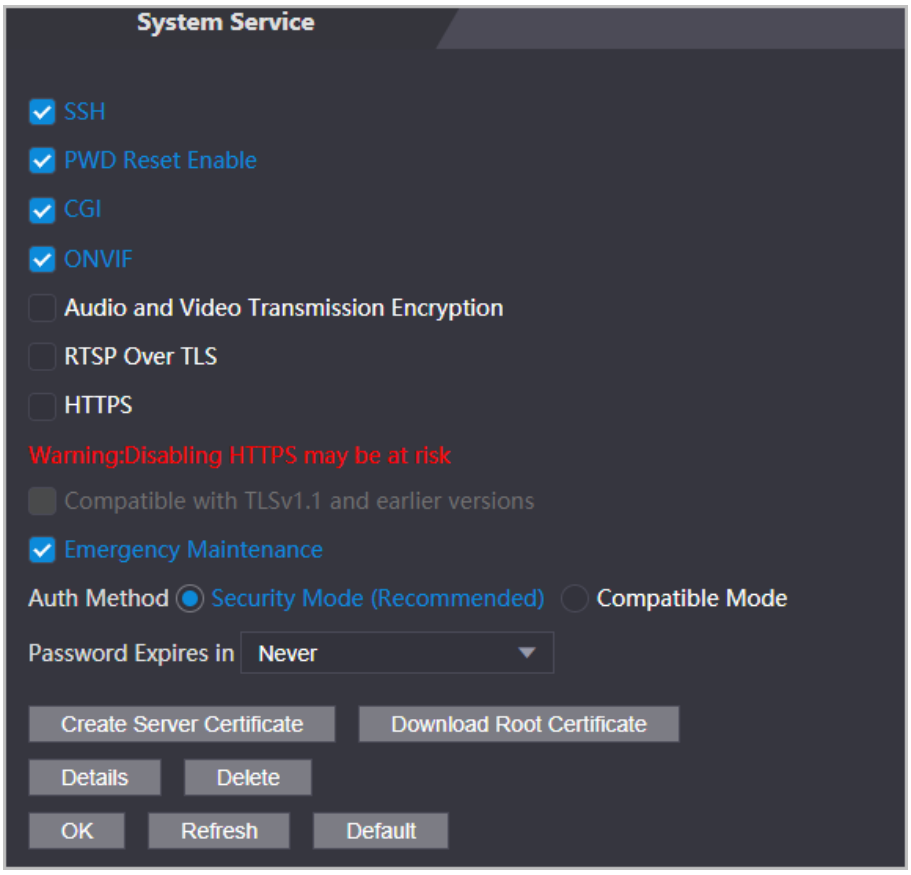


Table 3-10 Description of system service

Parameter	Description
SSH	Secure Shell (SSH) is a cryptographic network protocol for operating network services securely over an unsecured network. When SSH is enabled, SSH provides cryptographic service for the data transmission.
PWD Reset Enable	If enabled, you can reset the password. This function is enabled by default.
CGI	Common Gateway Interface (CGI) offers a standard protocol for web servers to execute programs similarly to console applications running on a server that dynamically generates web pages. When CGI is enabled, CGI commands can be used. The CGI is enabled by default.
ONVIF	Enable other devices to pull the video stream of the VTO via the ONVIF protocol.
Audio and Video Transmission Encryption	If this function is enabled, audio and video transmission is automatically encrypted.
RTSP Over TLS	If this function is enabled, audio and video transmission is encrypted via THE RTSP protocol.
HTTPS	Hypertext Transfer Protocol Secure (HTTPS) is a protocol for secure communication over a computer network. When HTTPS is enabled, HTTPS will be used to access CGI commands; otherwise HTTP will be used.

Parameter	Description
Compatible with TLSv1.1 and earlier versions	Enable this function if your browser is using TLS V1.1 or earlier versions.
Emergency Maintenance	Enable it for faults analysis and maintenance.
Auth Method	We recommend you select the security mode .

Step 4 Click **OK**.

3.8.2.1 Creating Server Certificate

Configure HTTPS server to improve your website security with server certificate.

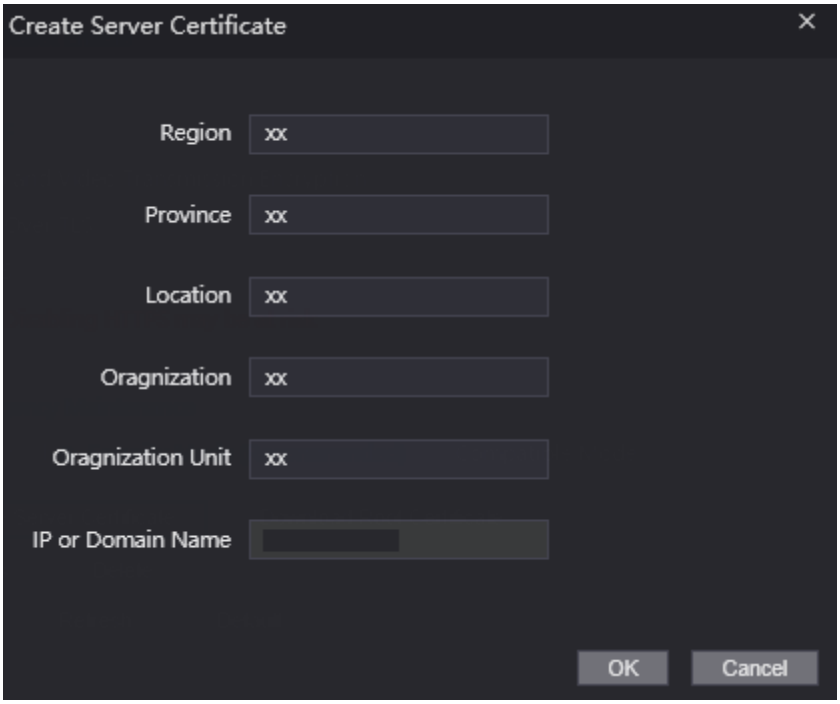
- If you use HTTPS for the first time or the IP address of the Time & Attendance is changed, create a server certificate and install a root certificate.
- If you use another computer to log in to the webpage of the Time & Attendance, you need to download and install the root certificate again on the new computer or copy the root certificate to the it.

Step 1 On the **System Service** page, click **Create Server Certificate**.

Step 2 Enter information and click **OK**.

The Time & Attendance will restart.

Figure 3-15 Create Server Certificate

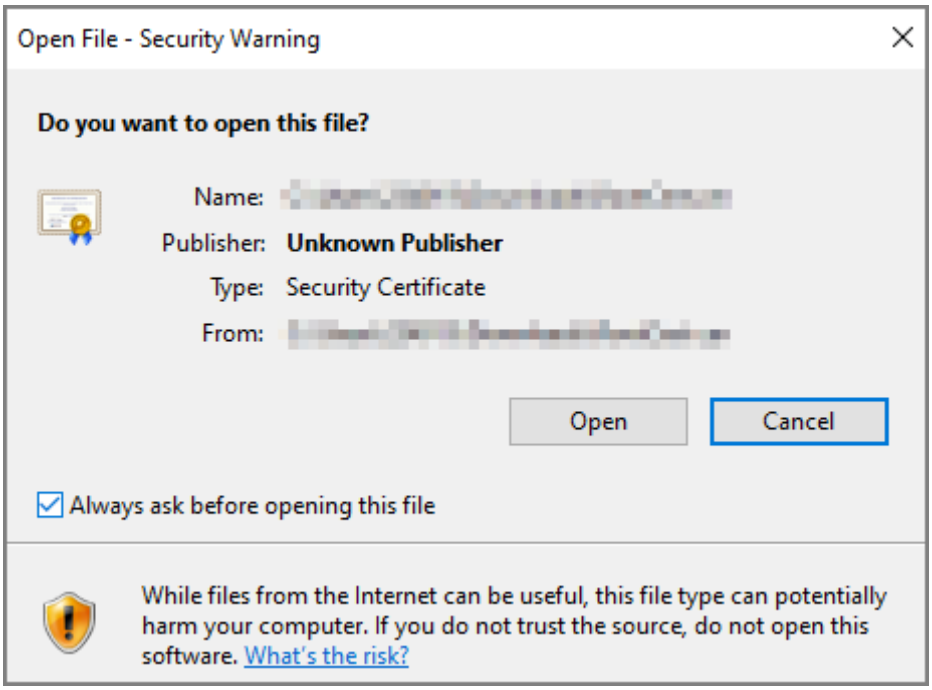


3.8.2.2 Downloading Root Certificate

Step 1 On the **System Service** page, click **Download Root Certificate**.

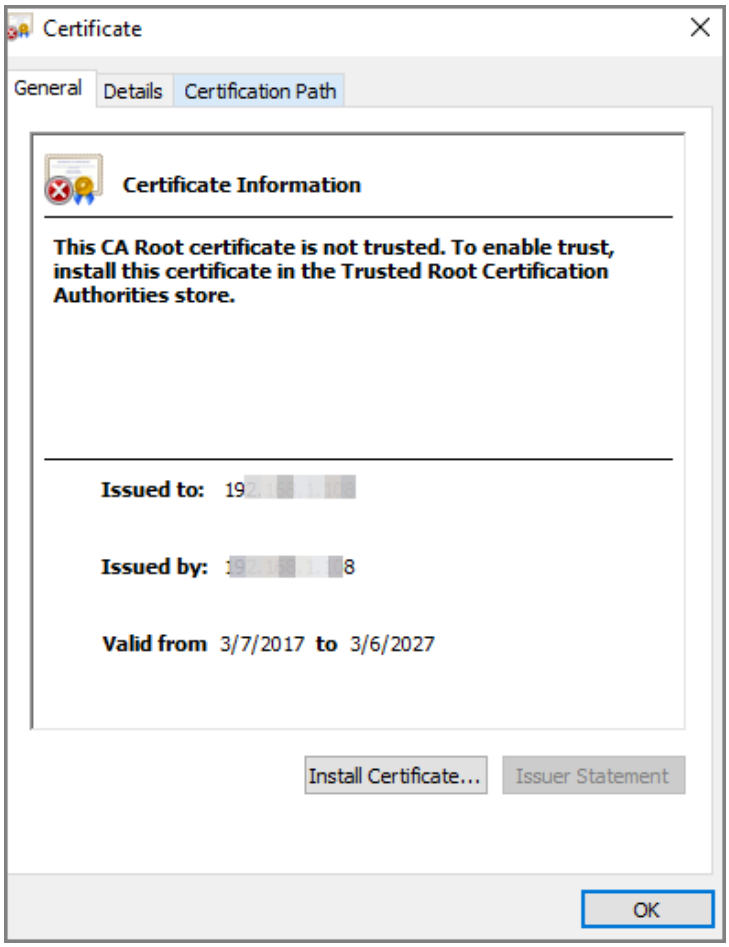
Step 2 Double-click the file that you have downloaded, and then click **Open**.

Figure 3-16 File download



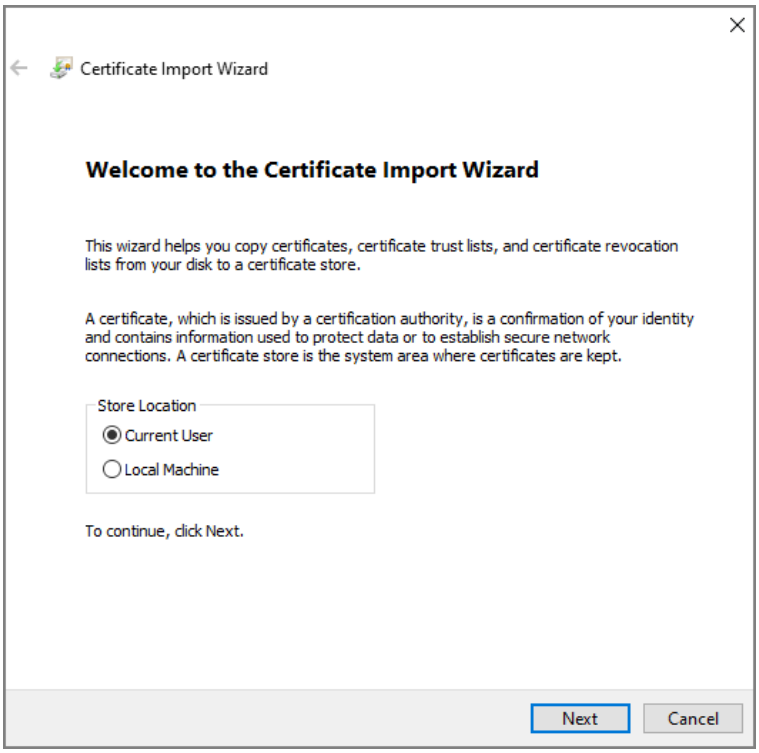
Step 3 Click **Install Certificate**.

Figure 3-17 Certificate information



Step 4 Select **Current User** or **Local Machine**, and then click **Next**.

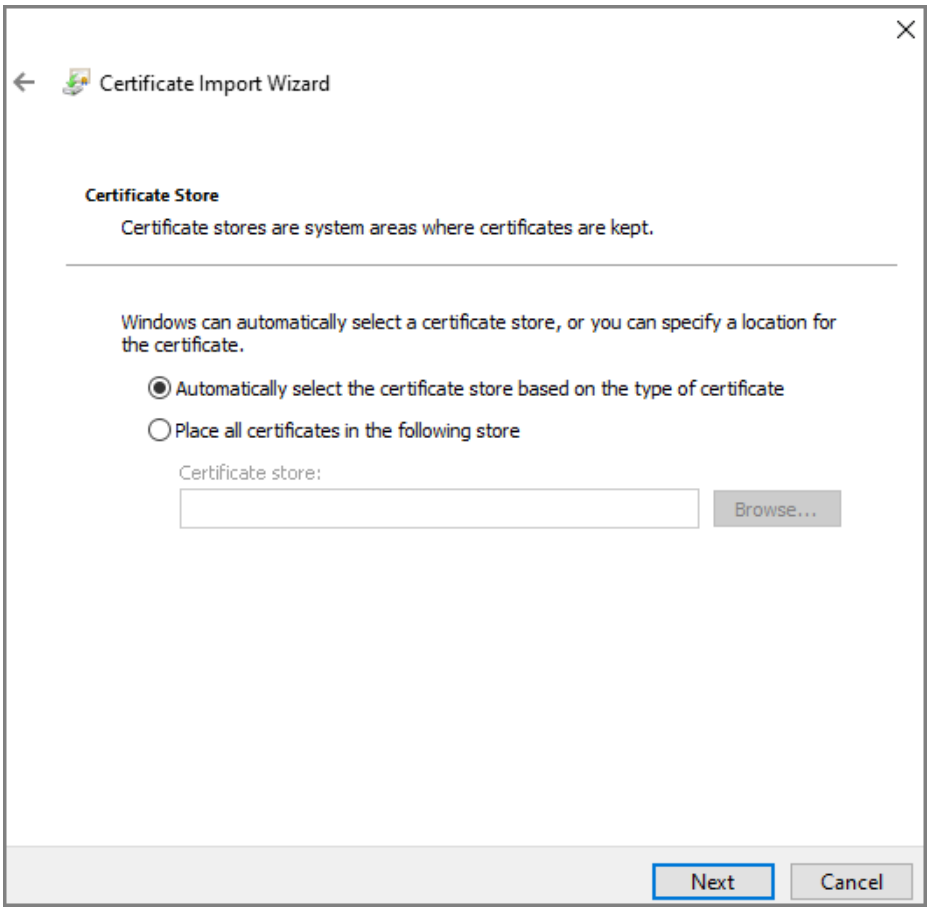
Figure 3-18 Certificate import wizard (1)



Step 5 Select the appropriate storage location.

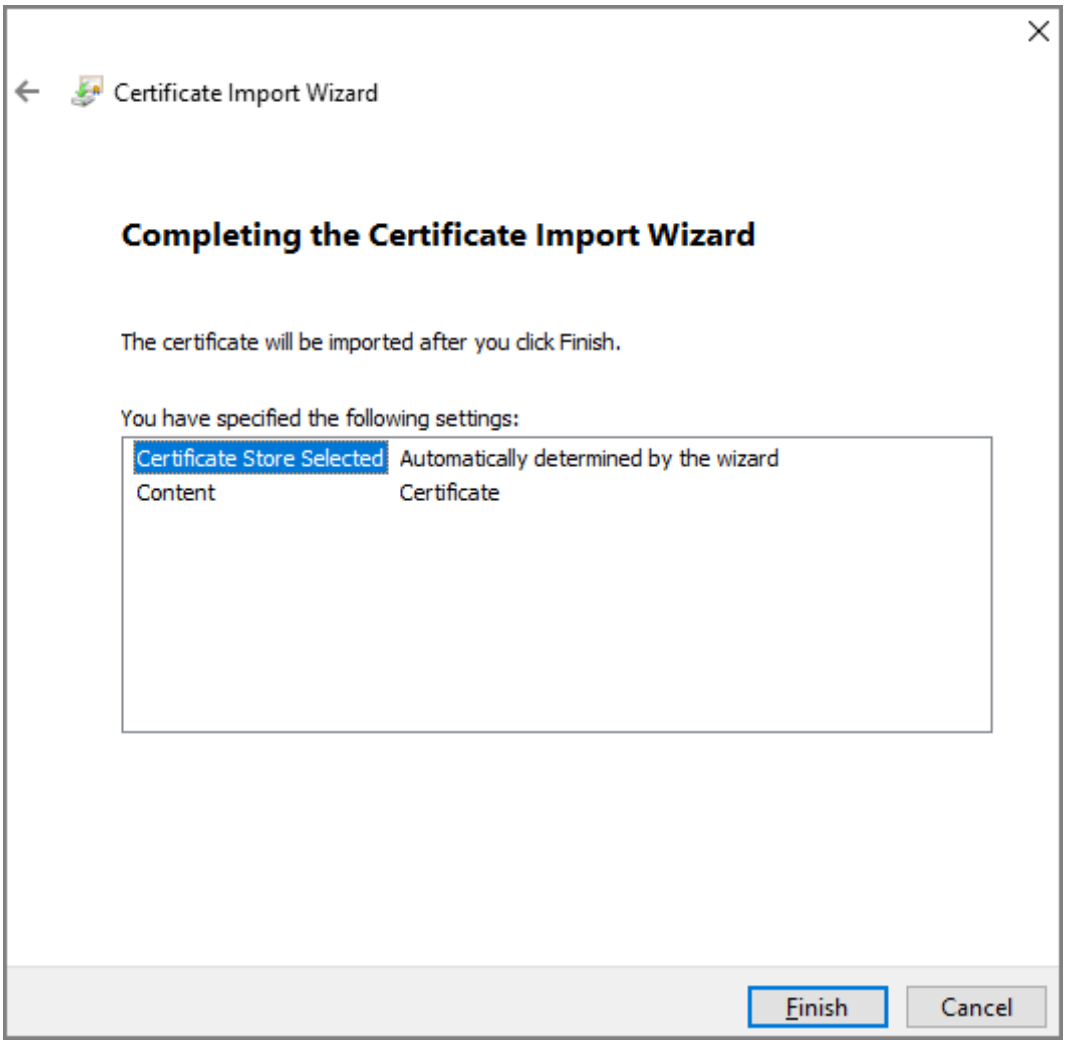
1) Select **Place all certificates in the following store**.
2) Click **Browse** to import the certificate to the **Trusted Root Certification Authorities** store, and then click **Next**.

Figure 3-19 Certificate Import Wizard (2)



Step 6 Click **Finish**.

Figure 3-20 Certificate import wizard (3)



3.9 User Management

You can add or delete users, change users' passwords, and enter an email address for resetting the password when you forget your password.

3.9.1 Adding Users

You can add new users and then they can log in to the webpage of the Time & Attendance.

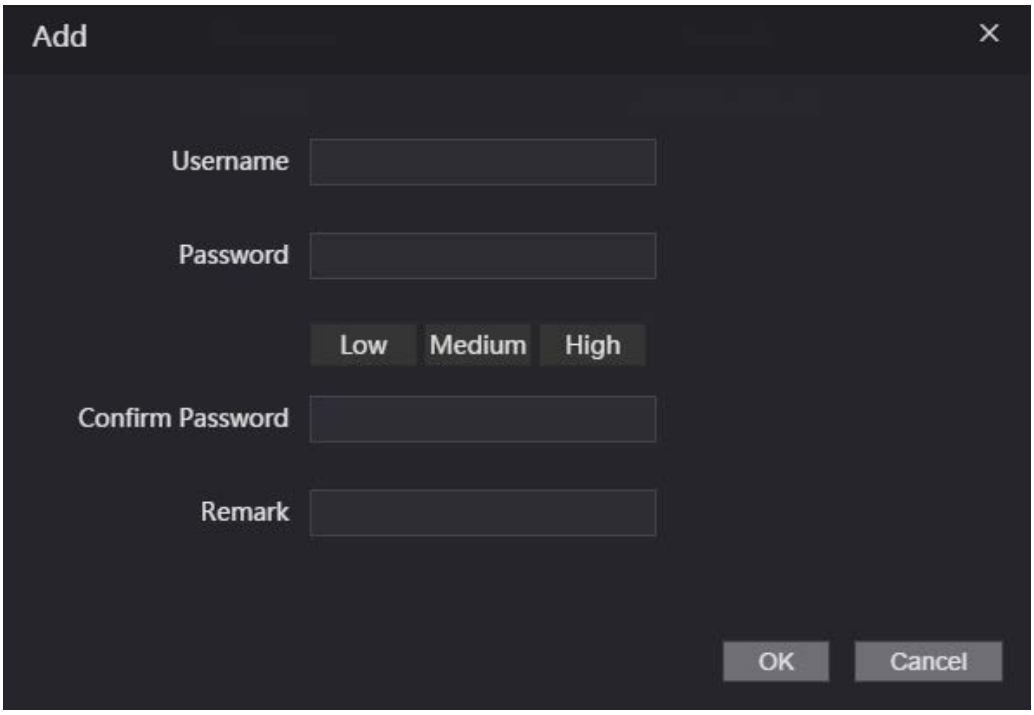
Procedure

Step 1 On the home page, select **User Mgmt.** > **User Mgmt.**.

Step 2 Click **Add**, and enter the user information.

- The username cannot be the same with existing account. The username consists of up to 31 characters and only allows for numbers, letters, underscores, midlines, dots, or @.
- The password must consist of 8 to 32 non-blank characters and contain at least two types of the following characters: Upper case, lower case, numbers, and special characters (excluding ' " ; : &).
  Set a high-security password by following the password strength prompt.

Figure 3-21 Add user



Step 3 Click **OK**.

Only admin account can change password and admin account cannot be deleted.

3.9.2 Adding ONVIF Users

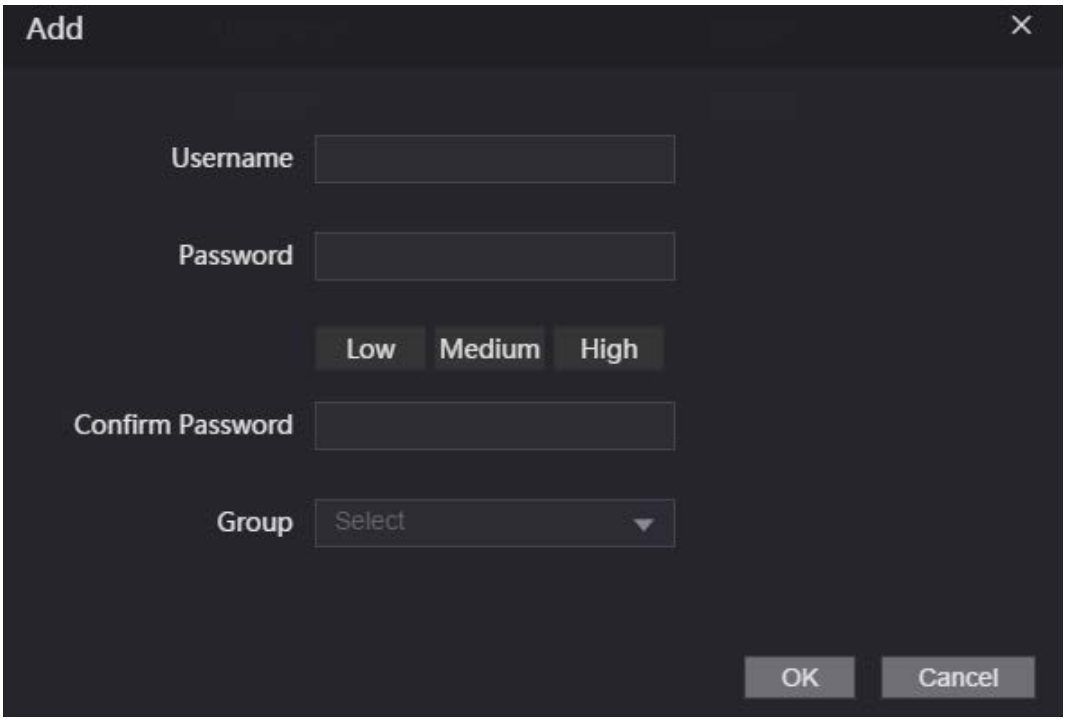
Open Network Video Interface Forum (ONVIF), a global and open industry forum that is established for the development of a global open standard for the interface of physical IP-based security products, which allows the compatibility from different manufactures. ONVIF users have their identities verified through ONVIF protocol. The default ONVIF user is admin.

Procedure

Step 1 On the home page, select **User Mgmt.** > **Onvif User**.

Step 2 Click **Add** and then configure parameters.

Figure 3-22 Add ONVIF user



Step 3 Click **OK**.

3.9.3 Viewing Online Users

You can view online users who currently log in to the webpage.

On the home page, select **Online User**.

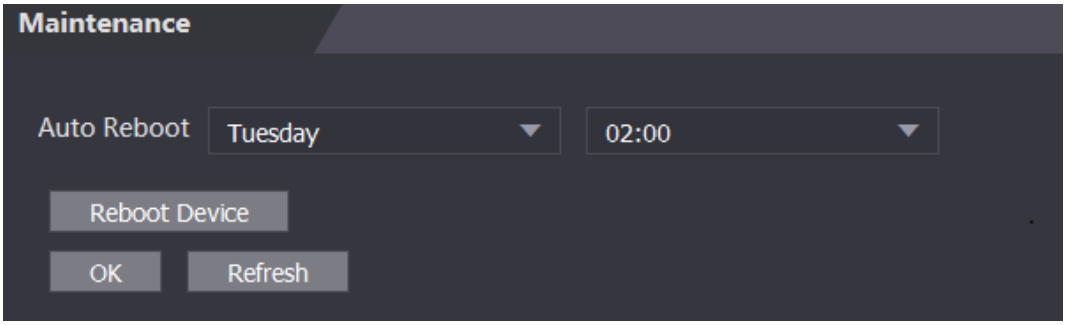
3.10 Maintenance

You can regularly restart the Time & Attendance during the idle time to improve its performance.

Step 1 Log in to the webpage.

Step 2 Select **Maintenance**.

Figure 3-23 Maintenance



Step 3 Set the time, and then click **OK**.

Step 4 (Optional) Click **Reboot Device**, the Time & Attendance will restart immediately.

3.11 Configuration Management

When more than one Time & Attendance need the same configurations, you can configure parameters for them by importing or exporting configuration files.

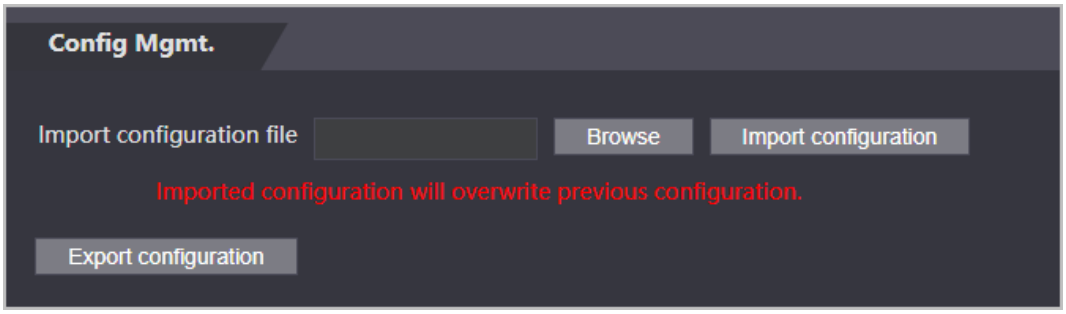
3.11.1 Exporting/Importing Configuration Files

You can import or export the configuration file of the Time & Attendance. When you want to apply the same configurations to multiple devices, you can import the configuration file to them.

Step 1 Log in to the webpage.

Step 2 Select **Config Mgmt.** > **Config Mgmt.**.

Figure 3-24 Configuration management



Step 3 Export or import configuration files.

- Export configuration file.
  Click **Export Configuration** to download the file to the local.

  IP will not be exported.
- Import configuration file.
  1. Click **Browse** to select the configuration file.
  2. Click **Import configuration**.

     Configuration file can only be imported to the device with the same model.

3.11.2 Restoring Factory Defaults

Restoring the **Time & Attendance** to default configurations will cause data loss. Please be advised.

Step 1 Select **Config Mgmt.** > **Default**

Step 2 Restore factory defaults if necessary.

- **Restore Factory**: Resets configurations of the Time & Attendance and delete all data.
- **Restore Factory (Save user & log)**: Resets configurations of the Time & Attendance and deletes all data except for user information and logs.

3.12 Upgrading System



- Use the correct update file. Make sure you get the correct update file from the technical support.
- Do not disconnect the power supply or network, or restart or shut down the Time & Attendance during the update.

3.12.1 File Update

Step 1 On the home page, select **Upgrade**.

Step 2 In the **File Upgrade** area, click **Browse**, and then upload the update file.



The upgrade file should be a .bin file.

Step 3 Click **Update**.

The Time & Attendance will restart after update completes.

3.12.2 Online Update

Step 1 On the home page, select **Upgrade**.

Step 2 In the **Online Upgrade** area, select an update method.

- Select **Auto Check**, the Time & Attendance will automatically check whether the its latest version is available.
- Select **Manual Check**, and you can immediately check whether the latest version is available.

Step 3 Update the Time & Attendance when the latest version is available.

3.13 Viewing Version Information

On the home page, select **Version Info**, and you can view version information, such as device model, serial number, hardware version, legal information and more.

3.14 Viewing Logs

View logs such as system logs, admin logs, and unlock records.

3.14.1 System Logs

View and search for system logs.

Step 1 Log in to the webpage.

Step 2 Select **System Log** > **System Log**.

Step 3 Select the time range and the log type, and then click **Query**.

Click **Backup** to download the system log.

3.14.2 Admin Logs

Search for admin logs by using admin ID.

Step 1 Log in to the webpage.

Step 2 Select **System Log** > **Admin Log**.

Step 3 Enter the admin ID, and then click **Query**.

3.14.3 Attendance Logs

Search for time attendance records and export them.

Step 1 Log in to the webpage.

Step 2 Select **System Log** > **Search Records**.

Step 3 Select the time range and the log type, and then click **Query**.

You can click **Export Data** to download the log.



Face images will not be exported.

4 Smart PSS Lite Configuration

This section introduces how to manage and configure the Time & Attendance through Smart PSS Lite. You can also configure time attendance rules on the platform, such as shifts, modes, schedules and more. For details, see the user's manual of Smart PSS Lite.

4.1 Installing and Logging In

Install and log in to Smart PSS Lite. For details, see the user manual of Smart PSS Lite.

Step 1 Get the software package of the Smart PSS Lite from the technical support, and then install and run the software according to instructions.

Step 2 Initialize Smart PSS Lite when you log in for the first time, including setting password and security questions.



Set the password is for the first-time use, and then set security questions to reset your password when you forgot it.

Step 3 Enter your username and password to log in to Smart PSS Lite.

4.2 Adding Devices

You need to add the Time & Attendance to Smart PSS Lite. You can add them in batches or individually.

4.2.1 Adding Individually

You can add Time & Attendance individually by entering their IP addresses or domain names.

Step 1 Log in to Smart PSS Lite.

Step 2 Click **Device Manager** and click **Add**.

Step 3 Enter the device information.

Figure 4-1 Device information

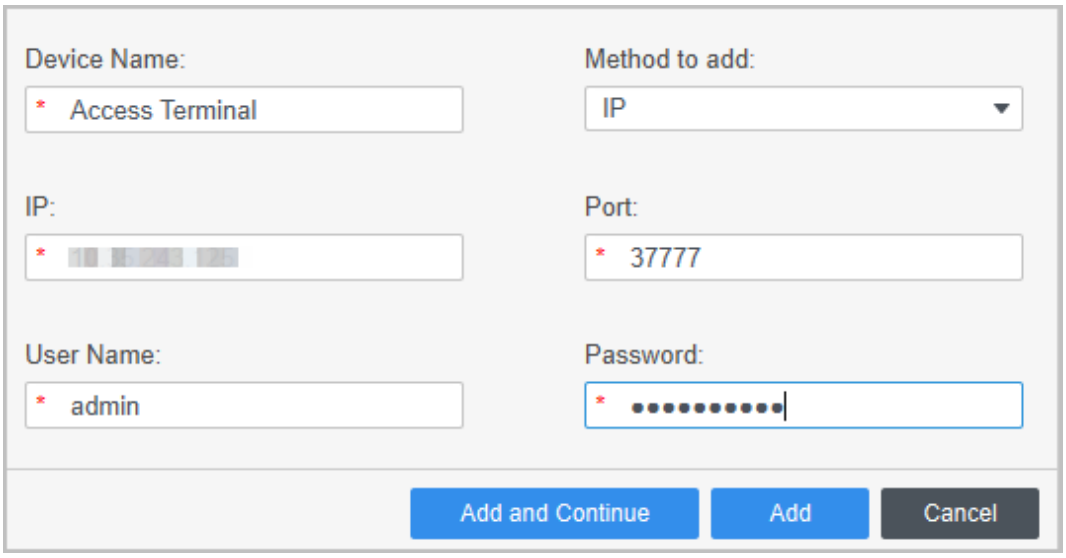


Table 4-1 Device parameters Description

Parameter	Description
Device Name	Enter a name of the Time & Attendance. We recommend you name it after its installation area.
Method to add	Select **IP** to add the Access Terminal by entering its IP Address.
IP	Enter IP address of the Time & Attendance.
Port	The port number is 37777 by default.
User Name/Password	Enter the username and password of the Access Terminal.

Step 4 Click **Add**.

The added Time & Attendance displays on the **Devices** page. You can click **Add and Continue** to add more Time & Attendances.

4.2.2 Adding in Batches

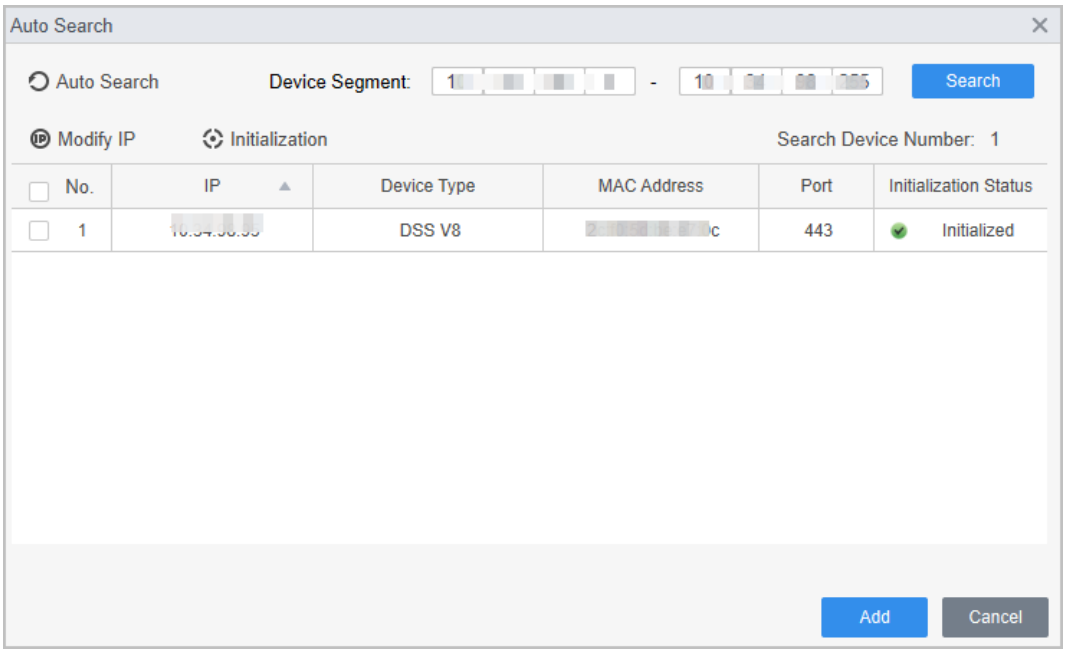
We recommend you use the auto-search function when you add want to Time & Attendances in batches. Make sure the Time & Attendances you add must be on the same network segment.

Step 1 Log in to Smart PSS Lite.

Step 2 Click **Device Manager** and search for devices.

- Click **Auto Search**, to search for devices on the same LAN.
- Enter the network segment range, and then click **Search**.

Figure 4-2 Auto search



A device list will be displayed.

Select a device, and then click **Modify IP** to modify its IP address.

Step 3 Select the Time & Attendance that you want to add to Smart PSS Lite, and then click **Add**.

Step 4 Enter the username and the password of the Time & Attendance.

You can view the added Time & Attendance on the **Devices** page.

The Time & Attendance automatically logs in to Smart PSS Lite after being added. **Online** is displayed after successful login.

4.3 User Management

Add users, assign cards to them, and configure their access permissions.

4.3.1 Configuring Card Type

Set the card type before you assign cards to users. For example, if the assigned card is an ID card, set card type to ID card.

Step 1 Log in to Smart PSS Lite.

Step 2 Click **Access Solution** > **Personnel Manager** > **User**.

Step 3 On the **Card Issuing Type** and then select a card type.

Make sure that the card type is same to the actually assigned card; otherwise, the card number cannot be read.

Step 4 Click **OK**.

4.3.2 Adding Users

4.3.2.1 Adding Individually

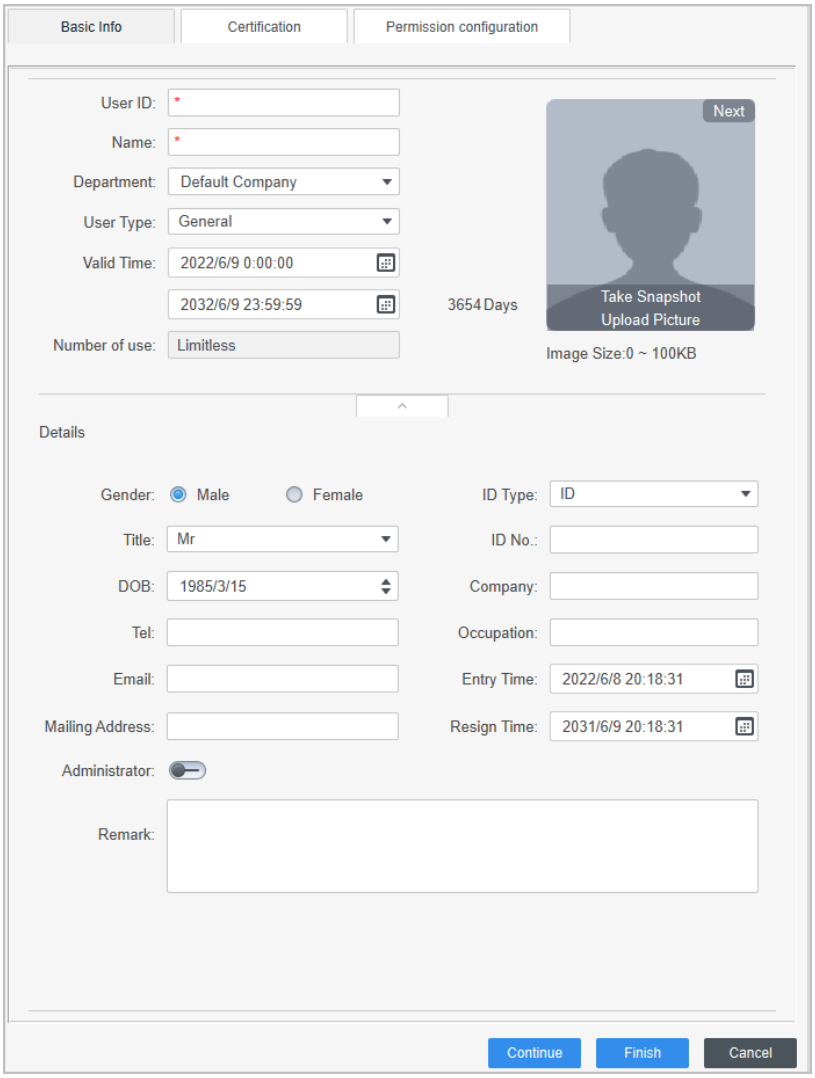
You can add users individually.

Step 1 Log in to Smart PSS Lite.

Step 2 Click **Access Solution** > **Personnel Manger** > **User** > **Add**.

Step 3 Click **Basic Info** tab, and enter the basic information of the user, and then import the face image.

Figure 4-3 Add basic information



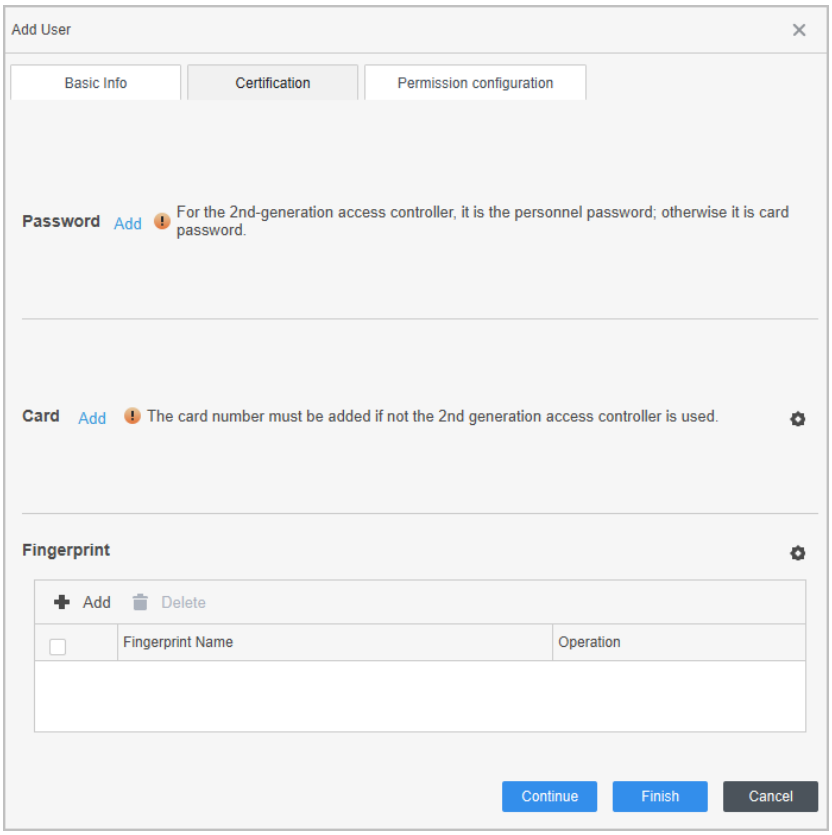
Step 4 Click the **Certification** tab to add certification information of the user.

- Configure password: The password must consist of 6–8 digits.
- Configure card: The card number can be read automatically or entered manually. To read the card number automatically, select a card reader, and then place the card on the card reader.
  1. On the **Card** area, click and select **Card issuer**, and then click **OK**.
  2. Click **Add**, swipe a card on the card reader.
     The card number is displayed.
  3. Click **OK**.

After adding a card, you can set the card to main card or duress card, or replace the card with a new one, or delete the card.

- Configure fingerprint.
  1. On the **Fingerprint** area, click and select **Fingerprint Scanner**, and then click **OK**.
  2. Click **Add Fingerprint**, press your finger on the scanner three times in a row.

Figure 4-4 Add password, card, and fingerprint



Step 5 Configure permissions for the user. For details, see #d894e6a1026.

Step 6 Click **Finish**.

4.3.2.2 Adding in Batches

You can add users in batches.

Step 1 Log in to Smart PSS Lite.

Step 2 Click **Personnel Manger** > **User** > **Batch Add**.

Step 3 Select **Card issuer** from the **Device** list, and then configure the parameters.

Figure 4-5 Add users in batches

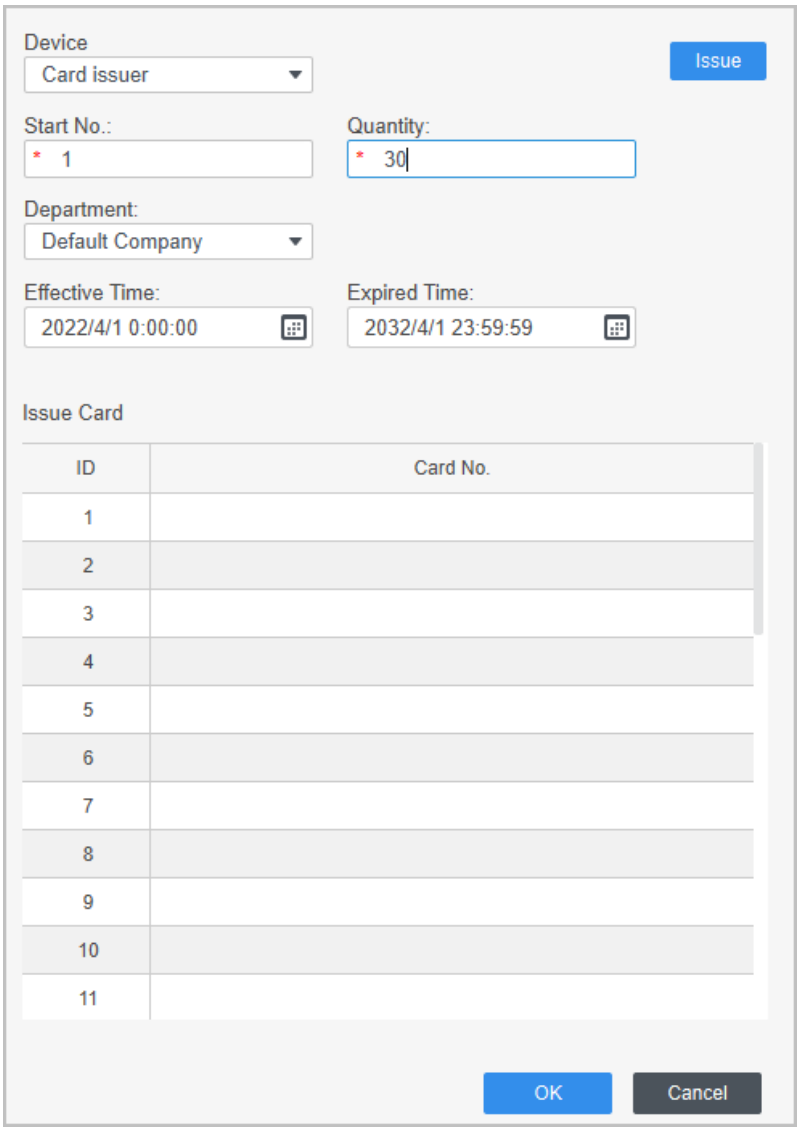


Table 4-2 Add users in batches parameters

Parameter	Description
Start No.	The user ID starts with the number you defined.
Quantity	The number of users you want to add.
Department	Select the department that the user belongs to.
Effective Time/Expired Time	The users can unlock the door within the defined period.

Step 4 Click **Issue**.

The card number will be read automatically.

Step 5 Click **OK**.

Step 6 On the **User** page, click to complete user information.

4.3.3 Assigning Attendance Permissions

Create a permission group that is a collection of time attendance permissions, and then associate employees with the group so that they can punch in/out through defined verification methods.

Step 1 Log in to the Smart PSS Lite.

Step 2 Click **Access Solution** > **Personnel Manger** > **Permission configuration**.

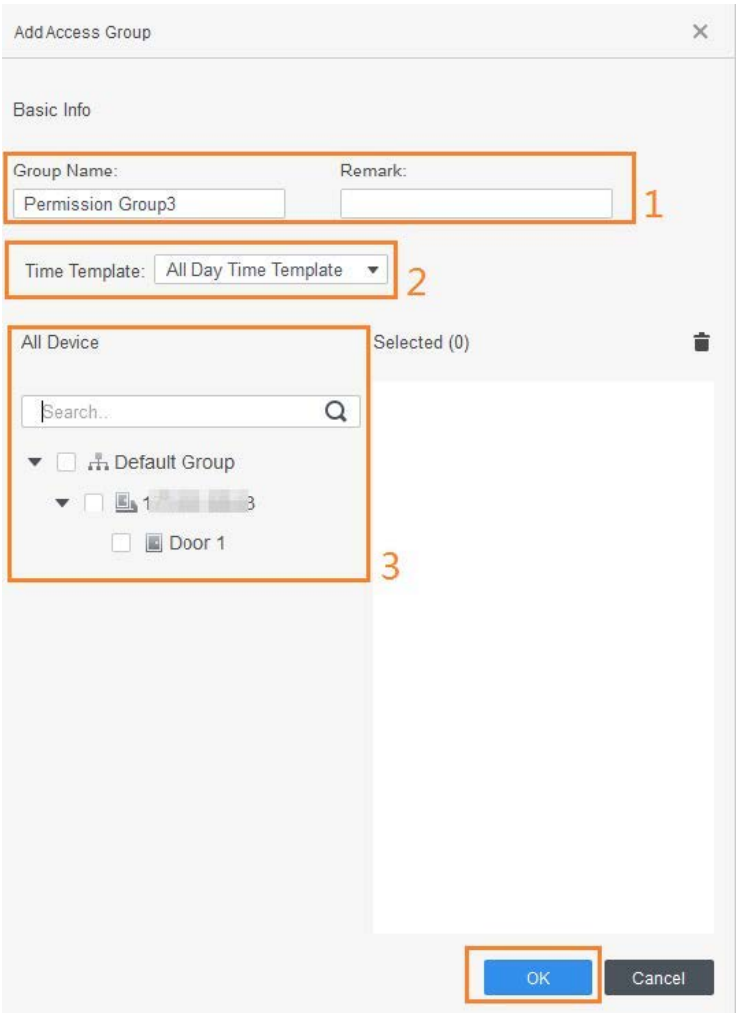
Step 3 Click ＋ .

Step 4 Enter the group name, remarks (optional), and select a time template.

Step 5 Select the access control device.

Step 6 Click **OK**.

Figure 4-6 Create a permission group

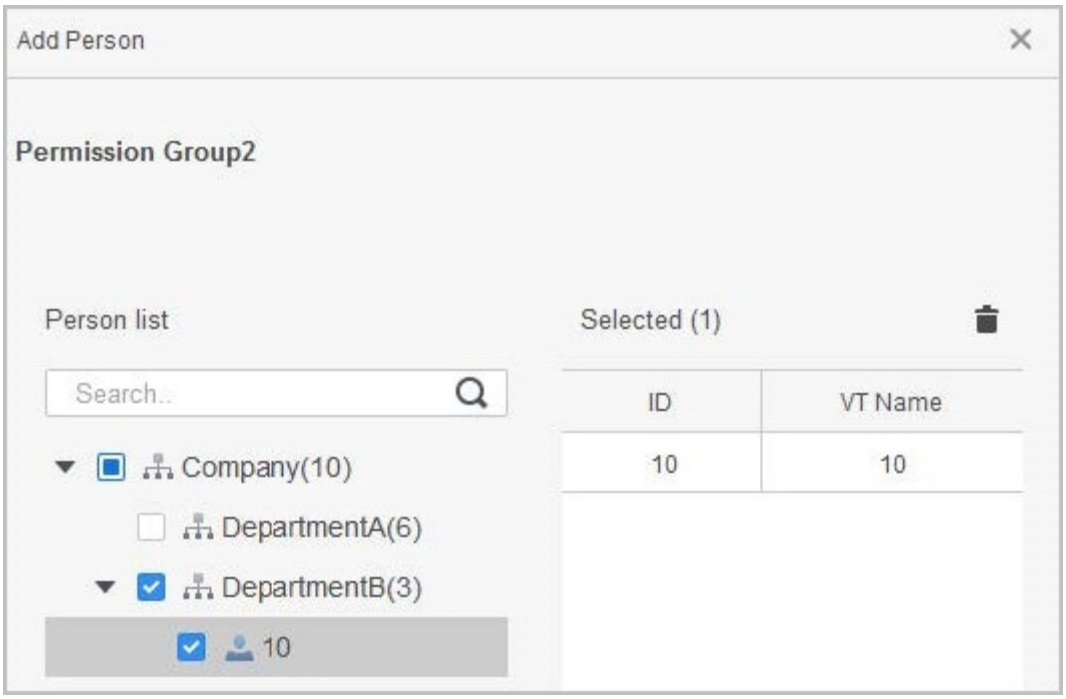


The Time & Attendance only supports punch-in/out through password and face attendance.

Step 7 Click of the permission group you added.

Step 8 Select users to associate them with the permission group.

Figure 4-7 Add users to a permission group



Step 9 Click **OK**.

Appendix 1 Important Points of Face Registration

Before Registration

- Glasses, hats, and beards might influence face recognition performance.
- Do not cover your eyebrows when wearing hats.
- Do not change your beard style greatly if you use the Time & Attendance; otherwise face recognition might fail.
- Keep your face clean.
- Keep the Time & Attendance at least two meters away from light source and at least three meters away from windows or doors; otherwise backlight and direct sunlight might influence face recognition performance of the Time & Attendance.

During Registration

- You can register faces through the Time & Attendance or through the platform. For registration through the platform, see the platform user manual.
- Make your head center on the photo capture frame. The face image will be captured automatically.

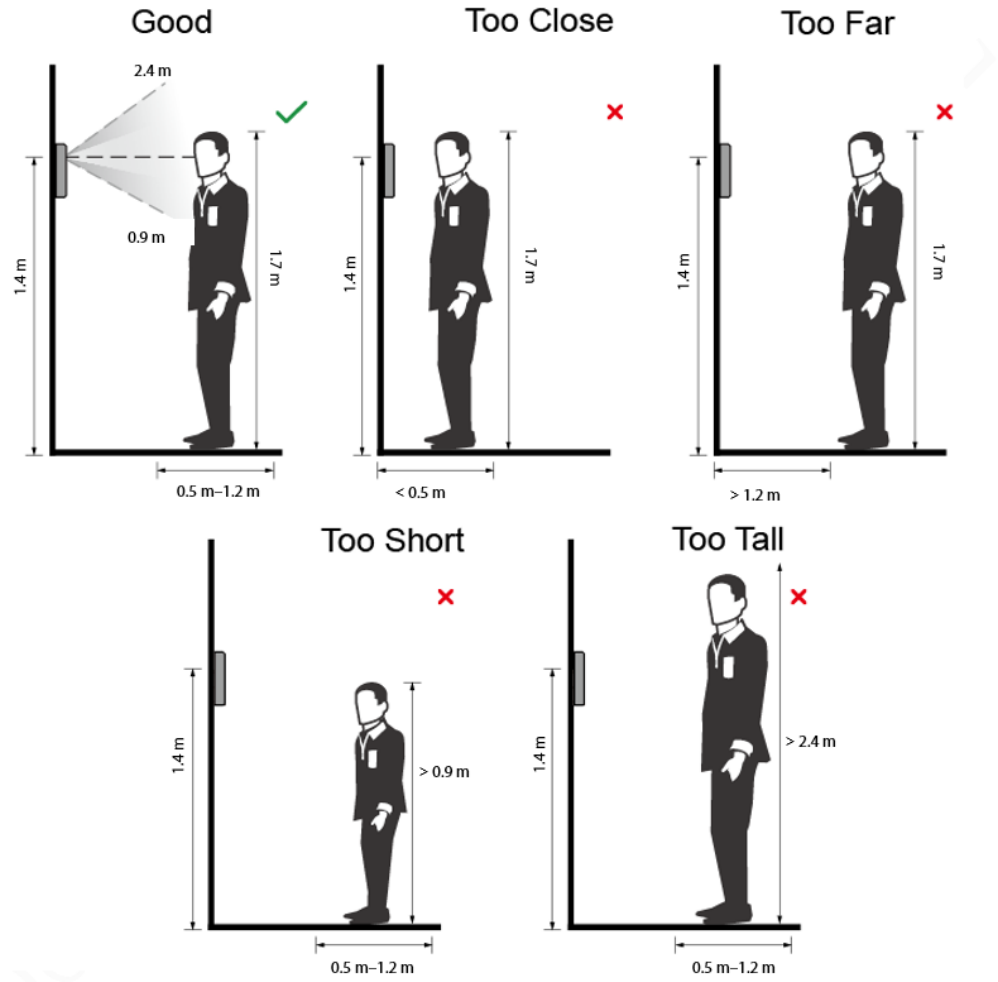


- Do not shake your head or body, otherwise the registration might fail.
- Avoid two faces appear in the capture frame at the same time.

Face Position

If your face is not at the appropriate position, face recognition accuracy might be affected.

Appendix Figure 1-1 Appropriate face position



Requirements of Faces

- Make sure that the face is clean and forehead is not covered by hair.
- Do not wear glasses, hats, heavy beards, or other face ornaments that influence face image recording.
- With eyes open, without facial expressions, and make your face toward the center of camera.
- When recording your face or during face recognition, do not keep your face too close to or too far from the camera.

Appendix Figure 1-2 Head position



Appendix Figure 1-3 Face distance



- When importing face images through the management platform, make sure that image resolution is within the range 150 × 300 pixels–600 × 1200 pixels; image pixels are more than 500 × 500 pixels; image size is less than 100 KB, and image name and person ID are the same.
- Make sure that the face takes up more than 1/3 but no more than 2/3 of the whole image area, and the aspect ratio does not exceed 1:2.

Appendix 2 Cybersecurity Recommendations

Mandatory actions to be taken for basic device 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 device (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 device 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 device network security:

1. **Physical Protection**

   We suggest that you perform physical protection to device, especially storage devices. For example, place the device 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 device (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 device 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. **MAC Address Binding**

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

8. **Assign Accounts and Privileges Reasonably**

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

9. **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.

10. 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.

11. Secure Auditing

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

12. Network Log

Due to the limited storage capacity of the device, 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.

13. Construct a Safe Network Environment

In order to better ensure the safety of device 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.
- Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.