

Attendance Standalone

User Manual



V1.1.0

Foreword

General

This manual introduces the functions and operations of the Attendance Standalone (hereinafter referred to as the Device). 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
V1.1.0	Updated content.	December 2025
V1.0.0	First release.	August 2024

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, audio, 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.

Table of Contents

Foreword.....	I
1 Product Overview.....	1
2 Local Operations.....	2
2.1 Keypad Introduction.....	2
2.2 Initialization.....	4
2.3 Powering On.....	5
2.4 Unlocking Methods.....	5
2.4.1 Unlocking by Cards.....	5
2.4.2 Unlocking by Fingerprints.....	5
2.4.3 Unlocking by User Password.....	6
2.4.4 Unlocking by Public Password.....	6
2.5 Creating Administrator Account.....	7
2.6 Logging In.....	7
2.7 User Management.....	8
2.7.1 Adding Users.....	8
2.7.2 User/Admin List.....	10
2.7.3 Configuring Public Password.....	11
2.8 Access Control Management.....	11
2.8.1 Configuring Unlock Combinations.....	12
2.8.2 Configuring Alarms.....	12
2.8.3 Configuring Lock Status.....	13
2.8.4 Configuring the Verification Time Interval.....	14
2.8.5 Managing Main Cards.....	14
2.8.6 Configuring PIN Code Authentication.....	15
2.9 Attendance Management.....	15
2.9.1 Configuring Departments.....	15
2.9.2 Configuring Shifts.....	16
2.9.3 Configuring Holiday.....	17
2.9.4 Configuring Work Schedules.....	18
2.9.5 Configuring Network Attendance.....	19
2.9.6 Configuring Attendance Modes.....	20
2.9.7 Using Attendance for Lock.....	20
2.10 Communication Settings.....	21
2.10.1 Configuring the IP Address.....	21
2.10.2 Configuring Wi-Fi.....	22
2.10.3 Configuring Wi-Fi AP.....	22
2.11 System Settings.....	23

2.11.1	Configuring Time.....	23
2.11.2	Configuring the Volume.....	24
2.11.3	Configuring the Language.....	25
2.11.4	Configuring Screen Parameters.....	25
2.11.5	Configuring Ringtone.....	26
2.11.6	Managing Device Password.....	26
2.11.7	Restoring Factory Defaults.....	27
2.11.8	Restarting the Device.....	27
2.12	USB Management.....	27
2.12.1	Exporting to USB.....	28
2.12.2	Importing from USB.....	28
2.12.3	Updating the System.....	29
2.13	Record Management.....	29
2.14	System Information.....	29
2.14.1	Viewing Data Capacity.....	29
2.14.2	Viewing Device Version.....	29
3	Webpage Operations.....	30
3.1	Initialization.....	30
3.2	Resetting the Password.....	30
3.3	Home Page.....	31
3.4	Access Monitoring.....	32
3.5	Person Management.....	33
3.6	Configuring Attendance.....	37
3.6.1	Configuring Departments.....	37
3.6.2	Configuring Shifts.....	37
3.6.3	Configuring Holiday.....	40
3.6.4	Configuring Work Schedules.....	41
3.6.5	Configuring Attendance Mode.....	43
3.7	Configuring Access Control.....	45
3.7.1	Configuring Access Control Parameters.....	45
3.7.2	Configuring Alarms.....	49
3.7.3	Configuring Alarm Event Linkage.....	51
3.7.4	Card Settings.....	52
3.7.5	Configuring Periods.....	54
3.8	Audio.....	57
3.8.1	Configuring Audio Parameters.....	57
3.8.2	Managing Audio Files.....	59
3.9	Communication Settings.....	59
3.9.1	Configuring TCP/IP.....	60
3.9.2	Configuring Wi-Fi.....	61

3.9.3	Configuring Wi-Fi AP.....	62
3.9.4	Configuring Port.....	63
3.9.5	Configuring Basic Service.....	64
3.9.6	Configuring Cloud Service.....	66
3.9.7	Configuring SDK Auto Registration.....	67
3.9.8	Configuring CGI Auto Registration.....	68
3.9.9	Configuring Auto Upload.....	69
3.10	Configuring the System.....	70
3.10.1	User Management.....	70
3.10.2	Viewing Online Users.....	73
3.10.3	Configuring Time.....	73
3.10.4	Configuring Ringtone.....	75
3.10.5	Configuring Always On.....	75
3.11	Maintenance Center.....	76
3.11.1	One-click Diagnosis.....	76
3.11.2	System Information.....	77
3.11.3	Data Capacity.....	77
3.11.4	Viewing Logs.....	77
3.11.5	Maintenance Management.....	79
3.11.6	Updating the System.....	80
3.11.7	Advanced Maintenance.....	81
3.12	Security Settings (Optional)	82
3.12.1	Security Status.....	82
3.12.2	Configuring System Service.....	83
3.12.3	Attack Defense.....	83
3.12.4	Installing Device Certificate.....	86
3.12.5	Installing the Trusted CA Certificate.....	89
3.12.6	Security Warning.....	90
3.12.7	Security Authentication.....	91
4	Phone Operations.....	92
4.1	Logging in to the Webpage.....	92
4.2	Home Page.....	93
4.3	Person Management.....	95
4.4	Configuring the System.....	98
4.4.1	Viewing Version Information.....	99
4.4.2	Maintenance.....	99
4.4.3	Configuring Time.....	99
4.4.4	Data Capacity.....	101
4.4.5	Configuring Ringtone.....	101
4.4.6	Language.....	102

4.5	Configuring Attendance.....	102
4.5.1	Configuring Departments.....	102
4.5.2	Configuring Shifts.....	104
4.5.3	Configuring Holiday.....	107
4.5.4	Configuring Work Schedules.....	107
4.5.5	Configuring Attendance Mode.....	109
4.6	Configuring Access Control.....	110
4.6.1	Configuring Unlock Methods.....	110
4.6.2	Configuring Access Control Parameters.....	111
4.6.3	Configuring Alarms.....	114
4.6.4	Configuring Alarm Event Linkage.....	115
4.6.5	Configuring Card Settings.....	116
4.6.6	Configuring Screen Settings.....	117
4.7	Communication Settings.....	118
4.7.1	Configuring TCP/IP.....	118
4.7.2	Configuring Wi-Fi.....	120
4.7.3	Configuring Wi-Fi AP.....	120
4.7.4	Configuring Cloud Service.....	121
4.7.5	Configuring Auto Registration.....	121
4.8	Configuring Audio Prompts.....	122
4.9	Viewing Logs.....	123
4.9.1	System Logs.....	123
4.9.2	Unlock Records.....	123
4.9.3	Alarm Logs.....	124
4.9.4	Attendance Logs.....	124
5	SmartPSS Lite Operations.....	125
5.1	Installation.....	125
5.2	Initialization.....	125
5.3	Adding Devices.....	128
5.3.1	Adding Device by Searching.....	129
5.3.2	Adding Device One by One.....	130
5.3.3	Importing Device in Batches.....	131
5.4	Adding Departments.....	132
5.5	Adding Personnel.....	132
5.5.1	Adding Personnel One by One.....	132
5.5.2	Adding Personnel in Batches.....	136
5.6	Permission Configuration.....	137
5.6.1	Adding Permission Areas.....	137
5.6.2	Assigning Permissions.....	138
5.7	Configuring Attendance Period.....	140

5.7.1 Configuring Fixed Attendance Schedules.....	140
5.7.2 Configuring Flexible Attendance Schedules.....	144
5.8 Adding Attendance Shifts.....	146
5.9 Configuring Shift Schedules.....	147
5.9.1 Configuring Shift Schedules for Department.....	147
5.9.2 Configuring Shifting Schedules for Personnel.....	149
Appendix 1 Important Points of Fingerprint Registration Instructions.....	152
Appendix 2 FAQ.....	154
Appendix 3 Security Recommendation.....	155

1 Product Overview

The Device can be used to track attendance of people and control the door status. People can clock in/out through fingerprint, password, and card.

2 Local Operations

2.1 Keypad Introduction

Figure 2-1 Appearance



The functions of F1, F2, F3 and F4 may differ according to the actual attendance mode. This section introduces the functions of the buttons when the mode is default **Auto/Manual Mode**. For details on other functions of other modes, see "2.9.6 Configuring Attendance Modes".

Table 2-1 Button description

Button	Description
0-9	- Press to input numbers and letters in the input box. - Press to verify the identity through the user ID and password on the standby screen. - Press and hold 0 for 3 seconds, and use the public password to open the door. The attendance function in this situation is invalid.
ESC/F1	- Exit or go to the previous screen. - Press it on the standby screen to configure the check in mode.

Button	Description
∧/F2	- Press it on the standby screen to configure the break out mode. - Press to go up the options.
∨/F3	- Press it on the standby screen to configure the break in mode. - Press it to go down through the options.
OK/F4	- Confirm your settings. - Press it on the standby screen to configure the check out mode.
#	- Delete. - Shortcut for reviewing records. Press the button, use your card or fingerprint to verify the identity, and the attendance records of the verified user are displayed.
	- If the device is in the standby mode and the screen is light up, press button for over 3 seconds to turn the Device off. - Press the button for 10 seconds in any screen to turn the Device off. - On the standby screen, press it to enter the main menu by fingerprints, passwords or cards.  Only administrators can enter the main menu. - Press it to change the input types (numbers, letters and symbols).

Input Types Overview

You can input content after you switch to corresponding input types.

- : Uppercase mode.
- : Lowercase mode.
- : Numeric mode.
- : The combination of uppercase and lowercase mode.
- : Character mode.

Entering Uppercase or Lowercase Letters

When using the uppercase or lowercase input mode, repeatedly press a numeric key to cycle through its assigned letters. For example, in lowercase letter mode:

- Press the **2** key once to enter **a**.
- Press the **2** key twice to enter **b**.
- Press the **2** key three times to enter **c**.

In the uppercase letter mode:

- Press the **2** key once to enter **A**.
- Press the **2** key twice to enter **B**.
- Press the **2** key three times to enter **C**.

Table 2-2 Letter-key mapping

Key	Press Once	Press Twice	Press Three Times
2	a / A	b / B	c / C
3	d / D	e / E	f / F
4	g / G	h / H	i / I
Similar logic applies to keys 5-9.			

Entering Uppercase and Lowercase Letters

In the combination mode, your first press of a numeric key will output an uppercase letter; subsequent presses only output lowercase letters. For example:

- First press: **A** (uppercase)
- Second press: **a** (lowercase)

Entering Numbers

In numeric mode, press the desired number key.

Entering Characters

In character mode, press the corresponding number keys to select the desired character, and then press $\wedge$ / $\vee$ to navigate to the previous/next page.

2.2 Initialization

Background Information

For the first-time use or after restoring factory defaults, you need to select a language, and then set the password and email address for the admin account. You can use the admin account to enter the main menu of the Device and its webpage.

Procedure

Step 1 Select the language, and then press the OK key.

Step 2 Press $\vee$ to select **Enter Password**, and then press OK.

Step 3 Configure the password, and then press OK.

- The input method is the letter method by default. Press  to change to the number method.
- Enter the letter: Press the corresponding letter key, and then press the number to select the letter. For example, if you want to enter the letter a, you need to press the 2 key, and then press the 1 key.



- If you forget the administrator password, send a reset request to your registered e-mail address.

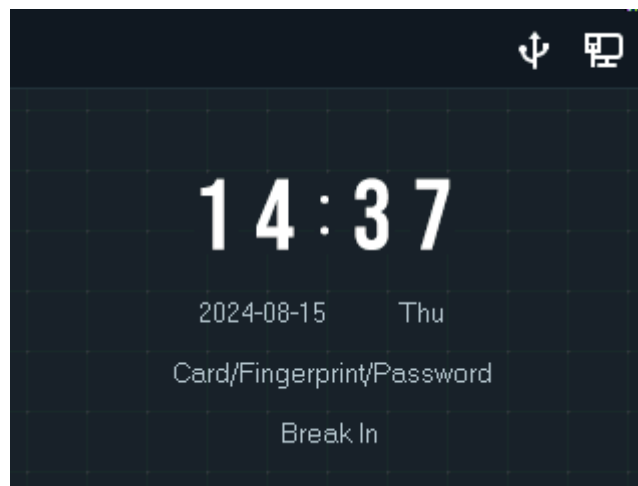
- The password must consist of 8 to 32 non-blank characters and contain at least two types of characters among upper case, lower case, number, and special character (excluding ' " ; : &).

- Step 4 Press ∇ to select **Confirm Password**, and then press OK.
- Step 5 Repeat Step 3, enter the same password, and then press OK.
- Step 6 Enter the email address, and then select the time zone.
- Step 7 Press ∇ to select **OK**, and then press OK.

2.3 Powering On

After the Device is powered on, the standby screen is displayed.

Figure 2-2 Standby screen



-  means the network is connected.
-  means the USB is inserted.
-  means the power is lower than 10%.

2.4 Unlocking Methods

You can unlock the door through passwords, fingerprints, and cards.

2.4.1 Unlocking by Cards

Place the card at the swiping area to unlock the door.

2.4.2 Unlocking by Fingerprints

Place your finger on the fingerprint scanner to unlock the door.

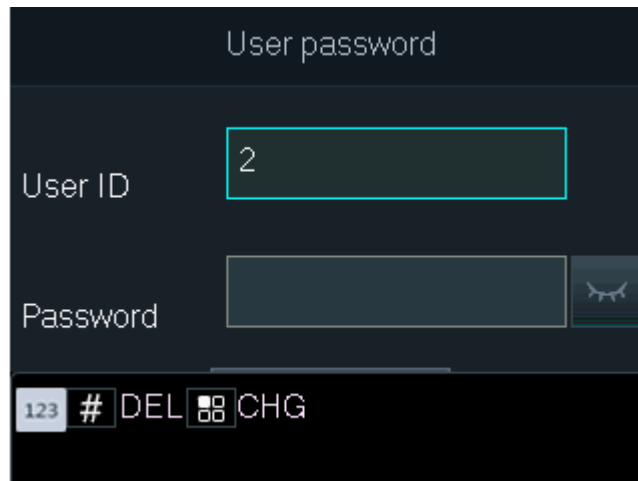
2.4.3 Unlocking by User Password

Enter the user ID and password to unlock the door.

Procedure

Step 1 Press the number key.

Figure 2-3 Unlock by password



Step 2 Enter the registered or delivered user ID and password.

After the successful verification, you can unlock the door.

Step 3 Select **OK**, and then press OK.

2.4.4 Unlocking by Public Password

After you set your public password and enable it, you can unlock the door by simply entering the public password. Using public password to unlock the door without being subject to user levels, unlock modes, periods, holiday plans, and anti-passback except for normally closed door. The Device only allows for one public password.

Background Information

To use the public password for door access, you need to enable the function.

Procedure

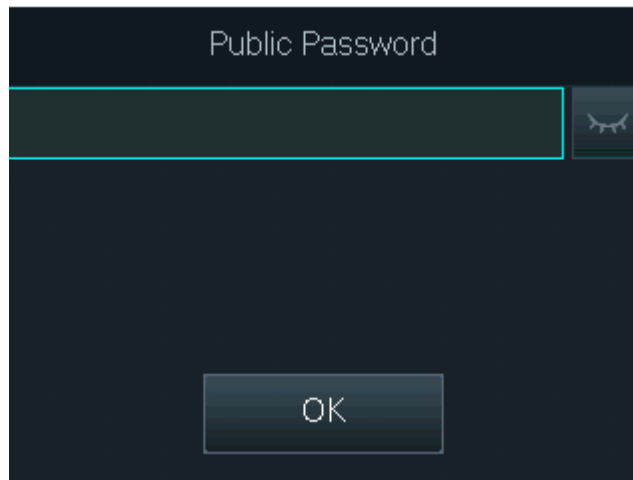
Step 1 Press and hold the **0** key for 3 seconds on the standby screen.

Step 2 Enter the public password, select **OK**, and then press **OK**.



On the main screen, press and hold the **0** key for 3 seconds to directly go to the **Public Password** screen for unlocking.

Figure 2-4 Unlock by public password



2.5 Creating Administrator Account

When the Device is started for the first time, anyone can enter the main menu and configure the Device. For the account security, we recommend you create the administrator account first, and then only administrators can enter the main menu.

Procedure

- Step 1 Press    to enter the main menu screen.
- Step 2 Select **Users** > **Create User**
- Step 3 Enter the user information.
- Step 4 Press OK to select **Admin** as **User Permission**.
- Step 5 Configure other parameters, press Esc, and then press OK to save the configurations.

2.6 Logging In

After the admin account is created, you can enter the main menu after you have verified your identifications through fingerprint, password or card.

On the standby screen, press   , and then enter the main menu after your identity has been verified.

- Swipe the card on the card reader area.
- Place your finger on the fingerprint sensor.
- Enter the user ID and password.



The user type must be **admin**.

- Enter the administrator's ID and password.

2.7 User Management

On the main menu, select **Users**, and then you can add new users.

2.7.1 Adding Users

Procedure

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

Step 2 Configure the parameters on the interface.

Table 2-3 Parameters description

Parameter	Description
No.	The No. is like employee ID, which can be numbers, letters, and their combinations, and the maximum length of the No. is 30 characters.
Name	The name can have up to 32 characters (including numbers, symbols, and letters).
Fingerprint	Register fingerprints. A user can register up to 3 fingerprints, and you can set a fingerprint to the duress fingerprint. An alarm will be triggered when the duress fingerprint is used to unlock the door.  • We do not recommend you set the first fingerprint as the duress fingerprint. • One user can only set one duress fingerprint. • Fingerprint function is available if the Access Controller supports connecting a fingerprint extension module.
Card	A user can register up to 5 cards at most. Enter your card number or swipe your card, and then the card information will be read by the Access Controller. You can enable the Duress Card function. An alarm will be triggered if a duress card is used to unlock the door.  One user can only set one duress card.
Password	Enter the user password. The maximum length of the password is 8 digits. The duress password is the unlock password + 1. For example, if the user password is 12345, the duress password will be 12346. A duress alarm will be triggered when a duress password is used to unlock the door.

Parameter	Description
User Permission	● User : Users only have door access or time attendance permissions. ● Admin : Administrators can log in to the main menu to configure the Device.
General Plan	People can unlock the door or take attendance during the defined period.
Holiday Plan	People can unlock the door or take attendance during the defined holiday.
Validity Period	Set a date on which the door access and attendance permissions of the person will be expired.
User Type	● General User : General users can unlock the door. ● Blocklist User : When users on the blocklist unlock the door, a blocklist alarm will be triggered. ● Guest User : Guests can unlock the door within a defined period or for a designated number of times. After the defined period expires or the unlocking times run out, they cannot unlock the door. ● Patrol User : Patrol users can take attendance on the Access Controller, but they do not have door permissions. ● VIP User : When VIP users unlock the door, service personnel will receive a notification. ● Other User : When they unlock the door, the door will stay unlocked for 5 more seconds.  The delay time is not available for remote verification methods. ● Custom User 1/Custom User 2 : Same with general users.
Department	Select departments, which is useful when configuring department schedules.
Schedule Mode	● Department Schedule: Apply department schedules to the user. ● Personal Schedule: Apply personal schedules to the user.  ◇ If you set the schedule mode to department schedule here, the personal schedule you have configured for the user in Attendance > Schedule Config > Personal Schedule becomes invalid.

Step 3 Press the Esc key, and then press OK to save the configurations.

2.7.2 User/Admin List

You can view and search all the general users and admin users, and edit user information.

On the main menu, select **Users** > **User List** or **Users** > **Admin List**.

Figure 2-5 User list

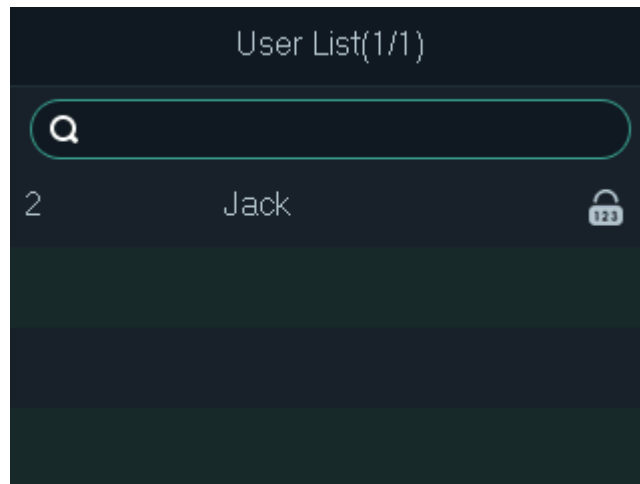
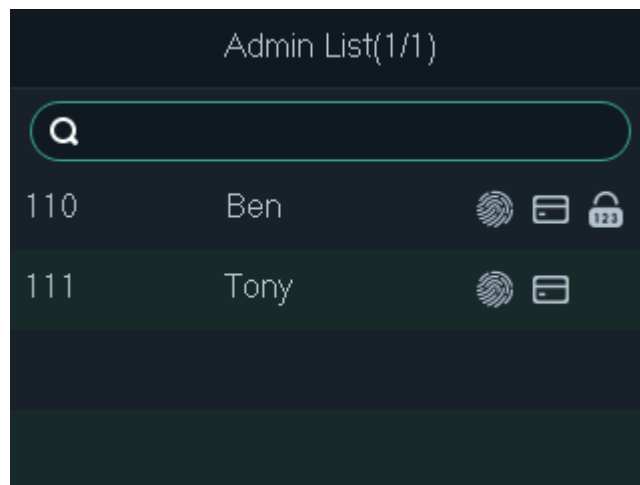


Figure 2-6 Admin list



Unlocking Method

- : Fingerprint.
- : Card.
- : Password.

Editing User Information

1. Select the user and press **OK**.
2. Edit the user information, and then press **Esc**.

3. Press **Esc** to save settings.

Searching for Users

1. Select  and press **OK**.
2. Enter the user ID, swipe a card, or press a fingerprint to search for the user.

Deleting Users

Select the user, press **OK**, and then select  to delete the user.

2.7.3 Configuring Public Password

Add and enable the public password. Public password can be used to unlock the door in any unlock modes.

Log in to the main menu, and then select **Users > Public Password**.

Add Public Password

1. Select **Configure Public Password**, enter the new password, and then press **OK**.
2. Enter the password again to confirm, and then press **OK**.
3. Press **OK** to save the configurations.

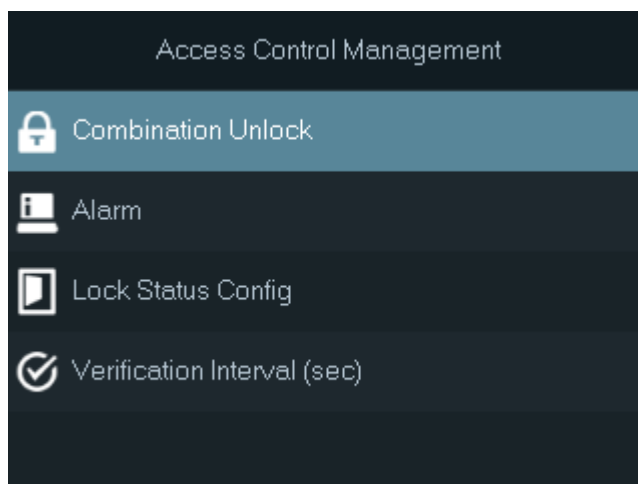
Enable Public Password

Select **Enable Public Password**, and then press **OK**.

2.8 Access Control Management

You can configure settings for doors such as the unlocking mode, alarm linkage and door schedules. The available unlock modes might differ depending on the product model.

Figure 2-7 Access control management



2.8.1 Configuring Unlock Combinations

Use card, fingerprint, password or their combinations to unlock the door. The available unlock modes might differ depending on the product model.

Procedure

Step 1 On the **Main Menu**, select **Access Control** > **Combination Unlock**.

Step 2 Press OK to configure the combination method and the verification method.

- For example, configure the **Combination Method** as **And**, configure **Yes** for card and password. You can unlock the door by swiping the card and entering the password.
- For example, configure the **Combination Method** as **Or**, configure **Yes** for card and password. You can unlock the door by swiping the card or entering the password.



The verification method of the fingerprint is available on the model with the fingerprint function.

Step 3 Press Esc, and then press OK to save the configurations.

2.8.2 Configuring Alarms

An alarm will be triggered when the entrance or exit is abnormally accessed.

Procedure

Step 1 On the **Main Menu**, select **Access Control** > **Alarm**.

Step 2 Configure the alarm parameters.

Table 2-4 Description of alarm parameters

Parameter	Description
Duress	An alarm will be triggered when a duress card, duress password or duress fingerprint is used to unlock the door.

Parameter	Description
Door Detector	With the door detector wired to your device, alarms can be triggered when doors are opened or closed abnormally. There are 2 types of door detectors: NC detector and NO detector.
Door Detector Type	• NC : The sensor is in a shorted position when the door or window is closed. • NO : An open circuit is created when the window or door is actually closed.
Intrusion	If the door is opened abnormally, an intrusion alarm will be triggered and last for a defined time.  This function is available when Door Detector is enabled.
Door Timed Out	If Door Timed Out is enabled, when the door remains unlocked for longer than the defined timeout duration, the door timeout alarm will be triggered and last for the defined time.
Door Timeout Duration	 This function is available when Door Detector is enabled.
Excessive Use Alarm	If the wrong password or card is used 5 times in a row within 60 seconds, the alarm for excessive use of illegal card will be triggered and lasts for a defined time.

Step 3 Press Esc, and then press OK to save the configurations.

2.8.3 Configuring Lock Status

Procedure

Step 1 On the main menu, select **Access Control** > **Lock Status Config**, and then press **OK**.

Step 2 Configure parameters.

Figure 2-8 Lock status

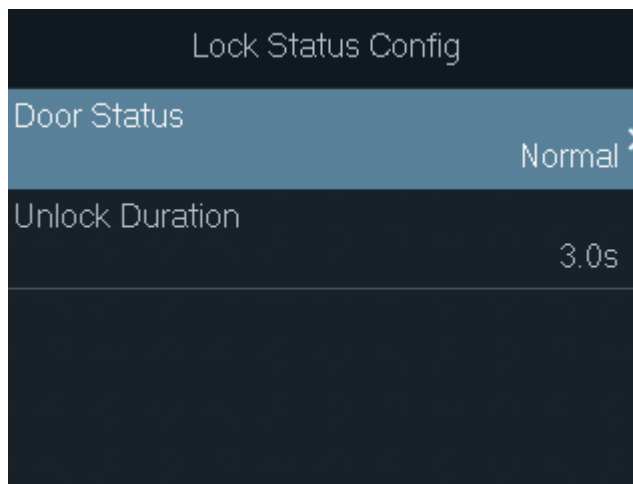


Table 2-5 Description of door status

Parameter	Description
Door Status	• Normal: The door will be open or closed according to settings. • NO: The door is always open. • NC: The door is always closed.
Unlock Duration	The duration during which the door lock remains open. It will be closed after this preset time.

2.8.4 Configuring the Verification Time Interval

If you verify your identity multiple times within a set period, only the earliest verification will be considered valid, and the door will not open after the second or later verifications. From the moment the door fails to open, you must wait for the configured verification time interval before attempting to verify your identity again.

Procedure

Step 1 On the **Main Menu** screen, select **Access Control** > **Verification Interval (sec)**.

Step 2 Enter the time interval, select **OK**, and then press OK.

2.8.5 Managing Main Cards

Adding Main Card

On the main menu, select **Access** > **Main Card Management** > **Add Main Card**, press **OK**, and then swipe the card.

Deleting Main Card

On the main menu, select **Access** > **Main Card Management** > **Delete Main Card**, and then press **OK** to delete the card.

Related Operations

On the main screen, after swiping the main card, wait for 3 seconds without any operation to go to the corresponding mode. If a regular card is swiped within these 3 seconds, the device will not respond.

The device determines the function based on the total number of main card swipes. Once the corresponding mode is activated, swiping the main card once will exit the current mode and go back to the main screen.



If a card is both a main card and a user card, the system prioritizes checking whether it is a main card.

- Swiping the main card to add the user card. Swiping the user card to add it to the device. Continuous adding is allowed.

- Swiping the main card twice to delete the user card. Swiping the user card to remove it from the device. Continuous deleting is allowed.
- Swiping the main card for 5 times to delete all users.

2.8.6 Configuring PIN Code Authentication

Procedure

Step 1 On the main menu, select **Access Control** > **PIN Code Authentication**.

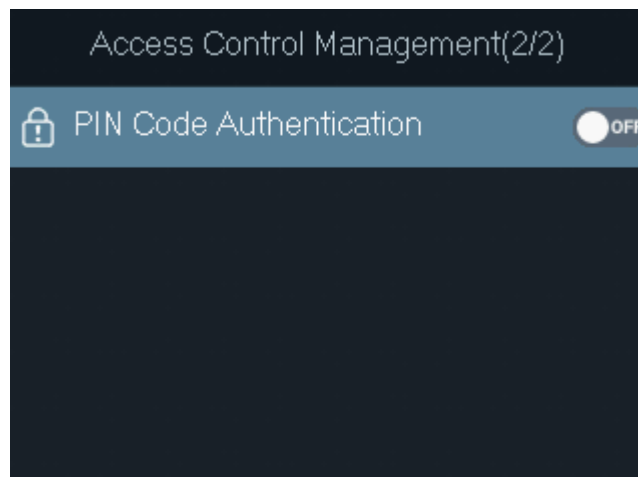
Step 2 Enable or turn off **PIN Code Authentication**.

The pin code authentication is turned off by default. When it is enabled, you can only open the door with password.



After PIN code authentication is enabled, you can directly enter their password for verification without entering user ID.

Figure 2-9 PIN code



2.9 Attendance Management

When **Use Attendance for Unlock** is enabled, if people verify the identity for the attendance, they can unlock the door at the same time.

2.9.1 Configuring Departments

Procedure

Step 1 On the **Main Menu**, select **Attendance** > **Department Settings**.

Step 2 Press $\wedge$ or $\vee$ to select the department, and then press OK to rename the department.

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

2.9.2 Configuring Shifts

Configure shifts to define time attendance rules. Employees need to work at the time scheduled for their shift to start, and leave at the end time, except when they choose to work overtime.

Procedure

Step 1 On the **Main Menu**, select **Attendance** > **Shift Config** > **Shift**.

Step 2 Press $\wedge$ or $\vee$ to select the shift, and then press OK to edit the shift.



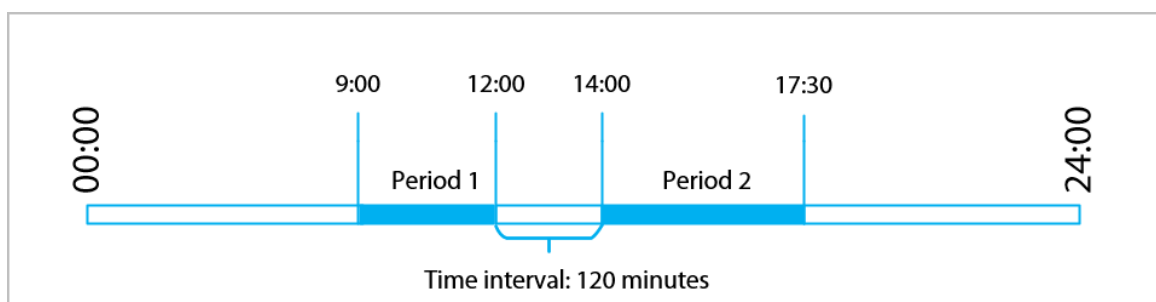
All attendance times are precise down to the second. For example, if the normal clock-in time is set to 8:05 AM, the employee who clocks in at 8:05:59 AM will not be considered as arriving late. But, the employee that arrives at 8:06 AM will be marked as late by 1 minute.

Table 2-6 Shift parameters description

Parameter	Description
Shift Name	Enter the name of the shift.
Period 1	Specify a time range when people can clock in and clock out for the workday.
Period 2	If you only set one attendance period, employees need to clock in and out by the designated times to avoid an anomaly appearing on their attendance record. For example, if you set 08:00 to 17:00, employees must clock in by 08:00 and clock out from 17:00 onwards. If you set 2 attendance periods, the 2 periods cannot overlap. Employees need to clock in and clock out for both periods.
Overtime Period	Employees who clock in or out during the defined period will be considered as working beyond their normal work hours.
Limit for Arriving Late (min)	A certain amount of time can be granted to employees to allow them to clock in a bit late and clock out a bit early. For example, if the regular time to clock in is 08:00, the tolerance period can be set as 5 minutes for employees who arrive by 08:05 to not be considered as late.
Limit for Leaving Early (min)	

- When the time interval between 2 periods is an even number, you can divide the time interval by 2, and assign the first half of the interval to the first period, which will be the clock out time. The second half of the interval should be assigned to the second period as the clock in time.

Figure 2-10 Time interval (even number)



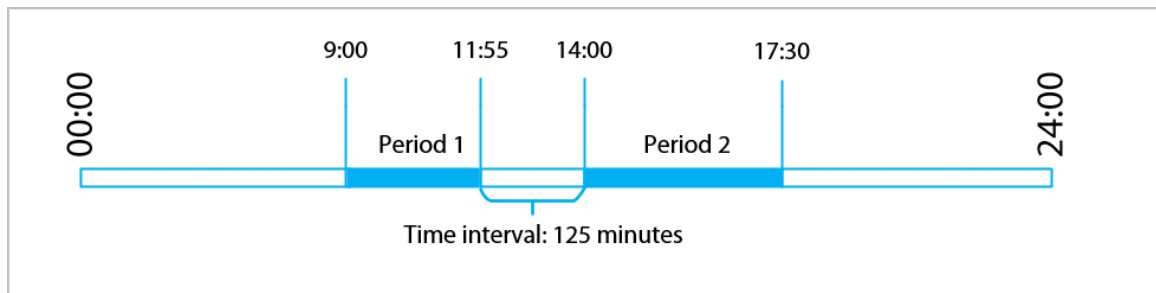
For example: If the interval is 120 minutes, then the clock-out time for period 1 is from 12:00 to 12:59, and the clock-in time for period 2 is from 13:00 to 14:00.



If a person clocks out multiple times during period 1, the latest time will be valid, and if they clock in multiple times during period 2, the earliest time will be valid.

- When the time interval between 2 periods is an odd number, the smallest portion of the interval will be assigned to the first period, which will be the clock out time. The largest portion of the interval will be assigned to the second period as the clock in time.

Figure 2-11 Time interval (even number)



For example: If the interval is 125 minutes, then the clock-out time for period 1 is from 11:55 to 12:57, and the clock-in time for period 2 is from 12:58 to 14:00. Period 1 has 62 minutes, and period 2 has 63 minutes.



If a person clocks out multiple times during period 1, the latest time will be valid, and if they clock in multiple times during period 2, the earliest time will be valid.

Step 3 Press Esc to save the configurations.

2.9.3 Configuring Holiday

Configure holiday plans to set periods for attendance to not be tracked.

Procedure

Step 1 On the **Main Menu**, select **Attendance** > **Shift Config** > **Holiday**.

Step 2 Select +, and then press OK to add holiday plans.

Step 3 Configure the parameters.

Table 2-7 Parameters description

Parameter	Description
Attendance Holiday No.	The number of the holiday.
Attendance Holiday	The name of the holiday.
Start Time	The start and end time of the holiday.
End Time	

Step 4 Press Esc to save the configurations.

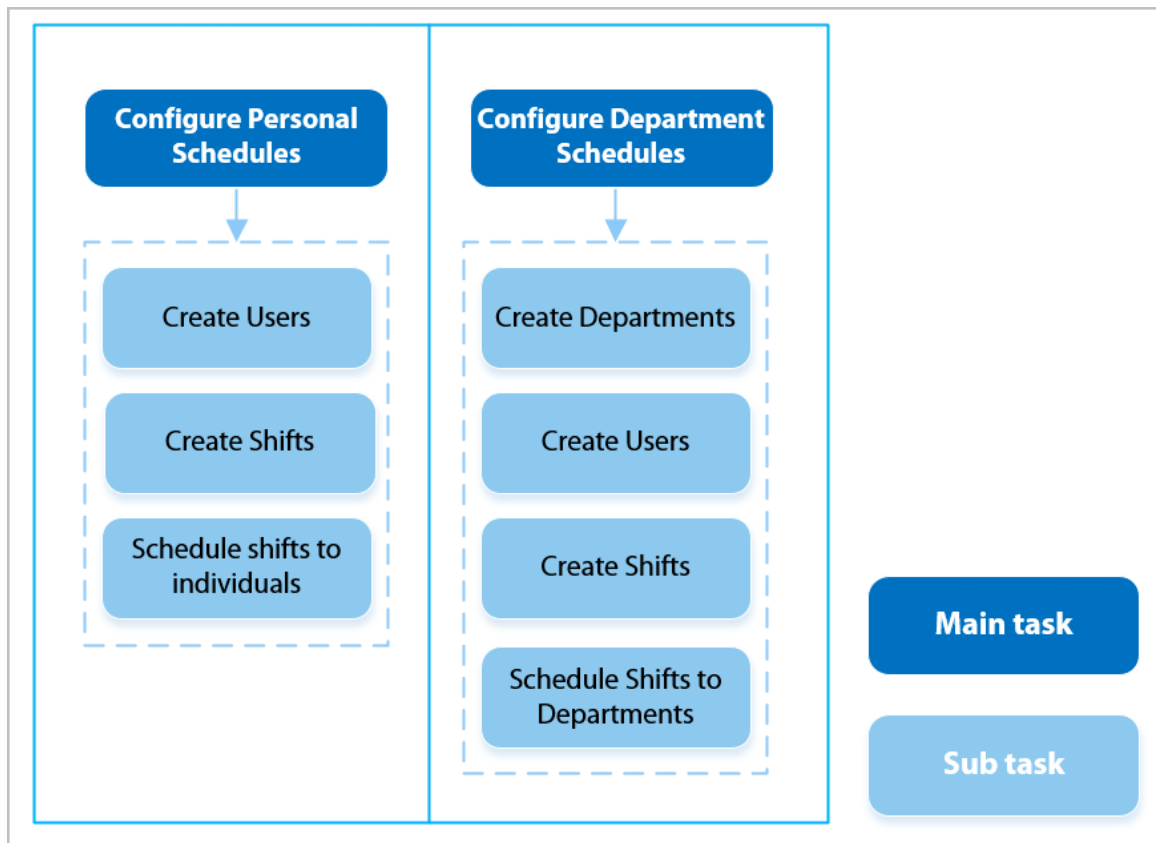
2.9.4 Configuring Work Schedules

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.

Background Information

Refer to the flowchart to configure personal schedules or department schedules.

Figure 2-12 Configuring work schedules



Procedure

- Step 1 On the **Main Menu**, select **Attendance** > **Schedule Config**.
- Step 2 Set work schedules for individuals.
1. Select **Personal Schedule**.

Figure 2-13 Personal schedule

- 2. Enter the user ID.
- 3. View the schedules of the week or edit the schedule of the current day.
You can press the number buttons of **2**, **4**, **6** or **8** to select the day. **2** and **8** are used to shift the option in upward and downward directions. **4** and **6** are used to shift the option in left and right directions.
- 4. Select , and then press OK to save the configurations.



- 0 indicates break.
- 1 to 24 indicates the number of the per-defined shifts.
- 25 indicates business trip.
- 26 indicates leave of absence.

Step 3 Set works schedules for departments.

- 1. Select **Department Schedule**.
- 2. Select a department in the department list.
- 3. View the schedules of the week or edit the schedule of the current day.
- 4. Select , and then press OK to save the configurations.
- 0 indicates rest.
- 1 to 24 indicates the number of the per-defined shifts.
- 25 indicates business trip.
- 26 indicates leave of absence.



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

2.9.5 Configuring Network Attendance

On the main menu, select **Attendance** . Enable the **Network Attendance** or turn it off.



After it is enabled, the attendance status cannot be configured and reported to the platform.

2.9.6 Configuring Attendance Modes

Prerequisites

Make sure that you have enabled **Network Attendance** on the **Attendance** screen.

Procedure

Step 1 On the **Main Menu**, select **Attendance** > **Mode Settings**.

Step 2 Configure attendance mode.

Table 2-8 Attendance mode

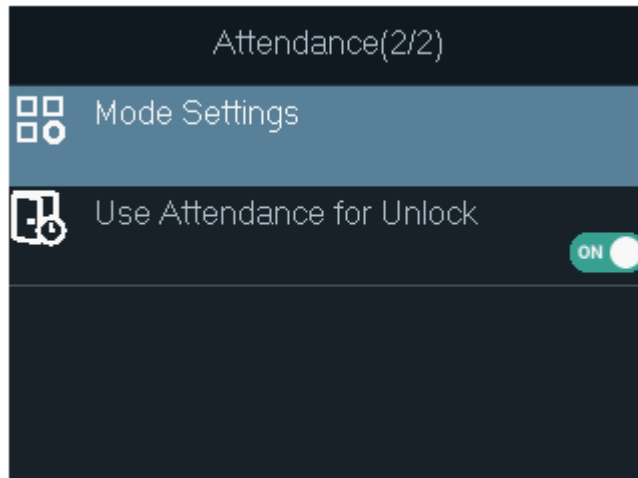
Parameter	Description	Attendance Mode
Auto/Manual Mode	Select the mode, select the period, and then configure the start time and the end time of each period. The screen displays the attendance status automatically after you clock in or out, but you can also manually change your attendance status using the buttons of F1 to F4.	● Check in: Clock in when your normal workday starts. ● Break out: Clock out when your break starts. ● Break in: Clock in when your break ends. ● Check out: Clock out when your normal workday starts. ● Overtime check in: Clock in when your overtime period starts. ● Overtime check out: Clock out when your overtime period ends.
Auto Mode	Select the mode, select the period, and then configure the start time and the end time of each period. The screen displays the attendance status automatically according to your configurations. You cannot use the buttons to change the status.	
Manual Mode	● After you clock in or out, manually select the attendance status. ● Press F1 to F4 to change the attendance mode, and then verify the identity.  The status is not displayed on the screen. After you press F1 to F4 to select the status first, the status will be displayed for 10 seconds.	
Fixed Mode	When you clock in or out, the screen will display the per-defined attendance status all the time.	

Step 3 Press Esc to save the configurations.

2.9.7 Using Attendance for Lock

On the main menu, select **Attendance** . Enable the **Use Attendance for Unlock** or turn it off.

Figure 2-14 Use attendance for unlock



2.10 Communication Settings

2.10.1 Configuring the IP Address

Set an IP address for the Device to connect it to the network. After that, you can log in to the webpage and the management platform to manage the Device.

Procedure

- Step 1 On the **Main Menu**, select **Communication Settings** > **IP Settings**.
- Step 2 Set the IP Address.



The displayed parameters may differ according to different device models.

Figure 2-15 IP settings

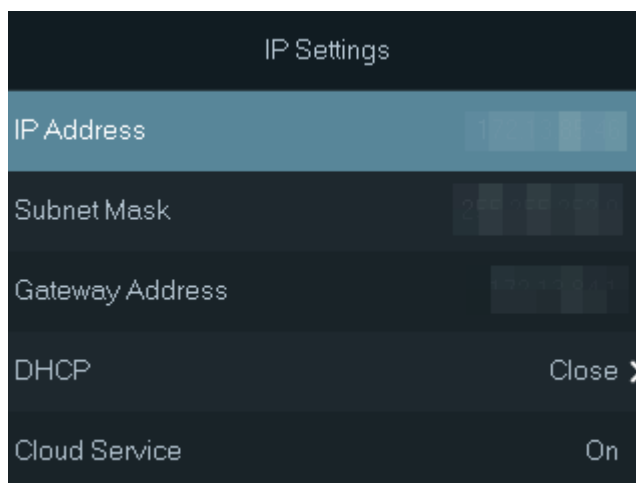


Table 2-9 IP configuration parameters

Parameter	Description
IP Address/Subnet Mask/Gateway Address	Enter the IP address, subnet mask, and gateway IP address. They must be on the same network segment.
DHCP	It stands for Dynamic Host Configuration Protocol. When DHCP is turned on, the Device will automatically be assigned the IP address, subnet mask, and gateway.
Cloud Service	If this function is turned on, you can manage devices without applying for DDNS, setting port mapping or deploying transit servers.

2.10.2 Configuring Wi-Fi

You can connect the Device to the network through the Wi-Fi network.

Background Information



- This function is only available on select models.
- Wi-Fi AP and Wi-Fi function cannot be enabled at the same time.

Procedure

Step 1 On the **Main Menu**, select **Communication Settings** > **Wi-Fi**.

Step 2 Select **Search**, and then press OK.

Step 3 Press OK to turn on Wi-Fi.



After Wi-Fi is enabled, wait about 1 minute to connect Wi-Fi.

Step 4 Select a wireless network, and then press OK.

Step 5 Enter the password for the Wi-Fi, select **Connect**, and then press OK.

Step 6 (Optional) If the system does not find a Wi-Fi network, select **SSID** to enter the name of the Wi-Fi.

Results

If the phone and the device connect to the same Wi-Fi, enter the IP address that is displayed on the Wi-Fi screen in the address bar of the browser to access to the device.

Related Operations

DHCP: Turn on this function, and the Device will automatically be assigned a Wi-Fi address. Turn off this function, and you can configure the IP address.

2.10.3 Configuring Wi-Fi AP

Enable the Wi-Fi AP function, you can access the Device through the AP.



- This function is only available on select models.
- Wi-Fi AP and Wi-Fi function cannot be enabled at the same time.

Procedure

Step 1 On the **Main Menu**, select **Communication Settings** > **Wi-Fi AP**.

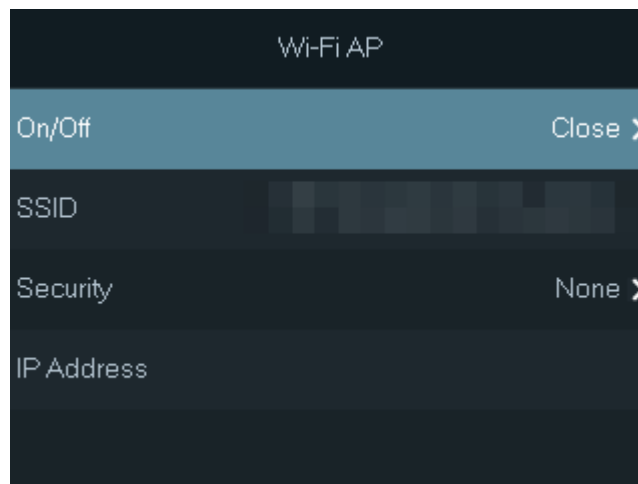
Step 2 Turn on Wi-Fi AP.

You can modify the SSID and configure the password through **Security**.



- After the Wi-Fi AP is enabled, wait about 1 minutes to connect it.
- The security is **None** by default.

Figure 2-16 Connect to Wi-Fi AP



Results

Use your computer to connect to Wi-Fi AP of the Device to access its webpage.

2.11 System Settings

2.11.1 Configuring Time

Configure system time, such as date and time.

Procedure

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

Step 2 Configure the time parameters.

Figure 2-17 Time settings

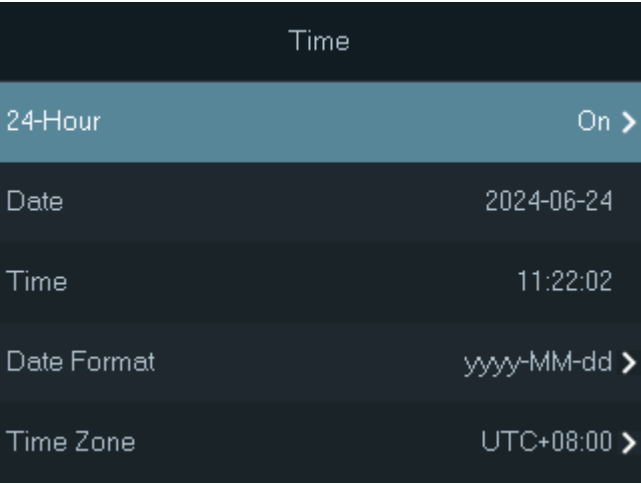


Table 2-10 Description of time parameters

Parameter	Description
24-Hour	Press OK to turn on or turn off the 24-hour format. Turn on it, the time is displayed in the 24-hour format. Turn off it, the time is displayed in the 12-hour format.
Date & Time	1. Press $\wedge$ or $\vee$ to select Date&Time , and then press OK. 2. Press the number button to enter the date, and then press Esc.
Time	1. Press $\wedge$ or $\vee$ to select Time , and then press OK. 2. Press the number button to enter the time, and then press Esc.
Date Format	1. Press $\wedge$ or $\vee$ to select Date Format . 2. Press OK to select the date format.
Time Zone	1. Press $\wedge$ or $\vee$ to select Time Zone . 2. Press OK to select the time zone.

2.11.2 Configuring the Volume

Procedure

- Step 1 On the **Main Menu**, select **System** > **Volume Settings**.
- Step 2 Configure the parameters.

Table 2-11 Parameters description

Parameters	Description
Speaker Volume	Select Speaker Volume , press OK, and then press $\wedge$ or $\vee$ to adjust the volume.

Parameters	Description
Key Sound	When this function is enabled, there is sound if you press the buttons.

2.11.3 Configuring the Language

Change the language on the Device. On the **Main Menu**, select **System** > **Language**, select the language for the Device.

2.11.4 Configuring Screen Parameters

Procedure

- Step 1 On the main menu, select **System** > **Screen Settings**, and then press **OK**.
- Step 2 Configure parameters.

Figure 2-18 Screen settings

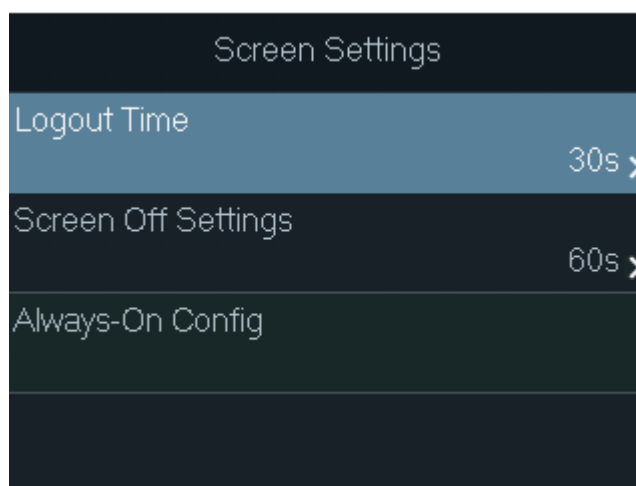


Figure 2-19 Always-on

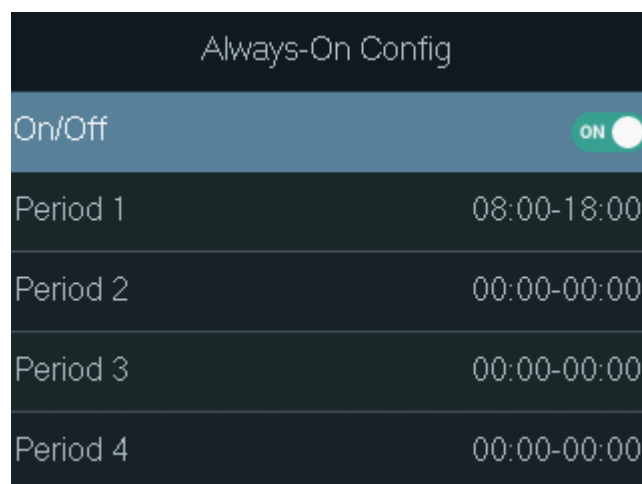


Table 2-12 Description of screen parameters

Parameter	Description	
Logout Time	If there is no operation on any interface for more than the set time, the system returns to the screensaver interface.	Example: If the logout time is set to 15 seconds and the screen-off time is set to 30 seconds:
Screen Off Settings	If there is no operation on any interface, the system first returns to the screensaver interface. If the total inactive time reaches the set duration and it is outside the screen always-on period, the system goes to a screen-off mode. If within the always-on period, the screen dims while continuing to display the screensaver image.	• When there is no operation on any interface for 15 seconds, the system returns to the screensaver interface. • If there is still no operation for another 15 seconds (total inactive time reaches 30 seconds): ◇ Outside the always-on period: The system enters the screen-off state. ◇ Within the always-on period: The screen dims but continues displaying the screensaver image.
Always-on Config	Enable it and configure the always-on period. During the time period, the screen is always on.  Keeping the screen on for extended periods might affect its lifespan. It is recommended that you limit the total daily screen always-on time to no more than 8 hours.	 The logout time must be lower than the screen time.

2.11.5 Configuring Ringtone

Configure the time when the bell rings as a reminder.

Procedure

- Step 1** On the main menu, select **System > Ringtone Config**.
- Step 2** Select the configuration item.
- Step 3** Configure the time when the bell rings.

Table 2-13 Parameters description

Parameter	Description
Time	The time when the bell rings.
Cycle	The bell rings in a cycle. For example, if you set cycle to Monday, the bell rings every Monday.
Duration	The ring duration.

2.11.6 Managing Device Password

2.11.6.1 Changing Admin Password

Procedure

- Step 1 On the main menu, select **System** > **Device Password** > **Change Password**, and then press **OK**.
- Step 2 Enter the old password, new password and then confirm it.
- Step 3 Press **OK** to save the settings.
- The new password becomes valid immediately after modification.

2.11.6.2 Modifying Reserved Email

Procedure

- Step 1 On the main menu, select **System** > **Device Password** > **Modify Reserved Info**, and then press **OK**.
- Step 2 Enter the reserved email address, and then press **OK**.

2.11.7 Restoring Factory Defaults

Background Information



Restoring factory defaults will cause data loss. Please be advised.

Procedure

- Step 1 On the **Main Menu**, select **System** > **Factory Defaults**.
- Step 2 Restore the Device to factory settings.
- **Factory Defaults** : Resets all configurations and data except for IP settings and the type of the extension module.
 - **Defaults (Keep User Info and Logs)** : Resets all the configurations except for user information and logs.

2.11.8 Restarting the Device

On the **Main Menu**, select **System** > **Restart**, press **OK**, and then press **OK** for the prompt. The Device will be restarted.

2.12 USB Management

You can use a USB to update the Device, and export or import user information or attendance records through USB.



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

Figure 2-20 USB management



2.12.1 Exporting to USB

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

Procedure

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

Step 2 Select the data type you want to export.



- When the data is exported in Excel, it can be edited.
 - The USB disk supports the format in FAT32, and the storage capacity is 4 GB –128 GB.
- Personnel information, card data, fingerprint data are encrypted when exporting.

Step 3 Press OK to confirm.

The exported data is saved to the USB.

2.12.2 Importing from USB

You can import data from USB to the Device.

Procedure

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

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



We recommend you import the data to the device with the same model and version. Data transmission between devices with different models and versions will cause data loss.

2.12.3 Updating the System

Update the system of the Device through USB.



If you start the Device for the first time or restore the Device to factory default settings, the Device automatically backups the system files within the first 10 minutes. Please do not update in this period.

Procedure

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 Device.

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

Step 3 Press **OK**.

The Device will restart when the updating completes.



Do not power off the Device during the update.

2.13 Record Management

On the main menu, select **Records** > **Search for Attendance Records**. Enter the user ID, and the attendance records are displayed.

2.14 System Information

You can view data capacity and device version.

2.14.1 Viewing Data Capacity

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

2.14.2 Viewing Device Version

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

3 Webpage Operations

On the webpage, you can also configure and update the Device.



Web configurations differ depending on models of the Device.

3.1 Initialization

Initialize the Device when you log in to the webpage for the first time or after the Device 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 Device.

Procedure

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



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

Step 2 Select a language for the Device.

Step 3 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 Resetting the Password

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

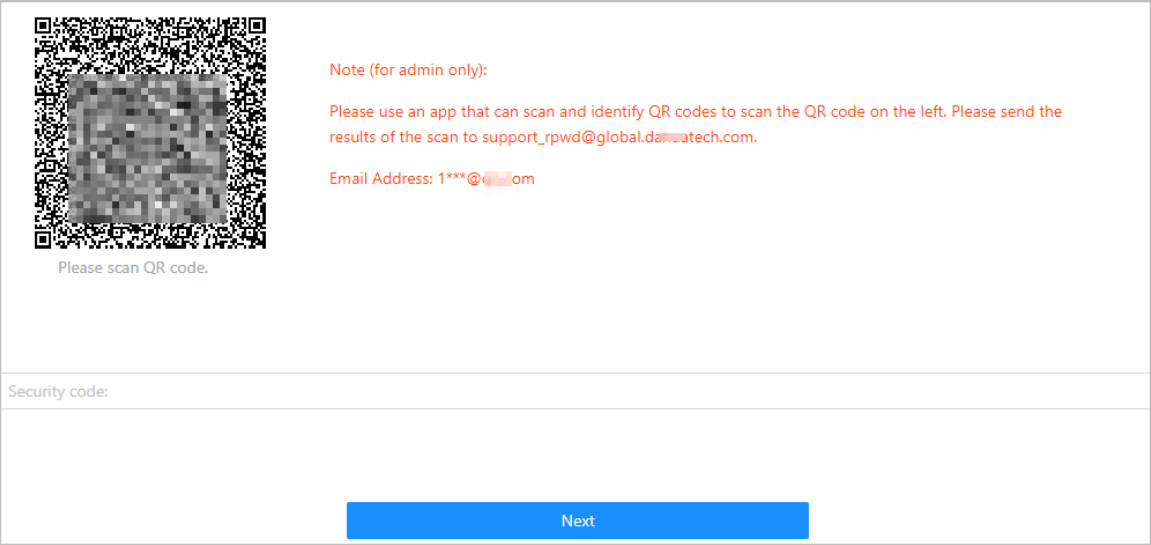
Procedure

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 receive a security code.

Figure 3-1 Reset password



Please scan QR code.

Note (for admin only):

Please use an app that can scan and identify QR codes to scan the QR code on the left. Please send the results of the scan to support_rpwd@global.damtech.com.

Email Address: 1***@damtech.com

Security code:

Next



- 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 5 times 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 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**.

3.3 Home Page

The home page is displayed after you successfully log in.

Figure 3-2 Home page

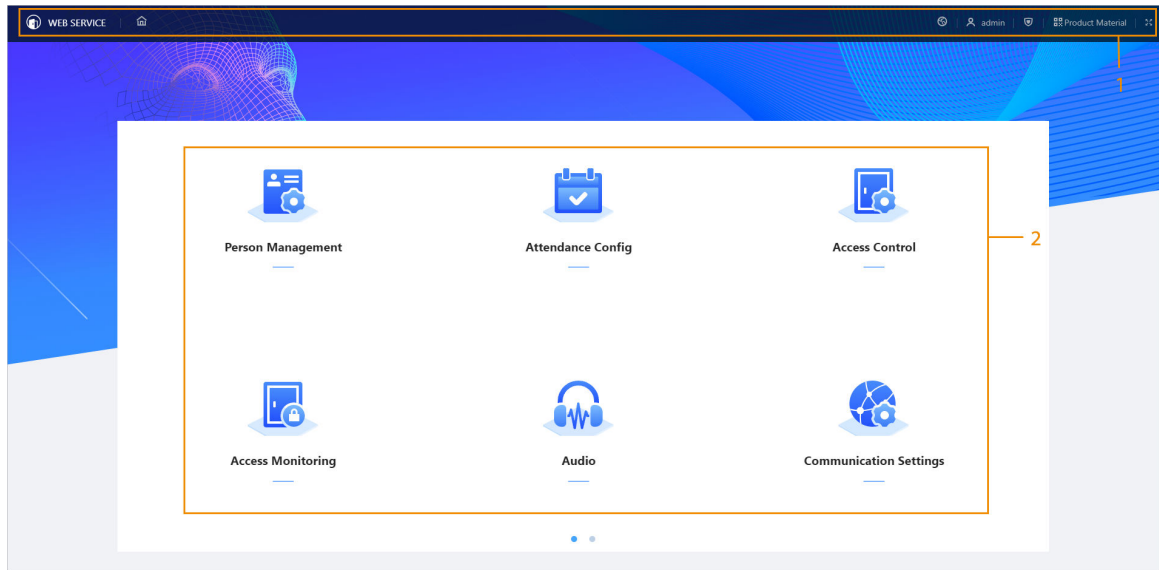


Table 3-1 Home page description

No.	Description
1	• : Enter the home page. • : Select a language on the device. • : Log out or restart the device. • : Enter the Security page. • Product Material : Scan the QR code to view the product material. This function is available on select models. • : Display in the full screen.
2	Main menu.

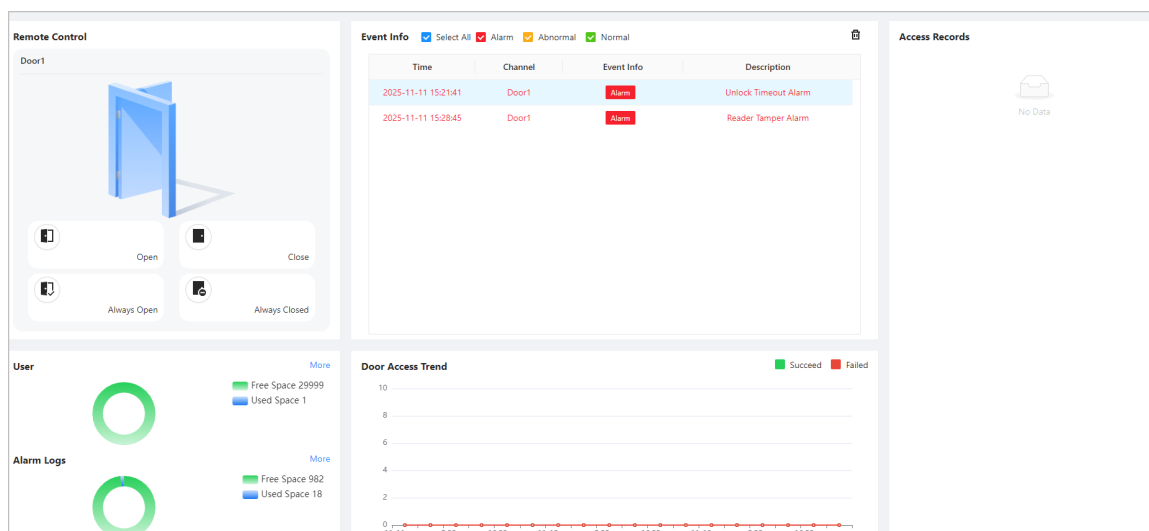
3.4 Access Monitoring

Log in to the webpage, and the system automatically go to the **Access Monitoring** page.



- For first-time use, please download and install the plug-in according to the prompt.
- You can also click the web service icon at the upper-left corner to view the access monitoring page.

Figure 3-3 Access monitoring



Remote Control

- Click **Open** or **Close** next to the door to remotely control the door.
- Click **Always Open** or **Always Closed** to remotely control the door. Click **Restore** to restore the door to normal status.

Door Access Trend

The access trend in the last 3 days is displayed. Green means successful access and the red means failed access.

Access Records

The real-time access records are displayed, including image, person information, verification method and verification time.

Event Information

In the **Event Info** area, select the event type to view the events. Click  to clear all the events.

User and Alarm Logs

View the space information of users and alarm logs. Click **More** to view the details.

3.5 Person Management

Procedure

Step 1 On the home page, select **Person Management**, and then click **Add**.

Step 2 Configure user information.

Figure 3-4 Add users

Add

Basic Info

* No.

Name

* Department

1-Default

* Schedule Mode

Department Schedule

Validity Period

2037-12-31 23:59:59

* Permission

User

* User Type

General User

* Times Used

Unlimited

* General Plan

255-Default x

* Holiday Plan

255-Default x

Verification Mode

▼ Password

Not Added

Add

> Card

Not Added

> Fingerprint

Not Added

Add

Add More

Cancel

Table 3-2 Parameters description

Parameter	Description
User ID	The User ID is like employee ID, which can be numbers, letters, and their combinations, and the maximum length of the number is 30 characters.
Name	The name can have up to 32 characters (including numbers, symbols, and letters).

Parameter	Description
Department	Add users to a department. If a department schedule is assigned to the person, they will follow the established department schedule.
Schedule Mode	• Department Schedule: Assign department schedule to the user. • Personal Schedule: Assign personal schedule to the user.  If you set the schedule mode to department schedule here, the personal schedule you have configured for the user in Attendance > Schedule Config > Personal Schedule is invalid.
Validity Period	Set a date on which the door access and attendance permissions of the person will be expired.
Permission	• User : Users only have door access or time attendance permissions. • Admin : Administrators can configure the Device besides door access and attendance permissions.
User Type	• General User : General users can unlock the door. • Blocklist User : When users in the blocklist unlock the door, service personnel will receive a notification. • Guest User : Guests can unlock the door within a defined period or for certain amount of times. After the defined period expires or the unlocking times runs out, they cannot unlock the door. • Patrol User : Patrol users can take attendance on the Device, but they do not have door permissions. • VIP User : When VIP unlock the door, service personnel will receive a notice. • Other User : When they unlock the door, the door will stay unlocked for 5 more seconds. • Custom User 1/Custom User 2: Same with general users.
Time Used	Set an unlock limit for guest users. After the unlock times run out, they cannot unlock the door.
General Plan	People can unlock the door or take attendance during the defined period.  You can select more than one plan.
Holiday Plan	People can unlock the door or take attendance during the defined holiday.  You can select more than one holiday.
Password	Enter the user password. The maximum length of the password is 8 digits. The duress password is the unlock password + 1. For example, if the user password is 12345, the duress password will be 12346. A duress alarm will be triggered when a duress password is used to unlock the door.

Parameter	Description
Card	- Enter the card number manually. - Click Add. - Enter the card number, and then click Add. - Read the number automatically through the enrollment reader or the Device. - Click Add, and then click Modify to select an enrollment reader or the Device. - Click Read Card, and then swipe cards on the card reader. A 60-second countdown is displayed to remind you to swipe cards, and the system will read the card number automatically. If the 60-second countdown expires, click Read Card again to start a new countdown. - Click Add. A user can register up to 5 cards at most. Enter your card number or swipe your card, and then the card information will be read by the Device. You can enable the Duress Card function. An alarm will be triggered if a duress card is used to unlock the door. : Set duress card. : Change card number.  One user can only set one duress card.
Fingerprint	Register fingerprints. A user can register up to 3 fingerprints, and you can set a fingerprint to the duress fingerprint. An alarm will be triggered when the duress fingerprint is used to unlock the door. Enroll fingerprints through an enrollment reader or the Device. - Click Add, and then click Modify to select an enrollment reader or the Device. - Press finger on the scanner according to the on-screen instructions. - Click Add.  - We do not recommend you set the first fingerprint as the duress fingerprint. - One user can only sets one duress fingerprint. - Fingerprint function is available if the Device supports connecting a fingerprint module.

Step 3 Click **OK**.

Related Operations

- Import user information: Click **Export**, and download the template and enter user information in it. Place face images and the template in the same file path, and then click **Import** to import the folder.
- Clear: Clear all users.

- Refresh: Refresh the user list.
- Click  to edit the person information.
- Select people, and then click **Delete** to delete users.
- Search: Search by user name or user ID.

3.6 Configuring Attendance

3.6.1 Configuring Departments

Procedure

Step 1 Select **Attendance Config** > **Department Settings**.

Step 2 Click  to rename the department.

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

Figure 3-5 Create departments

Default		
ID	Department Name	Operation
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

Related Operations

You can click **Default** to restore departments to default settings.

3.6.2 Configuring Shifts

Configure shifts to define time attendance rules. Employees need to work at the time scheduled for their shift to start, and leave at the end time, except when they choose to work overtime.

Procedure

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

Step 2 Click  to configure the shift.

Figure 3-6 Create shifts

Edit Shift

X

* Shift No.

1

* Shift Name

Default

* Period 1

08:00 → 17:00

* Period 2

00:00 → 00:00

* Overtime Period

00:00 → 00:00

* Limit for Arriving Late

3

min (0-99)

* Limit for Leaving Early

5

min (0-99)

OK

Cancel

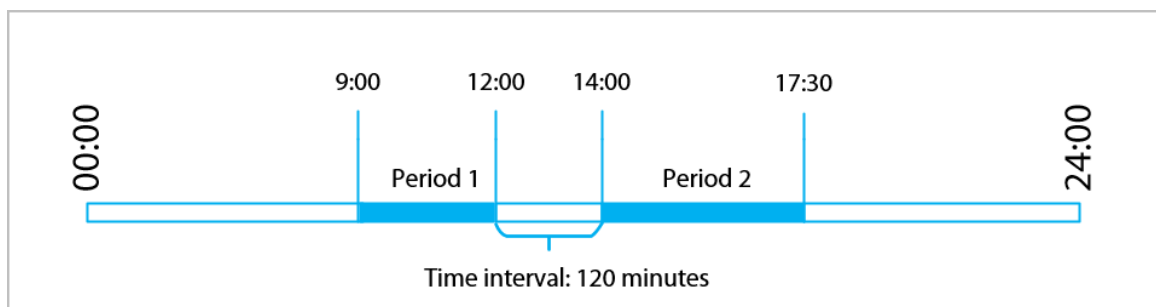
Table 3-3 Shift parameters description

Parameter	Description
Shift Name	Enter the name of the shift.
Period 1	Specify a time range when people can clock in and clock out for the workday. If you only set one attendance period, employees need to clock in and out by the designated times to avoid an anomaly appearing on their attendance record. For example, if you set 08:00 to 17:00, employees must clock in by 08:00 and clock out from 17:00 onwards. If you set 2 attendance periods, the 2 periods cannot overlap. Employees need to clock in and clock out for both periods.
Period 2	
Overtime Period	Employees who clock in or out during the defined period will be considered as working beyond their normal work hours.

Parameter	Description
Limit for Arriving Late (min)	A certain amount of time can be granted to employees to allow them to clock in a bit late and clock out a bit early. For example, if the regular time to clock in is 08:00, the tolerance period can be set as 5 minutes for employees who arrive by 08:05 to not be considered as late.
Limit for Leaving Early (min)	

- When the time interval between 2 periods is an even number, you can divide the time interval by 2, and assign the first half of the interval to the first period, which will be the clock out time. The second half of the interval should be assigned to the second period as the clock in time.

Figure 3-7 Time interval (even number)



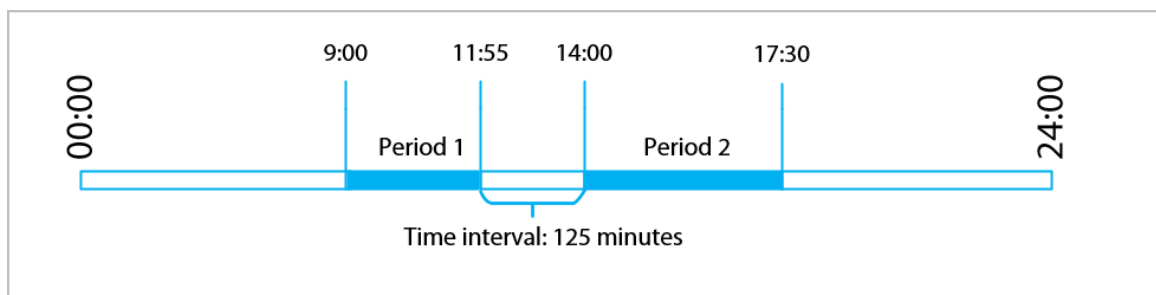
For example: If the interval is 120 minutes, then the clock-out time for period 1 is from 12:00 to 12:59, and the clock-in time for period 2 is from 13:00 to 14:00.



If a person clocks out multiple times during period 1, the latest time will be valid, and if they clock in multiple times during period 2, the earliest time will be valid.

- When the time interval between 2 periods is an odd number, the smallest portion of the interval will be assigned to the first period, which will be the clock out time. The largest portion of the interval will be assigned to the second period as the clock in time.

Figure 3-8 Time interval (even number)



For example: If the interval is 125 minutes, then the clock-out time for period 1 is from 11:55 to 12:57, and the clock-in time for period 2 is from 12:58 to 14:00. Period 1 has 62 minutes, and period 2 has 63 minutes.



If a person clocks out multiple times during period 1, the latest time will be valid, and if they clock in multiple times during period 2, the earliest time will be valid.



All attendance times are precise down to the second. For example, if the normal clock-in time is set to 8:05 AM, the employee who clocks in at 8:05:59 AM will not be considered as arriving late. But, the employee that arrives at 8:06 AM will be marked as late by 1 minute.

Step 3 Click **OK**.

Related Operations

You can click **Default** to restore shifts to factory defaults.

3.6.3 Configuring Holiday

Configure holiday plans to set periods for attendance to not be tracked.

Procedure

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

Step 2 Click **Add** to add holiday plans.

Step 3 Configure the parameters.

Figure 3-9 Create holiday plans

Add Attendance Holiday X

* Attendance Holiday No. 1 v

* Attendance Holiday Attendance Holiday for October

* Time 2024-10-01 → 2024-10-07

OK Cancel

Table 3-4 Parameters description

Parameter	Description
Attendance Holiday No.	The number of the holiday.
Attendance Holiday	The name of the holiday.
Start Time	The start and end time of the holiday.
End Time	

Step 4 Click **OK**.

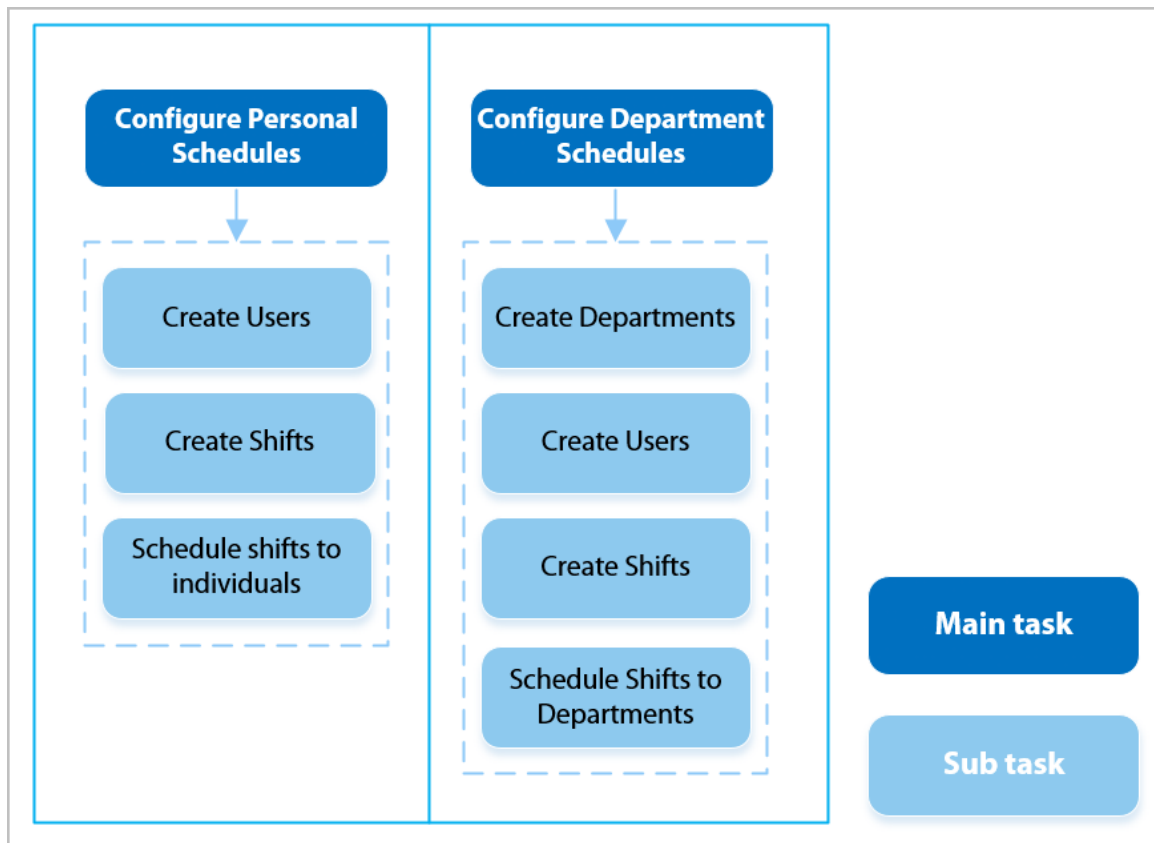
3.6.4 Configuring Work Schedules

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.

Background Information

Refer to the flowchart to configure personal schedules or department schedules.

Figure 3-10 Configuring work schedules



Procedure

Step 1 Select **Attendance Config > Schedule Config**.

Step 2 Set work schedules for individuals.

1. Click **Personal Schedule**.
2. Select a person in the person list.
3. On the calendar, select a day, and then select a shift.

You can also click **Batch Configure** to schedule shifts to multiple days.

Figure 3-11 Personal schedule

The screenshot displays the 'Personal Schedule' interface. On the left, there is a 'Person List' with three entries: '1-', '2-', and '2678490-'. The '2678490-' entry is selected. Below the list is a 'Batch Configure' button. The main area shows a calendar grid for the current month (labeled 'This Month') and the next month (labeled 'Next Month'). The calendar grid shows days of the week (Su, Mo, Tu, Th, Fr, Sa) and dates (01 to 11). A 'Select Shift' dropdown menu is open, showing options from 0-Rest to 8-Default. The calendar grid shows days of the week (Su, Mo, Tu, Th, Fr, Sa) and dates (01 to 11). A 'Batch Configure' button is visible.



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 per-defined shifts.
- 25 indicates business trip.
- 26 indicates leave of absence.

Step 3 Set works schedules for departments.

1. Click **Department Schedule**.
 2. Select a department in the department list.
 3. On the calendar, select a day, and then select a shift.
- 0 indicates rest.
 - 1 to 24 indicates the number of the per-defined shifts.
 - 25 indicates business trip.
 - 26 indicates leave of absence.

Figure 3-12 Schedule shifts to a department

The screenshot displays the 'Department Schedule' interface. On the left, a 'Department List' shows 18 default departments, with '3-Default' selected. The main area shows a weekly schedule for '3-Default' across the days of the week (Sun to Sat). The schedule is as follows:

Day	Sun	Mon	Tue	Wed	Thu	Fri	Sat
Shift	0	2	1	1	1	1	0

A 'Select Shift' dialog box is open, showing a list of shifts from '0-Rest' to '8-Default'. '2-Default' is selected in the dialog.



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

3.6.5 Configuring Attendance Mode

Procedure

Step 1 Select **Attendance Config** > **Attendance Config**.

Step 2 Enable **Local Attendance**, set the attendance mode, and then enter the verification interval..

When **Use Attendance for Unlock** is enabled, if people verify the identity for the attendance, they can unlock the door at the same time.

When an employee clocks in and out multiple times within a set interval, the earliest time will be valid.

Figure 3-13 Attendance mode

Use Attendance for Unlock ☒

Local Attendance ☒

Mode Settings
 ☒ Auto/Manual Mode
 ☐ Auto Mode
 ☐ Manual Mode
 ☐ Fixed Mode

Check In

06:00 → 09:59

Break Out

10:00 → 12:59

Break In

13:00 → 15:59

Check Out

16:00 → 20:59

Overtime Check In

00:00 → 00:00

Overtime Check Out

00:00 → 00:00

Apply

Refresh

Default

Table 3-5 Attendance mode

Parameter	Description	Attendance Mode
Auto/Manual Mode	Select the mode, select the period, and then configure the start time and the end time of each period. The screen displays the attendance status automatically after you clock in or out, but you can also manually change your attendance status using the buttons of F1 to F4.	• Check in: Clock in when your normal workday starts. • Break out: Clock out when your break starts. • Break in: Clock in when your break ends. • Check out: Clock out when your normal workday starts.
Auto Mode	Select the mode, select the period, and then configure the start time and the end time of each period. The screen displays the attendance status automatically according to your configurations. You cannot use the buttons to change the status.	• Overtime check in: Clock in when your overtime period starts. • Overtime check out: Clock out when your overtime period ends.

Parameter	Description	Attendance Mode
Manual Mode	- After you clock in or out, manually select the attendance status. - Press F1 to F4 to change the attendance mode, and then verify the identity.  The status is not displayed on the screen. After you press F1 to F4 to select the status first, the status will be displayed for 10 seconds.	
Fixed Mode	When you clock in or out, the screen will display the per-defined attendance status all the time.	

Step 3 Click **Apply**.

Related Operations

- Refresh: If you do not want to save the current changes, click **Refresh** to cancel changes and restore it to previous settings.
- Default: Restore the attendance settings to factory defaults.

3.7 Configuring Access Control

3.7.1 Configuring Access Control Parameters

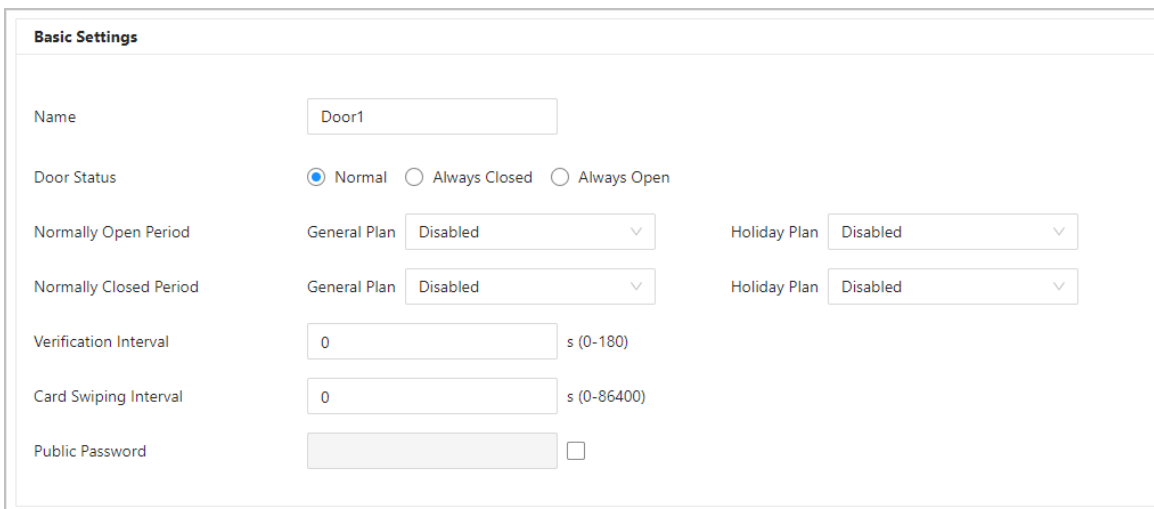
3.7.1.1 Configuring Basic Parameters

Procedure

Step 1 Select **Access Control** > **Access Control Parameters**.

Step 2 In **Basic Settings**, configure basic parameters for the access control.

Figure 3-14 Basic parameters



Basic Settings

Name: Door1

Door Status: ☒ Normal ☐ Always Closed ☐ Always Open

Normally Open Period: General Plan: Disabled Holiday Plan: Disabled

Normally Closed Period: General Plan: Disabled Holiday Plan: Disabled

Verification Interval: 0 s (0-180)

Card Swiping Interval: 0 s (0-86400)

Public Password: ☐

Table 3-6 Basic parameters description

Parameter	Description
Name	The name of the door.
Door Status	Set the door status. ● Normal: The door will be unlocked and locked according to your settings. ● Always Open: The door remains unlocked all the time. ● Always Closed: The door remains locked all the time.
Normally Open Period	When you select Normal, you can select a time template from the drop-down list. The door remains open or closed during the defined time. For details on how to configure general plans and holiday plans, see "3.7.5 Configuring Periods".  ● When normally open period conflicts with normally closed period, normally open period takes priority over normally closed period. ● When period conflict with holiday plan, holiday plans takes priority over periods.
Normally Closed Period	
Verification Interval	If you verify your identity multiple times within a defined period, only the earliest verification will be considered valid, and the door will not open after the second or later verifications. From the moment the door fails to open, you must wait for the configured verification time interval before attempting to verify your identity again.
Card Swiping Interval	For first-time verification through card, you can normally unlock the door or perform attendance, and the records are generated. Within the configured period, if you swipe the card for verification again, you cannot unlock the door or perform attendance, and the records are not generated. Please verify the identification after the configured period.  The Card Swiping Interval takes priority over Verification Interval.
Public Password	After the public password is enabled, configure the password. You can use the public password without entering the user ID to unlock the door. Only one public password is supported for one device.

Step 3 Click **Apply**.

3.7.1.2 Configuring Unlock Methods

You can use multiple unlock methods to unlock the door, such as fingerprint, card, and password. You can also combine them to create your own personal unlock method.

Procedure

Step 1 Select **Access Control** > **Access Control Parameters**.

Step 2 In **Unlock Settings**, select an unlock method.

- Combination unlock

1. Select **Combination Unlock** from the **Unlock Method** list.
2. Select **Or** or **And**.
 - ◇ Or: Use one of the selected unlock methods to open the door.
 - ◇ And: Use all the selected unlock methods to open the door.
3. Select unlock methods, and then configure other parameters.

Figure 3-15 Combination unlock

Unlock Settings

Unlock Method: Combination Unlock

Combination Method: ☒ Or ☐ And

Unlock Method (Multi-select): ☒ Card ☒ Fingerprint ☒ Password

Door Unlocked Duration: 3.0 s (0.2-600)

Apply Refresh Default

- Unlock by multiple users.
 - ◇ If only one group is added, the door unlocks only after the number of people in the group who grant access equals the defined valid number.
 - ◇ If more than one groups are added, the door unlocks only after the number of people in each group who grant access equals the defined valid number.
1. In the **Unlock Mode** list, select **Unlock by Multiple Users**.
 2. Click **Add** to add groups.
 3. Select the unlock method and users, configure the valid number, and then click **OK**.
 - ◇ You can add up to 4 groups.
 - ◇ The unlock methods only support the relationship of **Or**.
 - ◇ The valid number indicates the number of people in each group who need to verify their identities on the Device before the door unlocks. For example, if the valid number is set to 3 for a group, any 3 people in the group need to verify their identities to unlock the door.

The valid number cannot exceed the number of the users in the user list.

Figure 3-16 Add group

Add

×

No. 1

Unlock Method ... Card x

Valid No. 1

Select Person User ID/Name

	No.	User ID	Name
☒	1	1000...	10000001
☒	2	1000...	10000002
☐	3	1000...	10000003
☐	4	1000...	10000004
☐	5	1000...	10000005

Selected People Clear

No.	User ID	Name	Operation
1	100000...	100000...	
2	100000...	100000...	

OK

Cancel

Figure 3-17 Unlock by multiple users

Unlock Settings

Unlock Method

Unlock by Multiple Users

You can add up to 4 multi-person unlock groups.

Add

No.	User List	Unlock Method	Valid No.	Operation
No Data				

Verification of Multi-person Unlock Timeout Duration

20

s (10-60)

Door Unlocked Duration

3.0

s (0.2-600)

Apply

Refresh

Default

Table 3-7 Unlock settings description

Parameter	Description
Unlock Method (Multi-select)	Unlock methods might differ depending on the models of product.
Verification of Multi-person Unlock Timeout Duration	During verification, the interval between every two verifiers must be within this time period.
Door Unlock Duration	After a person is granted access, the door will remain unlocked for a defined time for the person to pass through. It ranges from 0.2 to 600 seconds.

- Unlock by period

1. In the **Unlock Method** list, select **Unlock by Period**.
2. Drag the slider to adjust time period for each day.



You can also click **Copy** to apply the configured time period to other days.

3. Select an unlock method for the time period, and then configure other parameters.

Figure 3-18 Unlock by period

Step 3 Click **Apply**.

3.7.2 Configuring Alarms

An alarm will be triggered when an abnormal access event occurs.

Procedure

- Step 1** Select **Access Control** > **Alarm** > **Alarm**.
- Step 2** Configure alarm parameters.

Figure 3-19 Alarm

Duress Alarm

☒

Anti-passback

☒

Door Detector

☒

☐ NC
☒ NO

Intrusion Alarm

☒

Unlock Timeout Alarm

☒

Unlock Timeout

60

s (1-9999)

Excessive Attempts Ala...

☒

Apply

Refresh

Default

Table 3-8 Description of alarm parameters

Parameter	Description
Duress Alarm	An alarm will be triggered when a duress card, duress password or duress fingerprint is used to unlock the door.
Door Detector	With the door detector wired to your device, alarm can be triggered when doors are opened or closed abnormally. The door detector includes 2 types, including NC detector and NO detector. • NC: The sensor is in a shorted position when the door or window is closed. • NO: An open circuit is created when the window or door is actually closed.
Intrusion Alarm	If the door is opened abnormally, an intrusion alarm will be triggered and last for a defined time.  The door detector and intrusion need to be enabled at the same time.

Parameter	Description
Unlock Timeout Alarm	When the door remains unlocked for longer than the defined timeout duration, the door timeout alarm will be triggered and last for the defined time.
Unlock Timeout	 The door detector and door timed out function need to be enabled at the same time.
Excessive Attempts Alarm	If the wrong password or card is used 5 times in a row within 60 seconds, the alarm for excessive use of illegal card will be triggered and lasts for a defined time.

Step 3 Click **Apply**.

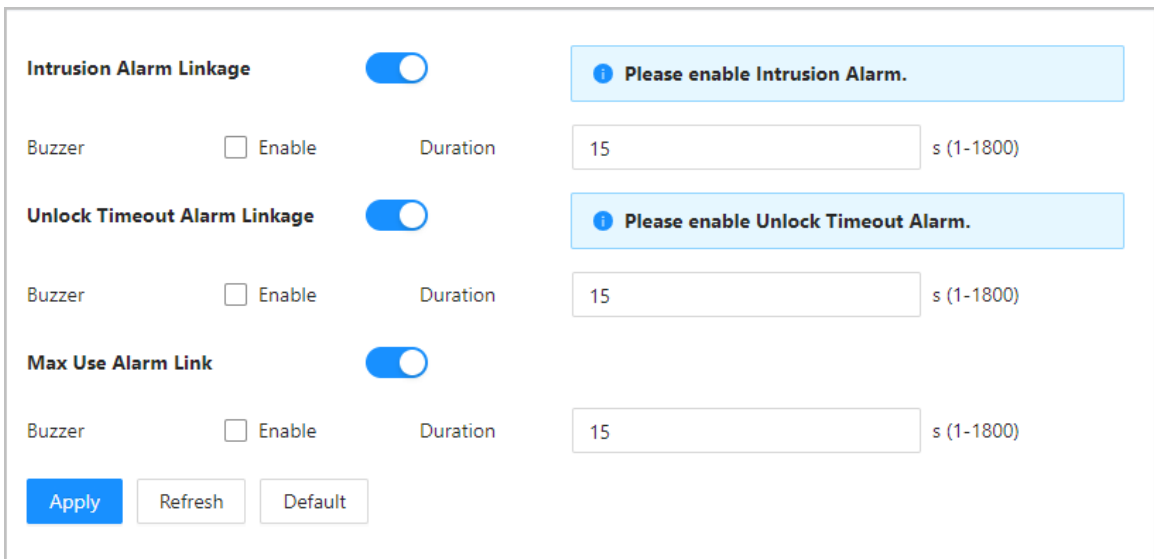
3.7.3 Configuring Alarm Event Linkage

Procedure

Step 1 On the **Main Menu**, select **Access Control** > **Alarm** > **Alarm Event Linkage**.

Step 2 Configure alarm event linkages.

Figure 3-20 Alarm event linkage



The screenshot shows the 'Alarm Event Linkage' configuration page. It contains three main sections, each with a toggle switch, a 'Buzzer' checkbox, and a 'Duration' input field.

- Intrusion Alarm Linkage:** Toggle is ON. Buzzer checkbox is unchecked. Duration is 15 s (1-1800). A blue message box says 'Please enable Intrusion Alarm.'
- Unlock Timeout Alarm Linkage:** Toggle is ON. Buzzer checkbox is unchecked. Duration is 15 s (1-1800). A blue message box says 'Please enable Unlock Timeout Alarm.'
- Max Use Alarm Link:** Toggle is ON. Buzzer checkbox is unchecked. Duration is 15 s (1-1800).

At the bottom, there are three buttons: 'Apply' (blue), 'Refresh' (white), and 'Default' (white).

Table 3-9 Alarm event linkage

Parameter	Description
Intrusion Alarm Linkage	If the door is opened abnormally, an intrusion alarm will be triggered. Buzzer: The buzzer sounds when an intrusion alarm is triggered. You can configure the alarm duration.

Parameter	Description
Unlock Timeout Alarm Linkage	When the door remains unlocked for longer than the defined timeout duration, the door timeout alarm will be triggered and last for the defined time. Buzzer: The buzzer sounds when the unlock timeout alarm is triggered. You can configure the alarm duration.
Max Use Alarm Linkage	If the wrong password or card is used 5 times in a row within 60 seconds, the alarm for excessive use of illegal card will be triggered and lasts for a defined time. Buzzer: The buzzer sounds when the excessive use alarm is triggered. You can configure the alarm duration.

Step 3 Click **Apply**.

3.7.4 Card Settings

3.7.4.1 Configuring Card Settings



This function is only available on select models.

Procedure

- Step 1 Log in to the webpage.
- Step 2 Select **Access Control** > **Card Settings** > **Card Settings**.
- Step 3 Configure the card parameters.

Figure 3-21 Card parameters

Table 3-10 Card parameters description

Item	Parameter	Description
Card No. System	Card No. System	Select decimal format or hexadecimal format for the card number when Wiegand card reader is connected. The card No. system is the same for both card number input and output.

Step 4 Click **Apply**.

3.7.4.2 Configuring Custom Conversion

When reading third-party cards using the built-in reader of the device, the external RS-485 card reader, or the external Wiegand card reader, if the actual card number does not match any card number in the system, you can configure the custom conversion for the card number to ensure that the converted card number matches the one in the system.

Procedure

Step 1 Log in to the webpage.

Step 2 Select **Access Control** > **Card Settings** > **Custom Conversion**.

Step 3 Enable the conversion function, and then select the matching mode.

- Auto match: Use the built-in conversion rule of the Device to convert the card number.
 1. Select the input type.
 - ◇ Device input: Swipe the card on the Device to read the card.
 - ◇ RS-485 input: Swipe the card on the connected RS-485 card reader to read the card.
 - ◇ Wiegand input: Swipe the card on the connected Wiegand card reader to read the card.
 2. Read the card number through the device or enter the card number before conversion, and then enter the card number after conversion.
 3. Click **Auto Match**.
 - ◇ If the card numbers are successfully matched, you can click **Export** to export the rule and import to another device for quickly switching the match rules.
 - ◇ If the card numbers failed to match, it indicates that there is no match rule in the system. You need to customized the match rule script, and select **Import Conversion Rule** to import the rule to the device.
 - ◇ If you need to modify the match rule, click **Change Matching Rule**.

Figure 3-22 Auto match (successfully matched)

The screenshot shows the 'Auto Match' configuration interface. At the top, there is an 'Enable' toggle switch that is turned on. Below it, the 'Matching Mode' is set to 'Auto Match' (selected with a radio button) and 'Import Conversion Rule' is unselected. The 'Status' is 'Applied' (selected with a radio button) and 'Default' is unselected. Under 'Input Type', three checkboxes are checked: 'Device Input', 'RS-485 Input', and 'Wiegand Input'. A table below shows the conversion of card numbers. The table has five columns: 'No.', 'Card No. Before Conversion (Device Input)', 'Card No. Before Conversion (RS-485 Input)', 'Card No. Before Conversion (Wiegand Input)', and 'Card No. After Conversion'. The first row shows a successful match for card number 1, where the 'Card No. After Conversion' is '4D3C2B1A'. Below the table, there is a green checkmark icon and the text 'Successfully Matched' with a sub-note 'This rule will automatically apply to this device.' At the bottom, there are two buttons: 'Change Matching Rule' and 'Export'.

No.	Card No. Before Conversion (Device Input)	Card No. Before Conversion (RS-485 Input)	Card No. Before Conversion (Wiegand Input)	Card No. After Conversion
1	1A283C4D	1A283C4D	1A283C4D	4D3C2B1A
2				
3				

- Import conversion rule: Import other rules to convert the card number.
Click **Upload File** , select the rule file, and then click **Open**.

Figure 3-23 Import conversion rule

The screenshot shows the 'Import Conversion Rule' configuration interface. At the top, there is an 'Enable' toggle switch that is turned on. Below it, the 'Matching Mode' is set to 'Import Conversion Rule' (selected with a radio button) and 'Auto Match' is unselected. The 'Version' is '2025-03-31'. There are two buttons: 'Upload File' and 'Default'. A blue box contains the text: 'You can only upload files in zip format and the size must not exceed 1 MB.'

3.7.5 Configuring Periods

Configure general plans and holiday plans, and then you can define when a user has the permissions to unlock doors.

3.7.5.1 Configuring General Plan

You can configure up to 128 periods (from No.0 through No.127) of general plans. In each period, you need to configure door access schedules for a whole week. People can only unlock the door during the scheduled time.

Procedure

- Step 1 Log in to the webpage.

Step 2 Select **Access Control** > **Period Config** > **General Plan**.

Step 3 Click **Add**.

1. Configure the plan number and the plan name.
2. Drag the time slider to configure time for each day.
3. (Optional) Click **Copy** to copy the configuration to the rest of days.

Figure 3-24 Configure general plan

The screenshot shows a web-based configuration window titled "Add". It contains the following elements:

- No.:** A dropdown menu with the value "0".
- General Plan Name:** A text input field containing "Plan 1".
- Time Plan:** A table with 7 rows (Sun, Mon, Tue, Wed, Thu, Fri, Sat) and 12 columns (0-11). A time slider is positioned above the table, and a pop-up window shows the selected time range from 12:30:00 to 23:59:59. Each row has a "Copy" button to its right.
- Buttons:** "OK" and "Cancel" buttons are located at the bottom right of the window.

Step 4 Click **OK**.

3.7.5.2 Configuring Holiday Plan

You can configure up to 128 holiday groups (from No.0 through No.127), and for each holiday group, you can add up to 16 holidays in it. After that, you can assign the configured holiday groups to the holiday plan. Users can only unlock the door during the defined time of the holiday plan.

Procedure

Step 1 Log in to the webpage.

Step 2 Select **Access Control** > **Period Config** > **Holiday Plan**.

Step 3 Click **Holiday Management**, and then click **Add**.

1. Select a number for the holiday group, and then enter a name for the group.

Figure 3-25 Add a holiday group

The 'Add' dialog box contains the following fields and elements:

- No.:** A dropdown menu with the value '2' selected.
- Holiday Group Name:** A text input field containing 'Holiday Group for 2023'.
- Holiday Group Config:** A section containing an 'Add' button and a table.
- Table:** A table with 5 columns: No., Holiday Name, Start Time, End Time, and Operation. It contains one row for 'National Day' from '2023-10-01' to '2023-10-07'.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom right.

No.	Holiday Name	Start Time	End Time	Operation
1	National Day	2023-10-01	2023-10-07	

2. Click **Add** , add a holiday to a holiday group, and then click **OK**.

Figure 3-26 Add a holiday to a holiday group

The 'Edit' dialog box contains the following fields and elements:

- Holiday Name:** A text input field containing 'National Day'.
- * Period:** A date range selector showing '2023-10-01' to '2023-10-07' with a calendar icon.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom right.

Step 4 Click **OK**.

Step 5 Click **Plan Management** , and then click **Add**.

1. Select a number for the holiday plan, and then enter a name for it.
2. Select a holiday group, and then drag the slider to configure time for each day.
Supports adding up to 4 time sections on a day.

Figure 3-27 Add holiday plan

The screenshot shows a software interface for editing a holiday plan. The main window is titled 'Edit' and contains the following fields:

- No.:** A dropdown menu with the value '0'.
- Holiday Plan Name:** A text input field containing 'Holiday plan for 2023'.
- Holiday Group No.:** A dropdown menu with the value '1'.
- Time Plan:** A section containing a calendar grid and a time selection pop-up.
 - The calendar grid has a header row with days 0 through 8, and a row below labeled 'Holid'. A blue highlight covers the area from day 8 to day 24.
 - The time selection pop-up is titled 'Time' and shows a range from '08:30:00' to '23:59:59'. It includes 'OK', 'Delete', and 'Copy' buttons.

At the bottom right of the 'Edit' window are 'OK' and 'Cancel' buttons.

Step 6 Click **OK**.

3.8 Audio

3.8.1 Configuring Audio Parameters

Configure voice recognition and voice announcements for successful or failed verification on the local main interface.

Procedure

- Step 1 Select **Audio** > **Audio Config**.
- Step 2 Configure audio parameters, and then click **Apply**.

Figure 3-28 Audio

Speaker Volume
 (0-100) ⓘ

Key Sound
☐

Voice Broadcast Settings

Successfully verified. ▼

Period1
 ⓘ
 ⓘ
☐ Enable

Audio File
 ▼

Period2
 ⓘ
 ⓘ
☐ Enable

Audio File
 ▼

Period3
 ⓘ
 ⓘ
☐ Enable

Audio File
 ▼

Period4
 ⓘ
 ⓘ
☐ Enable

Audio File
 ▼

Figure 3-29 DND

DND Mode
☒

Time

Period 1
 → ⓘ

Period 2
 → ⓘ

Period 3
 → ⓘ

Period 4
 → ⓘ

Table 3-11 Description of audio parameters

Parameters	Description
Speaker Volume	Adjust the speaker volume. 📖
	Only available on select models.

Parameters	Description
Key Sound	When enabled, touchscreen devices will produce a prompt sound for local touch operations, while non-touchscreen devices will produce a prompt sound for key/button operations.
Voice Broadcast Settings	Set voice prompts for successful and failed verification. Supports up to 6 time periods.  Only available on select models. Click corresponding time period to enable it. Configure the time period, and select an audio file. Supports selecting audio files uploaded in Audio > Audio File. For details, see "3.8.2 Managing Audio Files" .
DND Mode	When enabled, there will be no prompt sounds for local verification (such as door access or attendance) during the configured time periods. Supports up to 4 time periods.

3.8.2 Managing Audio Files

Background Information

Upload and manage audio files.



It is only supported on select models.

Procedure

- Step 1 Select **Audio > Audio File**.
- Step 2 Click **Upload** , select audio files, and then click **Open**.
- Step 3 (Optional) Click ► to listen to the audio file.

Figure 3-30 Manage audio file

 Supports MP3. The audio file must not exceed 100KB, and the audio sampling rate is 16K.

 Upload

No.	Name	Operation
 No Data		

3.9 Communication Settings

3.9.1 Configuring TCP/IP

You need to configure IP address of Device to make sure that it can communicate with other devices.

Procedure

Step 1 Select **Communication Settings** > **Network Setting** > **TCP/IP**.

Step 2 Configure the parameters.

Figure 3-31 TCP/IP

The screenshot displays the TCP/IP configuration window. At the top, the 'NIC' is set to 'NIC 1'. The 'Mode' is configured to 'Static' (selected with a radio button), with 'DHCP' also available. Below this, the 'MAC Address' is shown as a series of eight hexadecimal digits. The 'IP Version' is set to 'IPv4'. The 'IP Address', 'Subnet Mask', 'Default Gateway', 'Preferred DNS', and 'Alternate DNS' fields are each represented by a row of four hexadecimal input boxes. At the bottom, the 'MTU' is set to '1500'. Three buttons are located at the very bottom: 'Apply' (highlighted in blue), 'Refresh', and 'Default'.

Table 3-12 Description of TCP/IP

Parameter	Description
Mode	• Static: Manually enter IP address, subnet mask, and gateway. • DHCP: It stands for Dynamic Host Configuration Protocol. When DHCP is turned on, the Device will automatically be assigned with IP address, subnet mask, and gateway.
MAC Address	MAC address of the Device.
IP Version	IPv4 or IPv6.
IP Address	If you set the mode to Static , configure the IP address, subnet mask and gateway.
Subnet Mask	
Default Gateway	
	 • IPv6 address is represented in hexadecimal. • IPv6 version do not require setting subnet masks. • The IP address and default gateway must be in the same network segment.
Preferred DNS	Set IP address of the preferred DNS server.
Alternate DNS	Set IP address of the alternate DNS server.
MTU	MTU (Maximum Transmission Unit) refers to the maximum size of data that can be transmitted in a single network packet in computer networks. A larger MTU value can improve network transmission efficiency by reducing the number of packets and associated network overhead. If a device along the network path is unable to handle packets of a specific size, it can result in packet fragmentation or transmission errors. In Ethernet networks, the common MTU value is 1500 bytes. However, in certain cases such as using PPPoE or VPN, smaller MTU values may be required to accommodate the requirements of specific network protocols or services. The following are recommended MTU values for reference: • 1500: Maximum value for Ethernet packets, also the default value. This is a typical setting for network connections without PPPoE and VPN, some routers, network adapters, and switches. • 1492: Optimal value for PPPoE • 1468: Optimal value for DHCP. • 1450: Optimal value for VPN.

Step 3 Click **OK**.

3.9.2 Configuring Wi-Fi



- The Wi-Fi function is available on select models.
- The Wi-Fi and Wi-Fi AP cannot be enabled at the same time.

Procedure

Step 1 Select **Communication Settings** > **Network Setting** > **Wi-Fi**.

Step 2 Turn on Wi-Fi.

All available Wi-Fi are displayed.

Figure 3-32 Wi-Fi



- Wi-Fi and Wi-Fi AP cannot be enabled at the same time.
- Wi-Fi function is only available on select models.

Step 3 Click +, and then enter the password of the Wi-Fi.

The Wi-Fi is connected.

Related Operations

- DHCP: Enabled this function and click **Apply**, the Device will automatically be assigned a Wi-Fi address.
- Static: Enable this function, manually enter a Wi-Fi address, and then click **Apply**, the Device will connect to the Wi-Fi.

3.9.3 Configuring Wi-Fi AP



- The Wi-Fi function is available on select models.
- The Wi-Fi and Wi-Fi AP cannot be enabled at the same time.

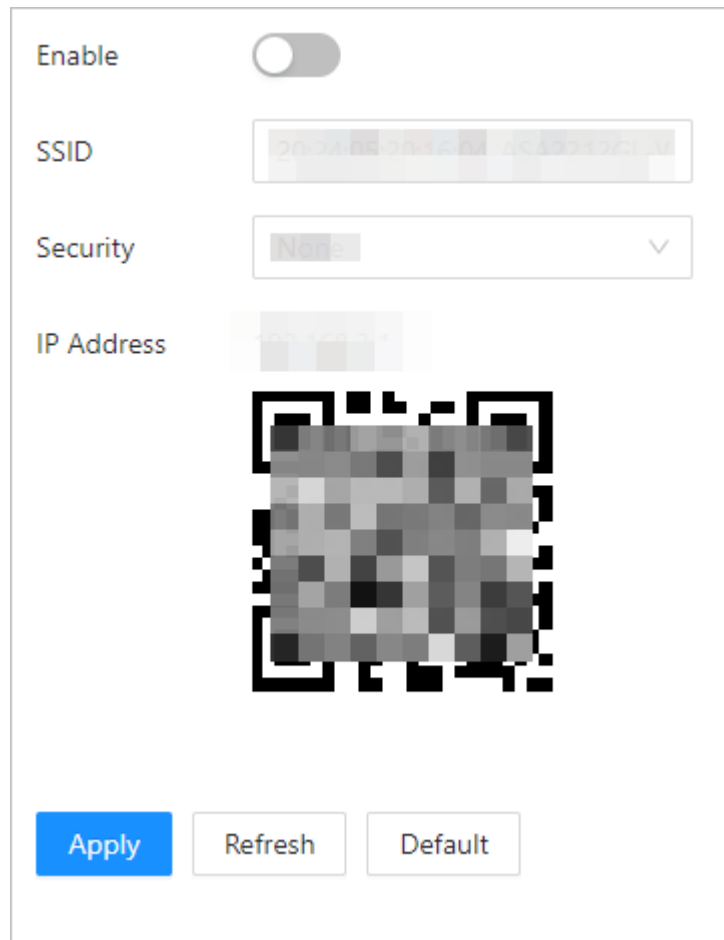
Procedure

Step 1 Select **Communication Settings** > **Network Setting** > **Wi-Fi AP**.

Step 2 Enable the function, and then click **Apply**.

If you select **WPA2-Personal** as **Security**, you can configure the password for Wi-Fi AP connection. If you select **None**, you can directly connect to the Wi-Fi AP without entering the password.

Figure 3-33 Wi-Fi AP

The image shows a web-based configuration interface for a Wi-Fi Access Point (AP). It features a toggle switch for 'Enable', which is currently turned off. Below this are input fields for 'SSID' (containing a blurred alphanumeric string), 'Security' (a dropdown menu showing 'None'), and 'IP Address' (containing a blurred IP address). A large QR code is displayed in the center of the interface. At the bottom, there are three buttons: 'Apply' (highlighted in blue), 'Refresh', and 'Default'.

Results

After enabled, you can connect to the Device Wi-Fi through your phone, and log in to the webpage of the Device on your phone.

3.9.4 Configuring Port

You can limit access to the Device at the same time through webpage, desktop client and mobile client.

Procedure

- Step 1 Select **Communication Settings** > **Network Setting** > **Port**.
- Step 2 Configure the ports.

Figure 3-34 Configure ports

Max Connection	50	(1-50)
TCP Port	37777	(1025-65535)
HTTP Port	80	
HTTPS Port	443	
Apply Refresh Default		



You need to restart the Device to make the configurations effective after you configure parameters.

Table 3-13 Description of ports

Parameter	Description
Max Connection	You can set the maximum number of clients (such as webpage, desktop client and mobile client) that can access the Device at the same time.
TCP Port	Default value is 37777.
HTTP Port	Default value is 80. If you have changed the port number, add the port number after the IP address when access the webpage.
HTTPS Port	Default value is 443.

Step 3 Click **Apply**.

3.9.5 Configuring Basic Service

When you want to connect the Device to a third-party platform, turn on the CGI and ONVIF functions.

Procedure

- Step 1 Select **Communication Settings** > **Network Settings** > **Basic Services**.
- Step 2 Configure the basic service.

Figure 3-35 Basic service

SSH ☒

Multicast/Broadcast Search ☒

CGI ☒

ONVIF ☒

Emergency Maintenance ☐

i For easy access to our after-sales service, enable this function. If the device has any trouble performing functions, such as updating, the system will automatically enable this function.

Private Protocol Authentication Mode Security Mode (Recommended) ▾

Private Protocol ☒

*Before enabling private protocol TLS, make sure that the corresponding device or software supports this function.

TLSv1.1 ☐

LLDP ☐

Apply Refresh Default

Table 3-14 Basic service parameter description

Parameter	Description
SSH	SSH, or Secure Shell Protocol, is a remote administration protocol that allows users to access, control, and modify their remote servers over the internet.
Mutlicast/Broadcast Search	Search for devices through multicast or broadcast protocol.
CGI	The Common Gateway Interface (CGI) is an intersection between web servers through which the standardized data exchange between external applications and servers is possible.
ONVIF	ONVIF stands for Open Network Video Interface Forum. Its aim is to provide a standard for the interface between different IP-based security devices. These standardized ONVIF specifications are like a common language that all devices can use to communicate.
Emergency Maintenance	It is turned on by default.
Private Protocol Authentication Mode	Set the authentication mode, including safe mode and compatibility mode. It is recommended to choose Security Mode. - Security Mode (recommended): Does not support accessing the device through Digest, DES, and plaintext authentication methods, improving device security. - Compatible Mode: Supports accessing the device through Digest, DES, and plaintext authentication methods, with reduced security.
Private Protocol	The platform adds devices through private protocol.

Parameter	Description
TLSv1.1	TLSv1.1 refers to Transport Layer Security version 1.1. TLS is a cryptographic protocol designed to provide secure and authenticated communication over a computer network.  Security risks might present when TLSv1.1 is enabled. Please be advised.
LLDP	LLDP is the abbreviation for Link Layer Discovery Protocol, which is a data link layer protocol. It allows network devices, such as switches, routers, or servers, to exchange information about their identities and capabilities with each other. The LLDP protocol helps network administrators gain a better understanding of network topology and provides a standardized way to automate the discovery and mapping of connections between network devices. This makes it easier to perform network configuration, troubleshoot issues, and optimize performance.

Step 3 Click **Apply**.

3.9.6 Configuring Cloud Service

The cloud service provides a NAT penetration service. Users can manage multiple devices through DMSS. You do not have to apply for dynamic domain name, configure port mapping or deploy server.

Procedure

Step 1 On the home page, select **Communication Settings > Network Setting > Cloud Service**.

Step 2 Turn on the cloud service function.

The cloud service goes online if the P2P and PaaS are online.

Figure 3-36 Cloud service

Enable ☒

After the function is enabled and the device connects to the network, we will collect device information such as the IP address, MAC address, device name and serial number. The collected information will only be used to remotely access the device. If you do not want to enable this function, please clear the selection from the check box.

P2P Status ● Offline

PaaS Status ● Offline

SN 8[REDACTED]759



Apply

Refresh

Step 3 Click **Apply**.

Step 4 Scan the QR code with DMSS to add the device.

3.9.7 Configuring SDK Auto Registration

The auto registration enables the devices to be added to the management platform without manual input of device information such as IP address and port.

Background Information

The auto registration only supports SDK.

Procedure

Step 1 On the home page, select **Network Setting** > **SDK Auto Registration**.

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

67

Figure 3-37 Auto Registration

Table 3-15 Automatic registration description

Parameter	Description
Status	Displays the connection status of auto registration.
Server Address	The IP address or the domain name of the server.
Port	The port of the server that is used for automatic registration.
Registration ID	The registration ID (user defined) of the device. Adding the device to the management by entering the registration ID on the platform.

Step 3 Click **Apply**.

3.9.8 Configuring CGI Auto Registration

Connect to a third-party platform through CGI protocol.

Background Information



Only supports IPv4.

Procedure

Step 1 On the home page, select **Communication Settings** > **Network Settings** > **CGI Auto Registration**.

Step 2 Enable this function, and then click  to configure the parameters.

Table 3-16 Automatic registration description

Parameter	Description
Device ID	Supports up to 32 bytes, including Chinese, numbers, letters, and special characters.
Address Type	Supports 2 methods to register. - Host IP: Enter the IP address of the third-party platform. - Domain Name: Enter the domain name of the third-party platform.
Host IP	
Domain Name	
HTTPS	Access the third-party platform through HTTPS. HTTPS secures communication over a computer network.

Step 3 Click **OK**.

3.9.9 Configuring Auto Upload

Send user information and unlock records through to the management platform.

Procedure

Step 1 On the home page, select **Communication Settings > Network Settings > Auto Upload**.

Step 2 (Optional) Enable **Push Person Info**.

When the user information is updated or new users are added, the Device will automatically push user information to the management platform.

Step 3 Enable HTTP upload mode.

Step 4 Click **Add**, and then configure parameters.

Figure 3-38 Automatic upload

Table 3-17 Parameters description

Parameter	Description
IP/Domain Name	The IP or domain name of the management platform.
Port	The port of the management platform.
HTTPS	Access the management platform through HTTPS. HTTPS secures communication over a computer network.
Authentication	Enable account authentication when you access the management platform. Login username and password are required.

Parameter	Description
Event Type	Select the type of event that will be pushed to the management platform.  • Before you use this function, enable Push Person Info. • Person information can only be pushed to one management platform and unlock records can be pushed to multiple management platforms.

Step 5 Click **Apply**.

3.10 Configuring the System

3.10.1 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.

3.10.1.1 Adding Administrators

You can add new administrator accounts, and then they can log in to the webpage of the Device.

Procedure

Step 1 On the home page, select **System** > **Account** > **Account**.

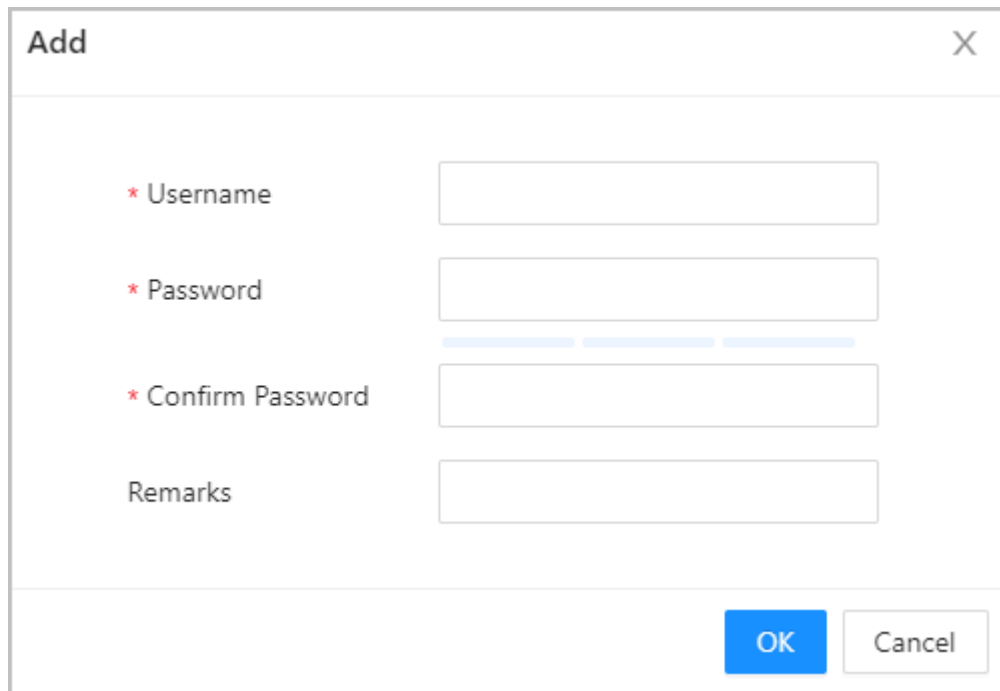
Step 2 Click **Add**, and enter the user information.



- 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 3-39 Add administrators



The screenshot shows a web-based dialog box titled "Add" with a close button (X) in the top right corner. The dialog contains four input fields arranged vertically. The first three fields are required, indicated by a red asterisk (*): "Username", "Password", and "Confirm Password". The fourth field is labeled "Remarks". Below the input fields, there are two buttons: "OK" (blue) and "Cancel" (white with a grey border).

Step 3 Click **OK**.



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

3.10.1.2 Adding ONVIF Users

Background Information

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 **System** > **Account** > **ONVIF User**.

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

Figure 3-40 Add ONVIF user

The screenshot shows a dialog box titled "Add" with a close button (X) in the top right corner. Inside the dialog, there are four required fields, each marked with a red asterisk (*):

- * Username**: A text input field.
- * Password**: A text input field with a strength indicator bar below it.
- * Confirm Password**: A text input field.
- * Group**: A dropdown menu with a downward arrow icon.

At the bottom right of the dialog, there are two buttons: a blue "OK" button and a white "Cancel" button with a gray border.

Table 3-18 ONVIF user description

Parameter	Description
Username	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 @.
Password	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 ' " ; &).
Group	There three permission groups which represents different permission levels. ● admin: You can view and manage other user accounts on the ONVIF Device Manager. ● Operator: You cannot view or manage other user accounts on the ONVIF Device Manager. ● User: You cannot view or manage other user accounts and system logs on the ONVIF Device Manager.

Step 3 Click **OK**.

3.10.1.3 Resetting the Password

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

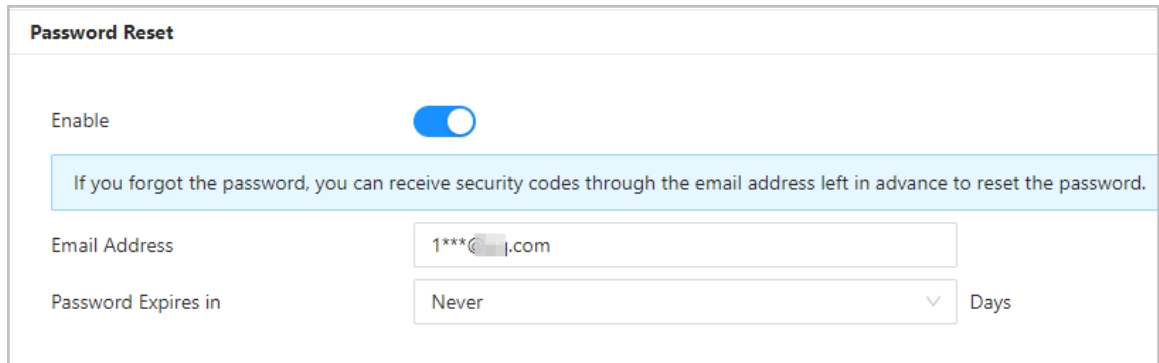
Procedure

Step 1 Select **System** > **Account** > **Account**.

Step 2 Enter the email address, and set the password expiration time.

Step 3 Turn on the password reset function.

Figure 3-41 Reset Password



If you forgot the password, you can receive security codes through the linked email address to reset the password.

Step 4 Click **Apply**.

3.10.2 Viewing Online Users

You can view online users who currently log in to the webpage. On the home page, select **System > Online User**.

3.10.3 Configuring Time

Procedure

- Step 1 Log in to the webpage.
- Step 2 Select **System > Time**.
- Step 3 Configure the time of the Platform.

Figure 3-42 Date settings

Time and Time Zone



Date :

2024-08-05 Monday

Time :

18:50:31

Time

☒ Manually Set

☐ NTP

System Time

2024-08-05 18:50:31



Sync PC

Time Format

YYYY-MM-DD



24-Hour



Time Zone

(UTC+09:30)



DST

Enable

☐

Type

☒ Date

☐ Week

Start Time

Jan



1



00:00



End Time

Jan



2



00:00



Apply

Refresh

Default

Table 3-19 Time settings description

Parameter	Description
Time	- Manual Set: Manually enter the time or you can click Sync Time to sync time with computer. - NTP: The Device will automatically sync the time with the NTP server. Server : Enter the domain of the NTP server. Port : Enter the port of the NTP server. Interval : Enter its time with the synchronization interval.
Time Format	Select the time format.
Time Zone	Enter the time zone.

Parameter	Description
DST	1. (Optional) Enable DST. 2. Select Date or Week from the Type. 3. Configure the start time and end time of the DST.

Step 4 Click **Apply**.

3.10.4 Configuring Ringtone

Configure the time when the bell rings as a reminder.

Procedure

Step 1 Log in to the webpage.

Step 2 Select **System** > **Local Device Ringer**.

Step 3 Click  to configure the item when the bell rings, and then click **OK**.

Table 3-20 Parameters description

Parameter	Description
Time	The time when the bell rings.
Ringtone Duration (sec)	The ring duration.
Repeat Time	The bell rings according to the configured repeat time. For example, if you set repeat time to Monday, the bell rings every Monday.

3.10.5 Configuring Always On

Procedure

Step 1 On the home page, select **System** > **Always-On Config**.

Step 2 Click , and then click **Apply**

The screen will stay on during the set time period after being enabled.



Keeping the screen on for extended periods might affect its lifespan. It is recommended that you use more than 8 hours of continuous screen-on time per day.

Step 3 Configure always on period, and then click **Apply**.

Figure 3-43 Always on

Display Always On

To help extend the lifespan of your screen, we recommend you limit the time it stays on to no more than 8 hours a day.

Period 1

08:00

→

18:00

Period 2

00:00

→

00:00

Period 3

00:00

→

00:00

Period 4

00:00

→

00:00

Apply

Refresh

Default

3.11 Maintenance Center

3.11.1 One-click Diagnosis

The system automatically diagnoses the configurations and the status of the device to improve its performance.

Procedure

Step 1

On the home page, select **Maintenance Center** > **One-click Diagnosis**.

Step 2

Click **Diagnose**.

The system automatically diagnoses the configurations and the status of the device and display diagnosis results after it completes.

Step 3

(Optional) Click **Details** to view details of abnormal items.

You can ignore the abnormality or optimize it. You can also click **Diagnose Again** to perform automatic diagnosis again.

Figure 3-44 One-click diagnosis

One-click Diagnosis

One-click diagnosis detects the configurations and status of your device to improve its performance.

The last scanning time: 2023-10-12 11:47:11

Diagnose Again

Network Condition-3 records

IP

IP Address Config

Normal

Checks if the IP address configuration is normal.

DHCP

DHCP

Normal

Checks if the DHCP function is normal.

Network Routing

Abnormal

Checks if the routing configuration is normal.

Details

Working Condition-1 records

Power Supply

Abnormal

Checks if the power is being normally supplied.

Details

76

3.11.2 System Information

3.11.2.1 Viewing Version Information

On the webpage, select **Maintenance Center** > **System Info** > **Version**, and you can view version information of the Device.

3.11.2.2 Viewing Legal Information

On the home page, select **Maintenance Center** > **System Info** > **Legal Info**, and you can view the software license agreement, privacy policy and open source software notice.

3.11.3 Data Capacity

You can see how many users, cards and face images that the Device can store.

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

3.11.4 Viewing Logs

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

3.11.4.1 System Logs

View and search for system logs.

Procedure

- Step 1 Log in to the webpage.
- Step 2 Select **Maintenance Center** > **Log** > **Log**.
- Step 3 Select the time range and the log type, and then click **Search**.

Related Operations

- Click **Export** to export the searched logs to your local computer.
- Click **Encrypt Log Backup**, and then enter a password. The exported file can be opened only after entering the password.
- Click  to view details of a log.

3.11.4.2 Unlock Records

Search for unlock records and export them.

Procedure

- Step 1 Log in to the webpage.
- Step 2 Select **Maintenance Center** > **Log** > **Unlock Records**.
- Step 3 Select the time range and the type, and then click **Search**.

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

3.11.4.3 Attendance Records

View attendance records.

Procedure

- Step 1 Log in to the webpage.
- Step 2 Select **Maintenance Center > Log > Attendance Records**.
- Step 3 Select the type and the time range.
- Step 4 Enter the admin ID, and then click **Search**.

3.11.4.4 Alarm Logs

View alarm logs.

Procedure

- Step 1 Log in to the webpage.
- Step 2 Select **Maintenance Center > Log > Alarm Logs**.
- Step 3 Select the type and the time range.
- Step 4 Enter the admin ID, and then click **Search**.

3.11.4.5 Admin Logs

Search for admin logs by using admin ID.

Procedure

- Step 1 Log in to the webpage.
- Step 2 Select **Maintenance Center > Log > Admin Logs**.
- Step 3 Enter the admin ID, and then click **Search**.
Click **Export** to export admin logs.

3.11.4.6 USB Management

Export user information from/to USB.

Procedure

- Step 1 Log in to the webpage.
- Step 2 Select **Maintenance Center > Log > USB Management**.



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

- Step 3 Select a data type, and then click **USB Import** or **USB Export** to import or export the data.

3.11.5 Maintenance Management

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

3.11.5.1 Exporting and Importing Configuration Files

You can import and export the configuration file for the Device. When you want to apply the same configurations to multiple devices, you can import the configuration file to them.

Procedure

Step 1 Log in to the webpage.

Step 2 Select **Maintenance Center > Maintenance Management > Config.**

Figure 3-45 Configuration management

Step 3 Export or import configuration files.

- Export the configuration file.

Click **Export Configuration File** to download the file to the local computer.



The IP will not be exported.

- Import the configuration file.

1. Click **Browse** to select the configuration file.
2. Click **Import configuration.**



Configuration files can only be imported to devices that have the same model.

3.11.5.2 Configuring the Fingerprint Similarity Threshold

Configure the fingerprint similarity threshold. The higher the value is, the higher accuracy is, and the lower the pass rate.

Procedure

Step 1 Log in to the webpage.

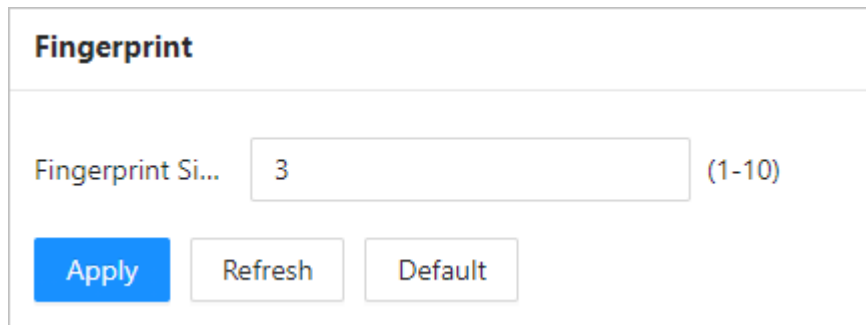
Step 2 Select **Maintenance Center > Maintenance Management > Config.**

Step 3 Enter the similarity threshold, and then click **Apply.**



- The parameter is available on the modular access controller with the fingerprint module.
- The parameter is available on the access controller with fingerprint function.

Figure 3-46 Fingerprint similarity threshold



The screenshot shows a web interface titled "Fingerprint". Below the title is a label "Fingerprint Si..." followed by a text input field containing the number "3". To the right of the input field is the range "(1-10)". Below the input field are three buttons: "Apply" (blue), "Refresh" (light gray), and "Default" (light gray).

3.11.5.3 Restoring the Factory Default Settings

Procedure

Step 1 Select **Maintenance Center** > **Maintenance Management** > **Config**.



Restoring the **Device** to its default configurations will result in data loss. Please be advised.

Step 2 Restore to the factory default settings if necessary.

- **Factory Defaults** : Resets all the configurations of the Device and delete all the data.
- **Restore to Default (Except for User Info and Logs)** : Resets the configurations of the Device and deletes all the data except for user information and logs.

3.11.5.4 Maintenance

Regularly restart the Device during its idle time to improve its performance.

Procedure

Step 1 Log in to the webpage.

Step 2 Select **Maintenance Center** > **Maintenance Management** > **Maintenance**.

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

The Device will restart at the scheduled time, or you can click **Restart** to restart it immediately.

3.11.6 Updating the System



- Use the correct update file. Make sure that you get the correct update file from technical support.
- Do not disconnect the power supply or network, and do not restart or shutdown the Device during the update.
- Update to a lower version may cause potential risks. Please be advised.
- If you start the Device for the first time or restore the Device to factory default settings, the Device automatically backups the system files within the first 10 minutes. Please do not update in this period.

3.11.6.1 File Update

Procedure

- Step 1 On the home page, select **Maintenance Center** > **Update**.
- Step 2 In **File Update**, click **Browse**, and then upload the update file.



The update file should be a .bin file.

- Step 3 Click **Update**.
- The Device will restart after the update finishes.

3.11.6.2 Online Update

Procedure

- Step 1 On the home page, select **Maintenance Center** > **Update**.
- Step 2 In the **Online Update** area, select an update method.
- Select **Auto Check for Updates**, and the Device will automatically check for the latest version update.
 - Select **Manual Check**, and you can immediately check whether the latest version is available.
- Step 3 (Optional) Click **Update Now** to update the Device immediately.

3.11.7 Advanced Maintenance

Acquire device information and capture packet to make easier for maintenance personnel to perform troubleshooting.

3.11.7.1 Exporting

Procedure

- Step 1 On the home page, select **Maintenance Center** > **Advanced Maintenance** > **Export**.
- Step 2 Click **Export** to export the serial number, firmware version, device operation logs and configuration information.

3.11.7.2 Packet Capture

Procedure

- Step 1 On the home page, select **Maintenance Center** > **Advanced Maintenance** > **Packet Capture**.

Figure 3-47 Packet Capture

Packet Capture							
NIC	Device Address	IP 1: Port 1		IP 2: Port 2		Packet Sniffer Size	Packet Sniffer Backup
eth0	192.168.1.166	Optional	Optional	Optional	Optional	0.00MB	►
eth2	192.168.1.101	Optional	Optional	Optional	Optional	0.00MB	►

Step 2 Enter the IP address, click .

 changes to .

Step 3 After you acquired enough data, click .

Captured packets are automatically downloaded to your local computer.

3.12 Security Settings (Optional)

3.12.1 Security Status

Scan the users, service, and security modules to check the security status of the Device.

Background Information

- User and service detection: Check whether the current configuration conforms to recommendation.
- Security modules scanning: Scan the running status of security modules, such as audio and video transmission, trusted protection, securing warning and attack defense, not detect whether they are enabled.

Procedure

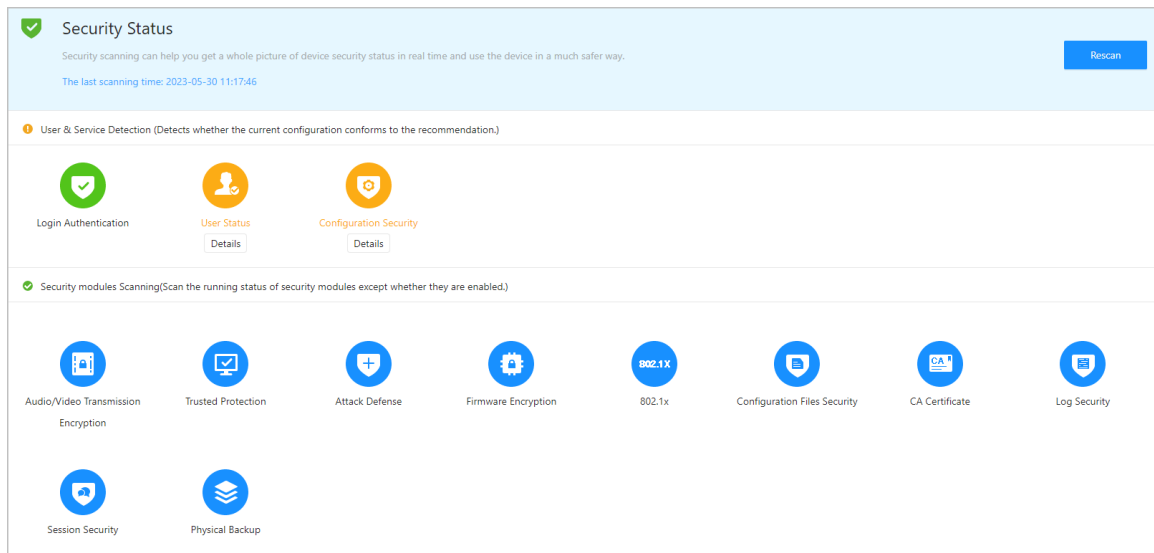
Step 1 Select  > **Security Status**.

Step 2 Click **Rescan** to perform a security scan of the Device.



Hover over the icons of the security modules to see their running status.

Figure 3-48 Security Status



Related Operations

After you perform the scan, the results will be displayed in different colors. Yellow indicates that the security modules are abnormal, and green indicates that the security modules are normal.

- Click **Details** to view the details on the results of the scan.
- Click **Ignore** to ignore the abnormality, and it will not be scanned. The abnormality that was ignored will be highlighted in grey.
- Click **Optimize** to troubleshoot the abnormality.

3.12.2 Configuring System Service

Create a certificate or upload an authenticated certificate, and then you can log in to the webpage through HTTPS on your computer. HTTPS secures communication over a computer network.

Procedure

Step 1 Select  > **System Service** > **System Service**.

Step 2 Turn on the HTTPS service.



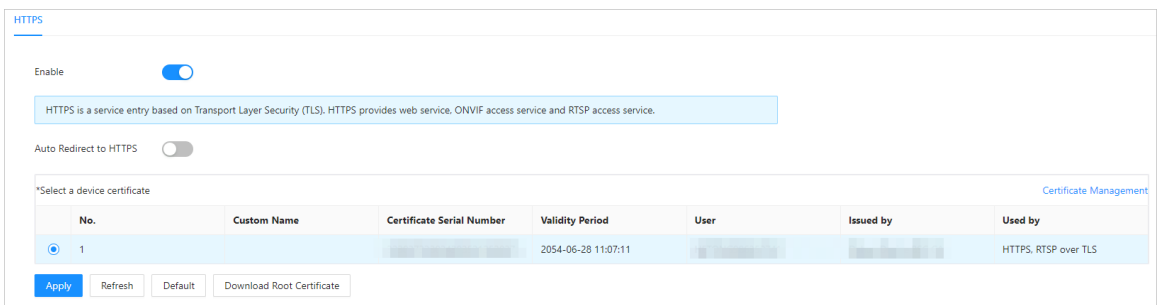
If you turn on the compatible with TLS v1.1 and earlier versions, security risks might occur. Please be advised.

Step 3 Select the certificate.



If there are no certificates in the list, click **Certificate Management** to upload a certificate.

Figure 3-49 System service



No.	Custom Name	Certificate Serial Number	Validity Period	User	Issued by	Used by
1			2054-06-28 11:07:11			HTTPS, RTSP over TLS

Step 4 Click **Apply**.

Enter "https://IP address: httpsport" in a web browser. If the certificate is installed, you can log in to the webpage successfully. If not, the webpage will display the certificate as wrong or untrusted.

3.12.3 Attack Defense

3.12.3.1 Configuring Firewall

Configure firewall to limit access to the Device.

Procedure

Step 1 Select  > **Attack Defense** > **Firewall**.

Step 2 Click  to enable the firewall function.

Figure 3-50 Firewall

Firewall Account Lockout Anti-DoS Attack

Enable ☒

Mode ☒ Allowlist ☐ Blocklist

Only source hosts whose IP/MAC are in the following list are allowed to access corresponding ports of the device.

Add Delete

No.	Host IP/MAC	Port	Operation
1	15.0.0.6	All Device Ports	

Total 1 records

Apply Refresh Default

Step 3 Select the mode: **Allowlist** and **Blocklist**.

- **Allowlist** : Only IP/MAC addresses on the allowlist can access the Device.
- **Blocklist** : The IP/MAC addresses on the blocklist cannot access the Device.

Step 4 Click **Add** to enter the IP information.

Figure 3-51 Add IP information

Add

Add Mode IP

IP Version IPv4

IP Address . . .

All Device Ports ☒

OK Cancel

Step 5 Click **OK**.

Related Operations

- Click to edit the IP information.
- Click to delete the IP address.

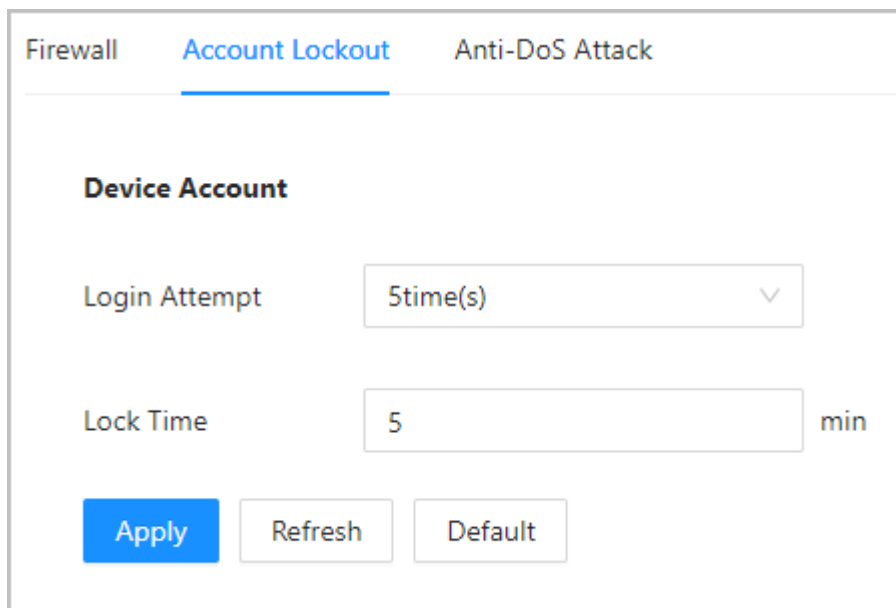
3.12.3.2 Configuring Account Lockout

If the incorrect password is entered for a defined number of times, the account will be locked.

Procedure

- Step 1 Select  > **Attack Defense** > **Account Lockout**.
- Step 2 Enter the number of login attempts and the time the administrator account and ONVIF user will be locked for.

Figure 3-52 Account lockout



- Login Attempt: The limit of login attempts. If the incorrect password is entered for a defined number of times, the account will be locked.
- Lock Time: The duration during which you cannot log in after the account is locked.

- Step 3 Click **Apply**.

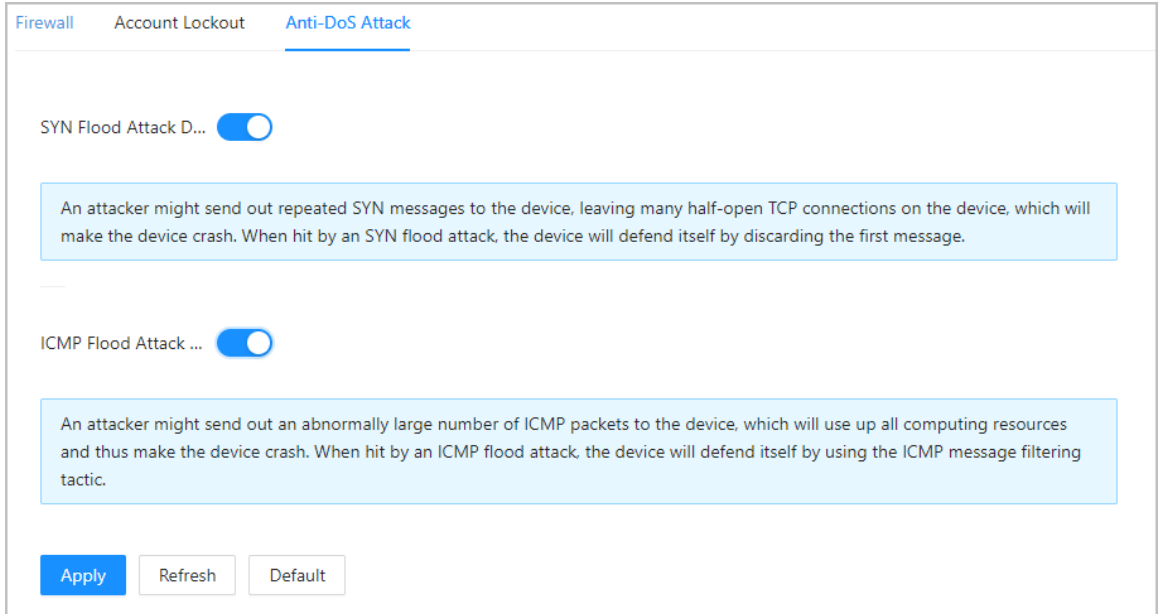
3.12.3.3 Configuring Anti-DoS Attack

You can enable **SYN Flood Attack Defense** and **ICMP Flood Attack Defense** to defend the Device against Dos attacks.

Procedure

- Step 1 Select  > **Attack Defense** > **Anti-DoS Attack**.
- Step 2 Turn on **SYN Flood Attack Defense** or **ICMP Flood Attack Defense** to protect the Device against Dos attack.

Figure 3-53 Anti-DoS attack



Firewall Account Lockout **Anti-DoS Attack**

SYN Flood Attack D... ☒

An attacker might send out repeated SYN messages to the device, leaving many half-open TCP connections on the device, which will make the device crash. When hit by an SYN flood attack, the device will defend itself by discarding the first message.

ICMP Flood Attack ... ☒

An attacker might send out an abnormally large number of ICMP packets to the device, which will use up all computing resources and thus make the device crash. When hit by an ICMP flood attack, the device will defend itself by using the ICMP message filtering tactic.

Apply Refresh Default

Step 3 Click **Apply**.

3.12.4 Installing Device Certificate

Create a certificate or upload an authenticated certificate, and then you can log in through HTTPS on your computer.

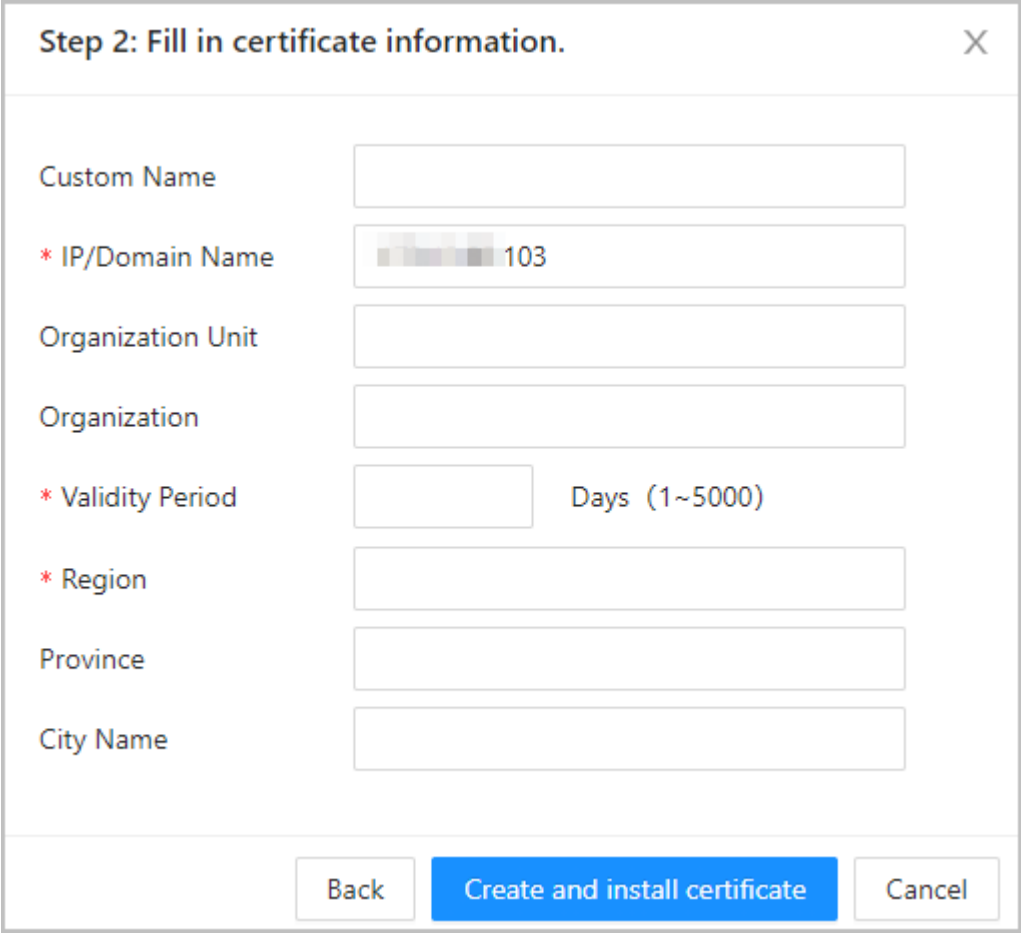
3.12.4.1 Creating Certificate

Create a certificate for the Device.

Procedure

- Step 1 Select  > **CA Certificate** > **Device Certificate**.
- Step 2 Select **Install Device Certificate**.
- Step 3 Select **Create Certificate**, and click **Next**.
- Step 4 Enter the certificate information.

Figure 3-54 Certificate information



The name of region cannot exceed 2 characters. We recommend entering the abbreviation of the name of the region.

Step 5 Click **Create and install certificate**.

The newly installed certificate is displayed on the **Device Certificate** page after the certificate is successfully installed.

Related Operations

- Click **Enter Edit Mode** on the **Device Certificate** page to edit the name of the certificate.
- Click  to download the certificate.
- Click  to delete the certificate.

3.12.4.2 Applying for and Importing CA Certificate

Import the third-party CA certificate to the Device.

Procedure

- Step 1** Select  > **CA Certificate** > **Device Certificate**.
- Step 2** Click **Install Device Certificate**.
- Step 3** Select **Apply for CA Certificate and Import (Recommended)**, and click **Next**.
- Step 4** Enter the certificate information.
 - IP/Domain name: the IP address or domain name of the Device.

- **Region:** The name of region must not exceed 3 characters. We recommend you enter the abbreviation of region name.

Figure 3-55 Certificate information (2)

Step 2: Fill in certificate information.

* IP/Domain Name: 172.16.0.03

Organization Unit:

Organization:

* Region:

Province:

City Name:

Back Create and Download Cancel

Step 5 Click **Create and Download**.

Save the request file to your computer.

Step 6 Apply to a third-party CA authority for the certificate by using the request file.

Step 7 Import the signed CA certificate.

1. Save the CA certificate to your computer.
2. Click **Installing Device Certificate**.
3. Click **Browse** to select the CA certificate.
4. Click **Import and Install**.

The newly installed certificate is displayed on the **Device Certificate** page after the certificate is successfully installed.

- Click **Recreate** to create the request file again.
- Click **Import Later** to import the certificate at another time.

Related Operations

- Click **Enter Edit Mode** on the **Device Certificate** page to edit the name of the certificate.
- Click  to download the certificate.
- Click  to delete the certificate.

3.12.4.3 Installing Existing Certificate

If you already have a certificate and private key file, import the certificate and private key file.

Procedure

Step 1 Select **Security** > **CA Certificate** > **Device Certificate**.

- Step 2 Click **Install Device Certificate**.
- Step 3 Select **Install Existing Certificate**, and click **Next**.
- Step 4 Click **Browse** to select the certificate and private key file, and enter the private key password.

Figure 3-56 Certificate and private key

Step 2: Select certificate and private key.

Custom Name

Certificate Path

Private Key

Private Key Password

- Step 5 Click **Import and Install**.

The newly installed certificate is displayed on the **Device Certificate** page after the certificate is successfully installed.

Related Operations

- Click **Enter Edit Mode** on the **Device Certificate** page to edit the name of the certificate.
- Click  to download the certificate.
- Click  to delete the certificate.

3.12.5 Installing the Trusted CA Certificate

A trusted CA certificate is a digital certificate that is used for validating the identities of websites and servers. For example, when 802.1x protocol is used, the CA certificate for switches is required to authenticate its identity.

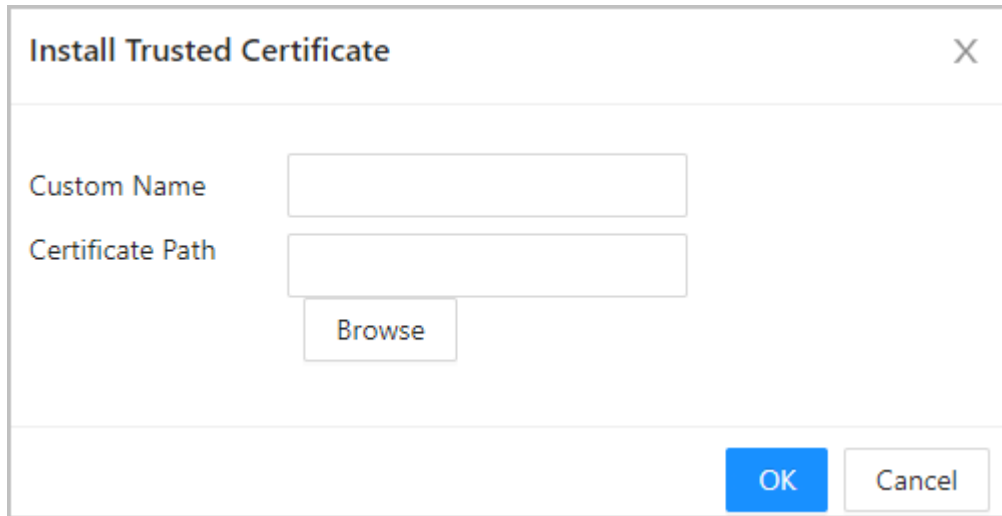
Background Information

802.1X is a network authentication protocol that opens ports for network access when an organization authenticates a user's identity and authorizes them access to the network.

Procedure

- Step 1 Select  > **CA Certificate** > **Trusted CA Certificates**.
- Step 2 Select **Install Trusted Certificate**.
- Step 3 Click **Browse** to select the trusted certificate.

Figure 3-57 Install the trusted certificate

A dialog box titled "Install Trusted Certificate" with a close button (X) in the top right corner. It contains two input fields: "Custom Name" and "Certificate Path". Below the "Certificate Path" field is a "Browse" button. At the bottom right are "OK" and "Cancel" buttons.

Install Trusted Certificate

Custom Name

Certificate Path

Browse

OK Cancel

Step 4 Click **OK**.

The newly installed certificate is displayed on the **Trusted CA Certificates** page after the certificate is successfully installed.

Related Operations

- Click **Enter Edit Mode** on the **Device Certificate** page to edit the name of the certificate.
- Click  to download the certificate.
- Click  to delete the certificate.

3.12.6 Security Warning

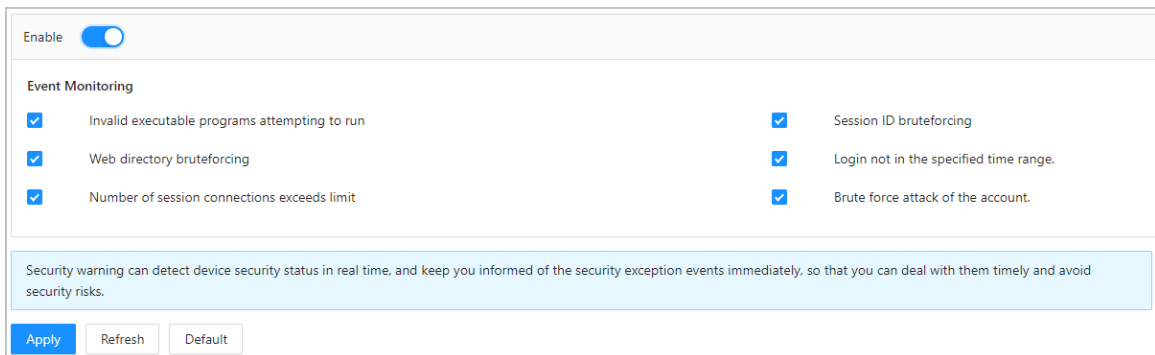
Procedure

Step 1 Select  > **Security Warning**.

Step 2 Enable the security warning function.

Step 3 Select the monitoring items.

Figure 3-58 Security warning

A configuration page for "Security Warning". At the top, there is an "Enable" toggle switch which is turned on. Below this is a section titled "Event Monitoring" containing a list of security events with checkboxes: "Invalid executable programs attempting to run", "Web directory bruteforcing", "Number of session connections exceeds limit", "Session ID bruteforcing", "Login not in the specified time range.", and "Brute force attack of the account.". All checkboxes are checked. At the bottom, there is a light blue informational box stating: "Security warning can detect device security status in real time, and keep you informed of the security exception events immediately, so that you can deal with them timely and avoid security risks." Below this box are three buttons: "Apply", "Refresh", and "Default".

Enable ☒

Event Monitoring

☒ Invalid executable programs attempting to run	☒ Session ID bruteforcing
☒ Web directory bruteforcing	☒ Login not in the specified time range.
☒ Number of session connections exceeds limit	☒ Brute force attack of the account.

Security warning can detect device security status in real time, and keep you informed of the security exception events immediately, so that you can deal with them timely and avoid security risks.

Apply Refresh Default

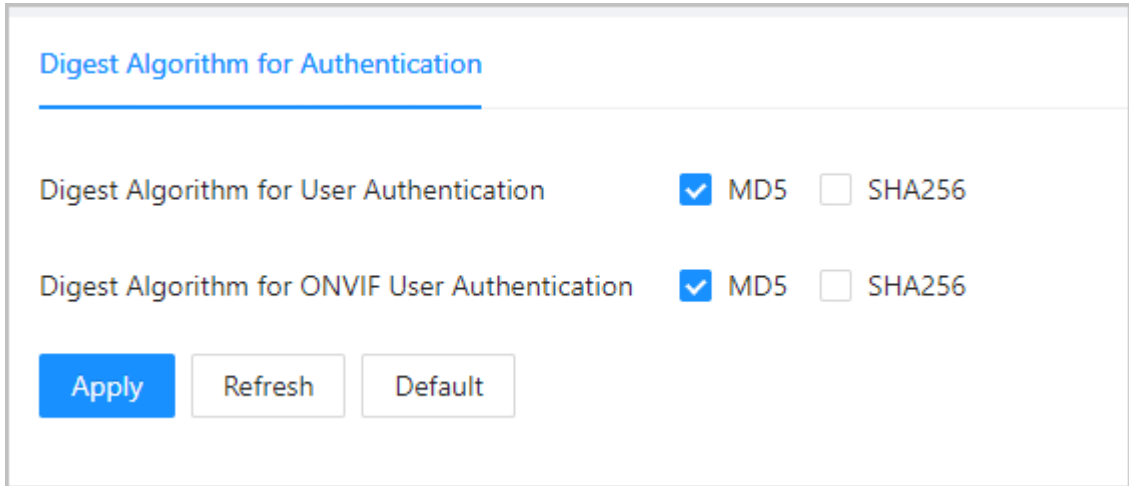
Step 4 Click **Apply**.

3.12.7 Security Authentication

Procedure

- Step 1 Select **Security** > **Security Authentication**.
- Step 2 Select a message digest algorithm.
- Step 3 Click **Apply**.

Figure 3-59 Security authentication



Digest Algorithm for Authentication

Digest Algorithm for User Authentication ☒ MD5 ☐ SHA256

Digest Algorithm for ONVIF User Authentication ☒ MD5 ☐ SHA256

Apply Refresh Default

4 Phone Operations

Before logging in to the webpage of the Device on your phone, make sure that you have initialized the Device through the webpage on the computer.

We recommend you use your phone in portrait mode and day mode. You can log in to the webpage of the Device on your phone through the following methods.

- Connect the Device to the network through the network cable. Make sure the phone and the Device are in the same network. Open the browser on the phone, and then enter the IP address of the Device.
- Connect the Device and the phone to the network through the same Wi-Fi. Open the browser on the phone, and then enter the IP address according to the connected Wi-Fi.
- Connect the phone to the network through the Device Wi-Fi. Open the browser on the phone, and then enter the IP address according to the Wi-Fi AP on the Device (it is 192.168.3.1 by default).



The Device Wi-Fi name is displayed in the **Device serial number + Device model** mode.



- The Wi-Fi and Wi-Fi AP are available on select models.
- Only English is supported when you log in to the webpage on the phone.

4.1 Logging in to the Webpage

Prerequisites

Make sure that the phone used to log in to the webpage is on the same LAN as the Device.

Procedure

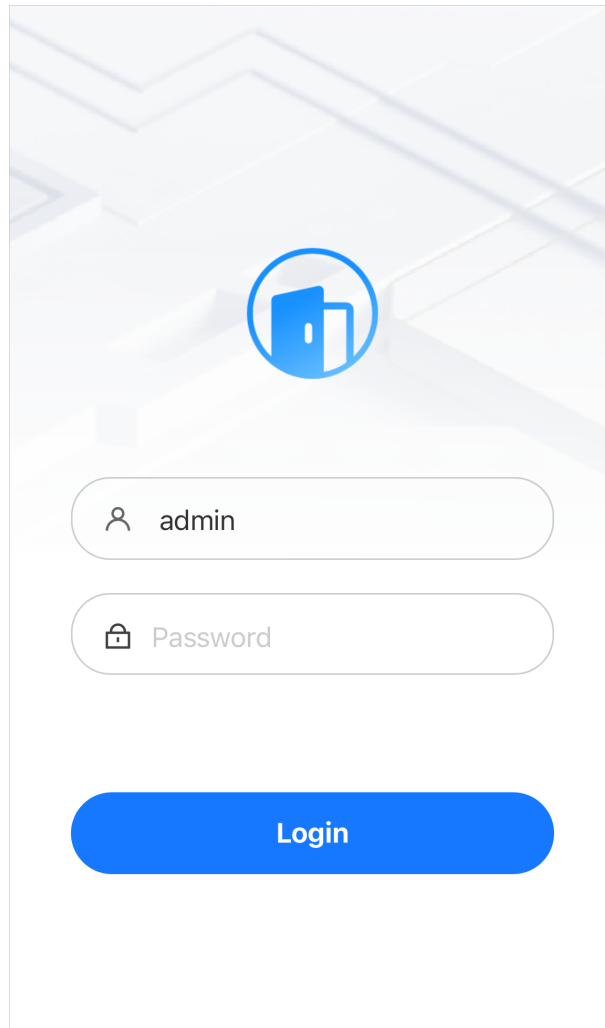
Step 1 Open a browser, and then enter to the IP address of the Device.

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 reset the password through the webpage on the computer. For details, see "3.2 Resetting the Password".

Figure 4-1 Login page

The login page features a light gray background with a subtle geometric pattern of overlapping planes. At the top center is a blue circular icon containing a white door symbol. Below this icon are two input fields: the first is labeled 'admin' with a user icon, and the second is labeled 'Password' with a lock icon. At the bottom center is a prominent blue rounded rectangle button with the word 'Login' in white text.

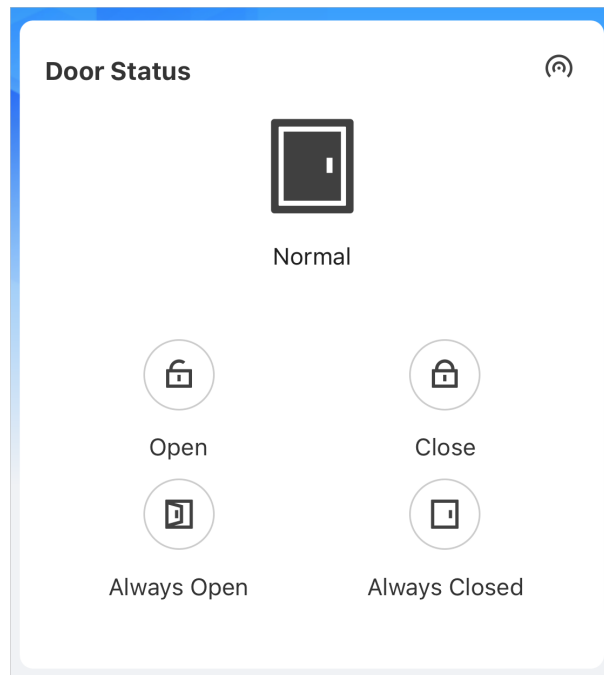
Step 3 Click **Login**.

4.2 Home Page

The home page is displayed after you successfully log in.

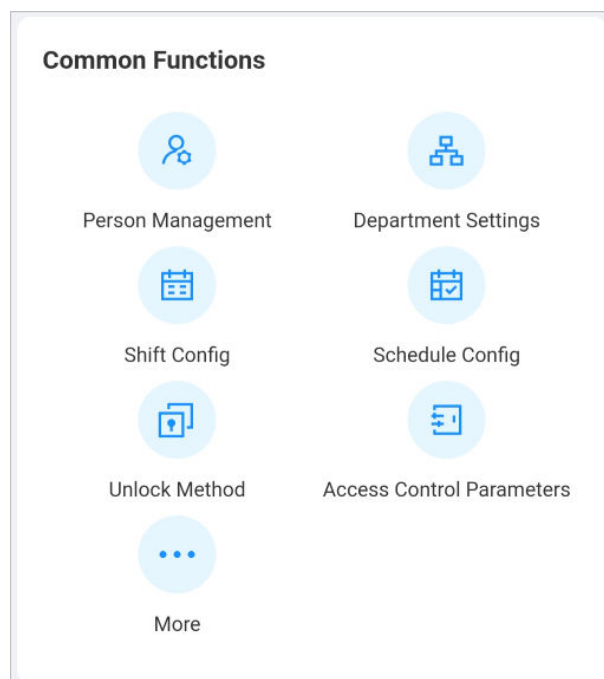
- The **Door Status** area displays the status of the door. You can remotely open or close the door. You can also configure the door status as **Always Open** or **Always Closed**.

Figure 4-2 Door status



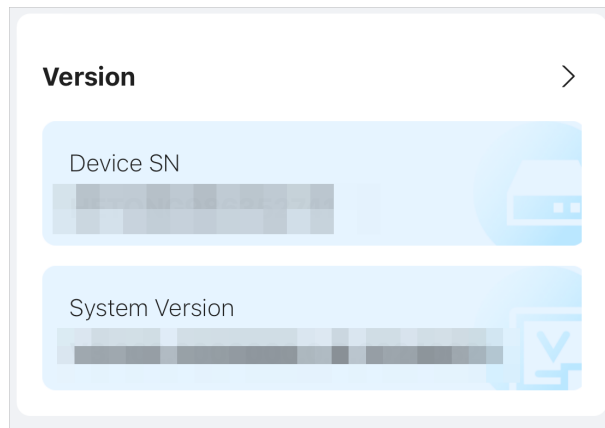
- The **Common Function** area displays the configuration menu of the Device. Click **More** to view all the configuration menus.

Figure 4-3 Common functions



- View the serial number and the version information on the **Version** area. Click > to view the version details.

Figure 4-4 Version



4.3 Person Management

Add the person and configure the permissions.

Procedure

- Step 1 Log in to the webpage.
- Step 2 Click **Person Management**, and then click +.
- Step 3 Configure user information.

Figure 4-5 Add the person (1)

A screenshot of a web form titled "Basic Info". It contains several input fields and a section for verification modes. The fields are: "User ID" (marked with a red asterisk), "Name", and a "Verification Mode" section. The "Verification Mode" section contains four rows: "Face" with a value of "0" and a right-pointing chevron, "Password" with a value of "Not Added" and a right-pointing chevron, "Card" with a value of "0" and a right-pointing chevron, and "Fingerprint" with a value of "0" and a right-pointing chevron.

Figure 4-6 Add the person (2)

Permission	User >
Validity Period	>
2037-12-31 23:59:59	
General Plan	255-Default >
Holiday Plan	255-Default >
User Type	General User >
Times Used	Unlimited
Department	1-Default >
Schedule Mode	Department Schedule >

Table 4-1 Parameters description

Parameter	Description
User ID	The User ID is like employee ID, which can be numbers, letters, and their combinations, and the maximum length of the number is 30 characters.
Name	The name can have up to 32 characters (including numbers, symbols, and letters).
Password	Configure the user password. The maximum length of the password is 8 digits. The duress password is the unlock password + 1. For example, if the user password is 12345, the duress password will be 12346. A duress alarm will be triggered when a duress password is used to unlock the door.

Parameter	Description
Card	- Enter the card number manually. - Click Add. - Enter the card number, and then click Add. - Read the number automatically through the Device. - Click Add. - Swipe cards on the card reader. A 60-second countdown is displayed to remind you to swipe cards, and the system will read the card number automatically. If the 60-second countdown expires, click Read Card again to start a new countdown. - Click OK. A user can register up to 5 cards at most. Enter your card number or swipe your card, and then the card information will be read by the Device. You can enable the Duress Card function. An alarm will be triggered if a duress card is used to unlock the door. Duress Card : Click to set duress card. Change Card No. : Click to change the card number.  One user can only set one duress card.
Fingerprint	Register fingerprints. A user can register up to 3 fingerprints, and you can set a fingerprint to the duress fingerprint. An alarm will be triggered when the duress fingerprint is used to unlock the door. Enroll fingerprints through an enrollment reader or the Device. - Click Add. - Press finger on the scanner according to the on-screen instructions. - Click OK.  - Fingerprint function is only available on select models. - We do not recommend you set the first fingerprint as the duress fingerprint. - One user can only sets one duress fingerprint.
Permission	User : Users only have door access or time attendance permissions. Admin : Administrators can configure the Device besides door access and attendance permissions.
Validity Period	Set a date on which the door access and attendance permissions of the person will be expired.

Parameter	Description
General Plan	People can unlock the door or take attendance during the defined period.  You can select more than one plan.
Holiday Plan	People can unlock the door or take attendance during the defined holiday.  You can select more than one holiday.
User Type	● General User : General users can unlock the door. ● Blocklist User : When users in the blocklist unlock the door, service personnel will receive a notification. ● Guest User : Guests can unlock the door within a defined period or for certain amount of times. After the defined period expires or the unlocking times runs out, they cannot unlock the door. ● Patrol User : Patrol users can take attendance on the Device, but they do not have door permissions. ● VIP User : When VIP unlock the door, service personnel will receive a notice. ● Other User : When they unlock the door, the door will stay unlocked for 5 more seconds. ● Custom User 1/Custom User 2: Same with general users.
Time Used	Set an unlock limit for guest users. After the unlock times run out, they cannot unlock the door.
Department	Add users to a department. If a department schedule is assigned to the person, they will follow the established department schedule. ● Department Schedule: Assign department schedule to the user. ● Personal Schedule: Assign personal schedule to the user.  ◇ This function is only available on select models. ◇ If you set the schedule mode to department schedule here, the personal schedule you have configured for the user in Attendance > Schedule Config > Personal Schedule is invalid.
Schedule Mode	

Step 4 Click **Add**.

4.4 Configuring the System

4.4.1 Viewing Version Information

On the webpage, select **More** > **System** > **Version**, and you can view version information on the Device.

4.4.2 Maintenance

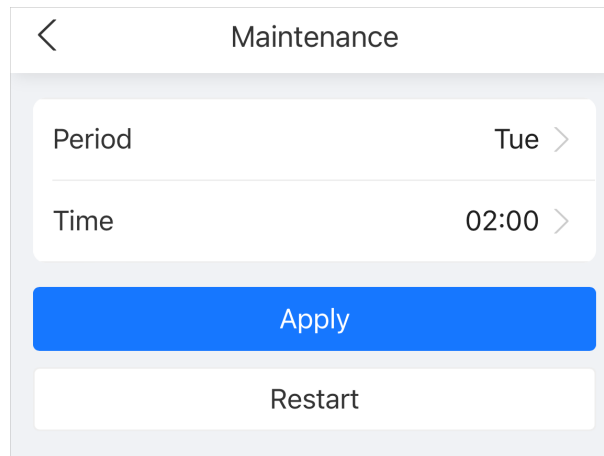
Regularly restart the Device during its idle time to improve its performance.

Procedure

- Step 1 Log in to the webpage.
- Step 2 Select **More** > **System** > **Maintenance**.
- Step 3 Set the time, and then click **Apply**.

The Device will restart at the scheduled time, or you can click **Restart** to restart it immediately.

Figure 4-7 Maintenance



Maintenance	
Period	Tue >
Time	02:00 >
Apply	
Restart	

4.4.3 Configuring Time

Procedure

- Step 1 Log in to the webpage.
- Step 2 Select **More** > **System** > **Time**.
- Step 3 Configure the time.

Figure 4-8 Configure the time parameters

<

Time

Time

Manually Set >

System Time

2024-06-25 11:13:03 >

Sync Time

Sync Phone

Date Format

YYYY-MM-DD >

Time Format

24-Hour >

Time Zone

(UTC+08:00) Beijing, >

DST

☐

Type

Date >

Start Time

01-01 00:00 >

End Time

01-02 00:00 >

Table 4-2 Time settings description

Parameter	Description
Time	- Manual Set: Manually enter the time or you can click Sync Phone to sync time with the phone. - NTP: The Device will automatically sync the time with the NTP server. Server : Enter the domain of the NTP server. Port : Enter the port of the NTP server. Interval : Enter its time with the synchronization interval.
Date Format	Select the date format and the time format.
Time Format	
Time Zone	Select the time zone.
DST	(Optional) Enable DST. - Select Date or Week as the Type. - Configure the start time and end time of the DST.

Step 4 Click **Apply**.

4.4.4 Data Capacity

You can see how many users, cards, face images, fingerprints, logs, unlock records, and other information that the Device can store.

Log in to the webpage and select **More > System > Data Capacity**.

4.4.5 Configuring Ringtone

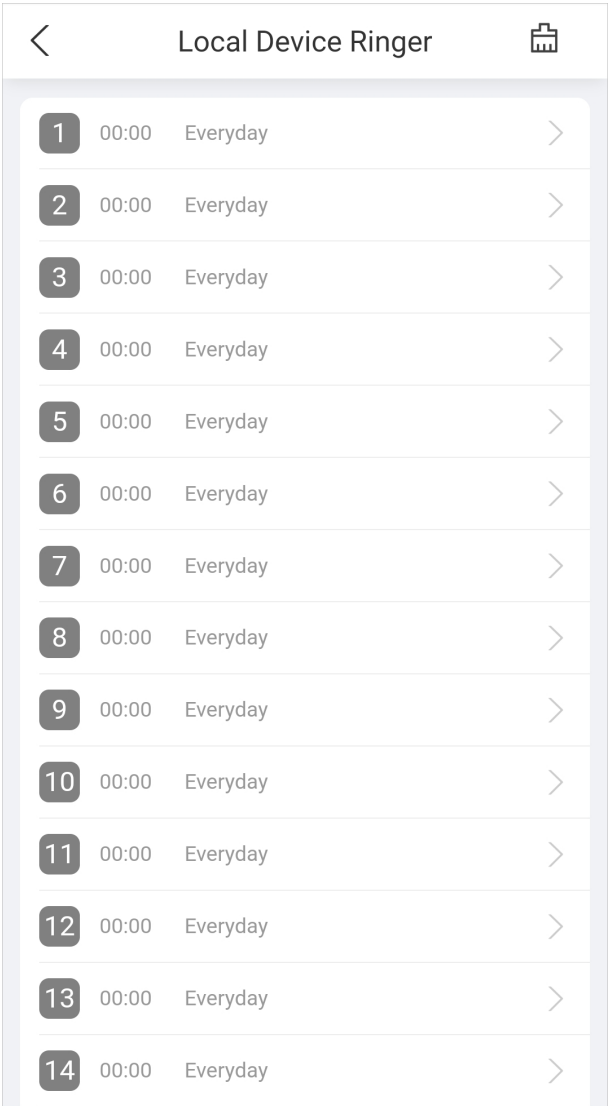
Configure the time when the bell rings as a reminder.

Procedure

Step 1 Log in to the webpage.

Step 2 Select **More > System > Local Device Ringer**.

Figure 4-9 Ringtone configuration



Step 3 Tap the target ringtone to configure the item when the bell rings, and then tap **Save**.

Figure 4-10 Configure the ringtone

The screenshot shows a mobile application interface titled "Ringtone Config". At the top left is a back arrow. Below the title, there are three input fields: "Time" with the value "00:00", "* Ringtone Duration (sec)" with the value "0", and "Repeat Time" with the value "Everyday". Each field has a right-pointing chevron. At the bottom is a large blue button labeled "Save".

Table 4-3 Parameters description

Parameter	Description
Time	The time when the bell rings.
Ringtone Duration (sec)	The ring duration.
Repeat Time	The bell rings according to the configured repeat time. For example, if you set repeat time to Monday, the bell rings every Monday.

4.4.6 Language

Log in to the webpage, select **More > System > Language**. Change the language, and then click **Apply**.

4.5 Configuring Attendance

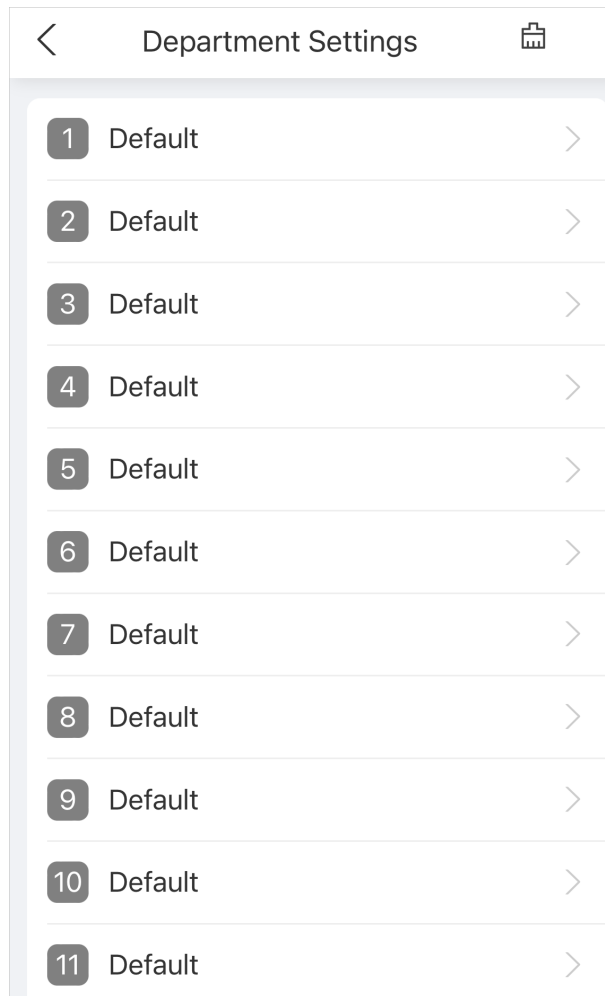
This function is only available on select models.

4.5.1 Configuring Departments

Procedure

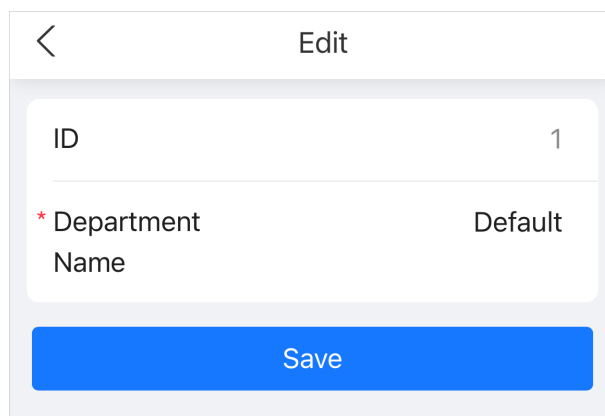
- Step 1 Log in to the webpage.
- Step 2 Select **More > Attendance Config > Department Settings**.

Figure 4-11 Department settings



Step 3 Click the department to rename the department, and then click **Save**.
There are 20 default departments. We recommend you rename them.

Figure 4-12 Rename the department



Related Operations

You can click  to restore departments to default settings.

4.5.2 Configuring Shifts

Configure shifts to define time attendance rules. Employees need to work at the time scheduled for their shift to start, and leave at the end time, except when they choose to work overtime.

Procedure

- Step 1 Log in to the webpage.
- Step 2 Select **More > Attendance Config > Shift Config > Shift.**

Figure 4-13 Shift list

Shift Config			
Shift		Holiday	
1	Default 08:00-17:00	00:00-00:00	>
2	Default 08:00-17:00	00:00-00:00	>
3	3 08:00-17:00	00:00-00:00	>
4	4 08:00-17:00	00:00-00:00	>
5	5 08:00-17:00	00:00-00:00	>
6	6 08:00-17:00	00:00-00:00	>
7	7 08:00-17:00	00:00-00:00	>
8	8 08:00-17:00	00:00-00:00	>

- Step 3 Click the shift to configure the shift parameters, and then click **Save**.

Figure 4-14 Configure the shift

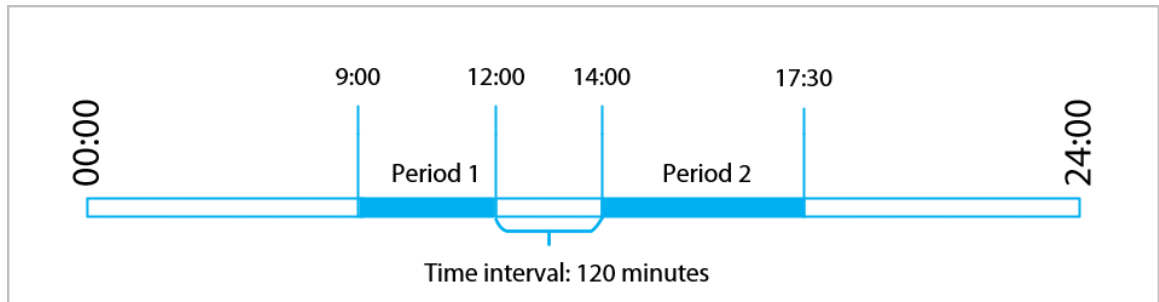
The screenshot shows a mobile application interface titled "Edit Shift". It contains several input fields and a "Save" button. The fields are: "Shift No." with the value "1", "* Shift Name" with the value "Default", "Period 1" with the value "08:00~17:00", "Period 2" with the value "00:00~00:00", "Overtime Period" with the value "00:00~00:00", "* Limit for Arriving Late" with the value "9 min", and "* Limit for Leaving Early" with the value "5 min". A blue "Save" button is located at the bottom of the form.

Table 4-4 Shift parameters description

Parameter	Description
Shift Name	Enter the name of the shift.
Period 1	Specify a time range when people can clock in and clock out for the workday.
Period 2	If you only set one attendance period, employees need to clock in and out by the designated times to avoid an anomaly appearing on their attendance record. For example, if you set 08:00 to 17:00, employees must clock in by 08:00 and clock out from 17:00 onwards. If you set 2 attendance periods, the 2 periods cannot overlap. Employees need to clock in and clock out for both periods.
Overtime Period	Employees who clock in or out during the defined period will be considered as working beyond their normal work hours.
Limit for Arriving Late	A certain amount of time can be granted to employees to allow them to clock in a bit late and clock out a bit early. For example, if the regular time to clock in is 08:00, the tolerance period can be set as 5 minutes for employees who arrive by 08:05 to not be considered as late.
Limit for Leaving Early	

- When the time interval between 2 periods is an even number, you can divide the time interval by 2, and assign the first half of the interval to the first period, which will be the clock out time. The second half of the interval should be assigned to the second period as the clock in time.

Figure 4-15 Time interval (even number)



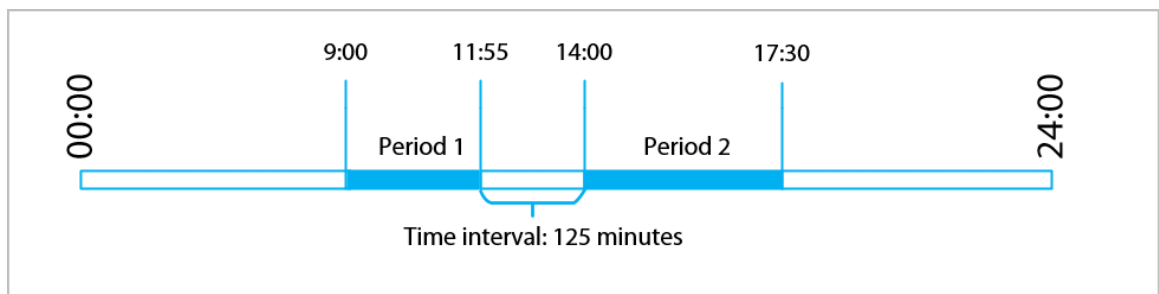
For example: If the interval is 120 minutes, then the clock-out time for period 1 is from 12:00 to 12:59, and the clock-in time for period 2 is from 13:00 to 14:00.



If a person clocks out multiple times during period 1, the latest time will be valid, and if they clock in multiple times during period 2, the earliest time will be valid.

- When the time interval between 2 periods is an odd number, the smallest portion of the interval will be assigned to the first period, which will be the clock out time. The largest portion of the interval will be assigned to the second period as the clock in time.

Figure 4-16 Time interval (even number)



For example: If the interval is 125 minutes, then the clock-out time for period 1 is from 11:55 to 12:57, and the clock-in time for period 2 is from 12:58 to 14:00. Period 1 has 62 minutes, and period 2 has 63 minutes.



If a person clocks out multiple times during period 1, the latest time will be valid, and if they clock in multiple times during period 2, the earliest time will be valid.



All attendance times are precise down to the second. For example, if the normal clock-in time is set to 8:05 AM, the employee who clocks in at 8:05:59 AM will not be considered as arriving late. But, the employee that arrives at 8:06 AM will be marked as late by 1 minute.

Related Operations

You can click  to restore shifts to factory defaults.

4.5.3 Configuring Holiday

Configure holiday plans to set periods for attendance to not be tracked.

Procedure

- Step 1 Log in to the webpage.
- Step 2 Select **More > Attendance Config > Shift Config > Holiday**.
- Step 3 Click **+** to add holiday plans.
- Step 4 Configure the parameters, and then click **Save**.

Figure 4-17 Add the holiday

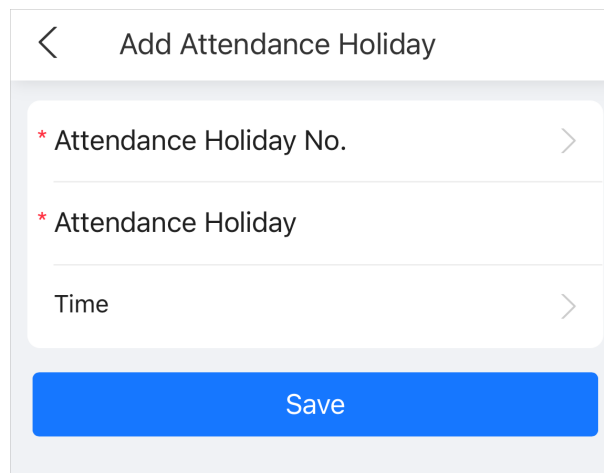


Table 4-5 Parameters description

Parameter	Description
Attendance Holiday No.	The number of the holiday.
Attendance Holiday	The name of the holiday.
Time	The start and end time of the holiday.

- Step 5 Click **OK**.

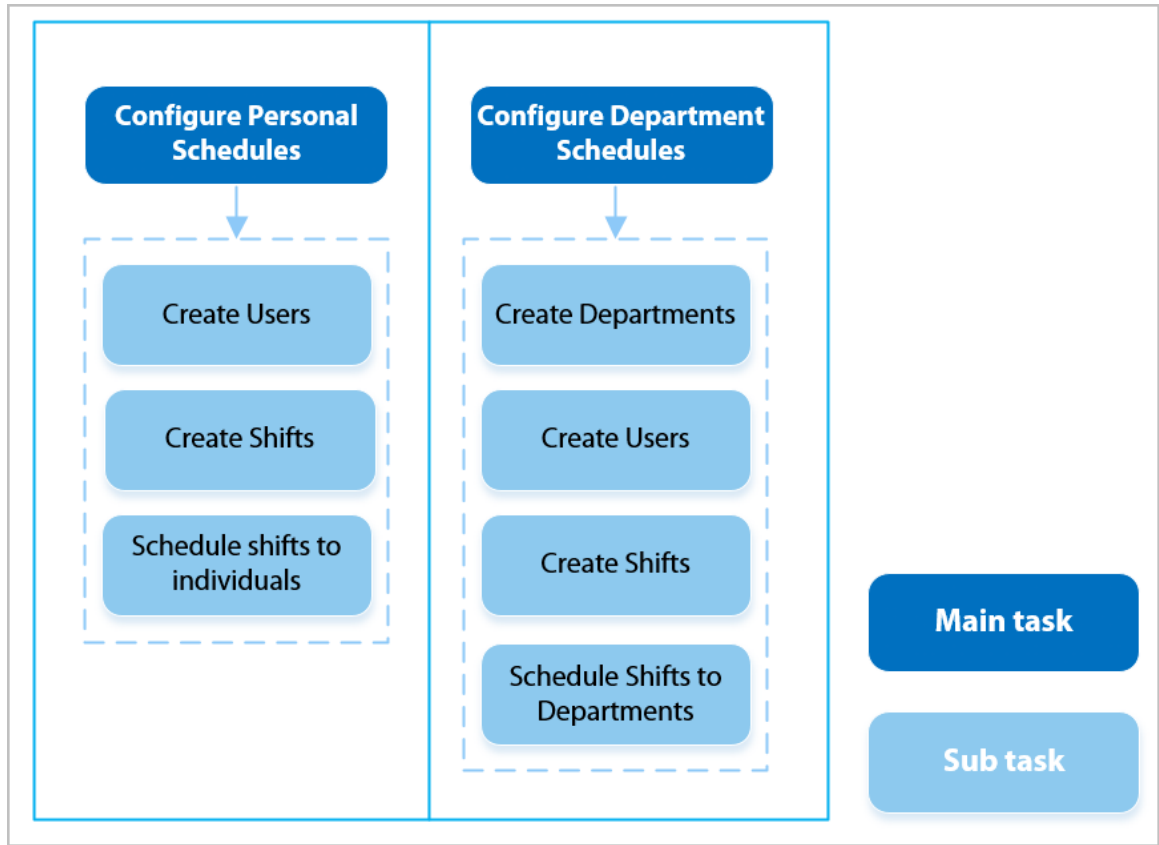
4.5.4 Configuring Work Schedules

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.

Background Information

Refer to the flowchart to configure personal schedules or department schedules.

Figure 4-18 Configuring work schedules



Procedure

- Step 1** Log in to the webpage.
- Step 2** Select **More > Attendance Config > Schedule Config**.
- Step 3** Set work schedules for individuals.

1. Click **Personal Schedule**.
2. Select a person in the person list.



After you configure the **Schedule Mode** as the **Personal Schedule** when you add the person, the person is displayed in the person list.

3. On the calendar, select a day, and then select a shift.



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 per-defined shifts.
- 25 indicates business trip.
- 26 indicates leave of absence.

- Step 4** Set works schedules for departments.

1. Click **Department Schedule**.
2. Select a department in the department list.
3. On the calendar, select a day, and then select a shift.

Figure 4-19 Department schedule

Sun	Mon	Tue	Wed	Thu	Fri	Sat
0	1	1	1	1	1	0

Shift	Time Range	Status
0-Rest		
1-Default	08:00:00-17:00:00 00:00:00-00:00:00	✓
2-Default	08:00:00-17:00:00 00:00:00-00:00:00	
3-3	08:00:00-17:00:00 00:00:00-00:00:00	
4-4	08:00:00-17:00:00 00:00:00-00:00:00	

- 0 indicates rest.
- 1 to 24 indicates the number of the per-defined shifts.
- 25 indicates business trip.
- 26 indicates leave of absence.



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

4.5.5 Configuring Attendance Mode

Procedure

- Step 1 Log in to the webpage.
- Step 2 Select **More** > **Attendance Config** > **Attendance Config**.
- Step 3 Enable **Local Attendance**, set the attendance mode, and then enter the verification interval..

When **Use Attendance for Unlock** is enabled, if people verify the identity for the attendance, they can unlock the door at the same time.

When an employee clocks in and out multiple times within a set interval, the earliest time will be valid.

Table 4-6 Attendance mode

Parameter	Description	Attendance Mode
Auto/Manual Mode	Select the mode, select the period, and then configure the start time and the end time of each period. The screen displays the attendance status automatically after you clock in or out, but you can also manually change your attendance status using the buttons of F1 to F4.	● Check in: Clock in when your normal workday starts. ● Break out: Clock out when your break starts. ● Break in: Clock in when your break ends. ● Check out: Clock out when your normal workday starts. ● Overtime check in: Clock in when your overtime period starts. ● Overtime check out: Clock out when your overtime period ends.
Auto Mode	Select the mode, select the period, and then configure the start time and the end time of each period. The screen displays the attendance status automatically according to your configurations. You cannot use the buttons to change the status.	
Manual Mode	● After you clock in or out, manually select the attendance status. ● Press F1 to F4 to change the attendance mode, and then verify the identity.  The status is not displayed on the screen. After you press F1 to F4 to select the status first, the status will be displayed for 10 seconds.	
Fixed Mode	When you clock in or out, the screen will display the per-defined attendance status all the time.	

Step 4 Click **Apply**.

4.6 Configuring Access Control

4.6.1 Configuring Unlock Methods

You can use multiple unlock methods to unlock the door, such as fingerprint, card, and password. You can also combine them to create your own personal unlock method.

Procedure

Step 1 Log in to the webpage.

Step 2 Click **Unlock Method** on the main menu, or select **More > Access Control > Unlock Method**.

Step 3 (Optional) Configure the combination method and the unlock method, and then click **Apply**.

- Combination method
 - ◇ Or: Use one of the selected unlock methods to open the door.
 - ◇ And: Use all the selected unlock methods to open the door.
- Unlock method

Select the unlock method according to the supported capabilities of the Device.

Figure 4-20 Unlock method

< Unlock Method

Unlock Method Combination Unlock

Combination Method Or >

Unlock Method Card, Fingerprint, Password >

Apply

4.6.2 Configuring Access Control Parameters

Procedure

- Step 1 Log in to the webpage.
- Step 2 Click **Access Control Parameters** on the main menu, or select **More** > **Access Control** > **Access Control Parameters**.
- Step 3 Configure basic parameters for the access control, and then tap **Apply**.

Figure 4-21 Access control parameters (1)

Name	Door1
Door Status	Normal >
Verification Interval	0 s
Card Swiping Interval	0 s (0-86400)
Public Password	☐
Normally Open Period	
General Plan	Disabled >
Holiday Plan	Disabled >
Normally Closed Period	
General Plan	Disabled >
Holiday Plan	Disabled >

Figure 4-22 Access control parameters (2)

Unlock Settings	
Unlock Method	Combination Unlock
Combination Method	Or >
Unlock Method	Card, Fingerprint, Password >
Door Unlocked Duration	3 s
<button>Apply</button>	

Table 4-7 Description of access control parameters

Parameter		Description
Basic Settings	Name	The name of the door.
	Door Status	Set the door status. • Normal: The door will be unlocked and locked according to your settings. • Always Open: The door remains unlocked all the time. • Always Closed: The door remains locked all the time.
	Verification Interval	If you verify your identity multiple times within a set period, only the earliest verification will be considered valid, and the door will not open after the second or later verifications. From the moment the door fails to open, you must wait for the configured verification time interval before attempting to verify your identity again.
	Card Swiping Interval	For first-time verification through card, you can normally unlock the door or perform attendance, and the records are generated. Within the configured period, if you swipe the card for verification again, you cannot unlock the door or perform attendance, and the records are not generated. Please verify the identification after the configured period.  The Card Swiping Interval takes priority over Verification Interval.
	Public Password	After the public password is enabled, configure the password. You can use the public password without entering the user ID to unlock the door. Only one public password is supported for one device.
Normally Open Period	Period/Holiday Plan	When you select Normal , you can select a time template from the drop-down list. The door remains open or closed during the defined time.
Normally Closed Period	Period/Holiday Plan	 • When normally open period conflicts with normally closed period, normally open period takes priority over normally closed period. • When period conflict with holiday plan, holiday plans takes priority over periods.
Unlock Settings	Unlock Method	Combination Unlock by default.

Parameter		Description
	Combination Method	• Or: Use one of the selected unlock methods to open the door. • And: Use all the selected unlock methods to open the door.
	Unlock Method	Select the unlock method according to the supported capabilities of the Device.
	Door Unlocked Duration	Configure the time in which the door keeps the open status. It is 3 seconds by default. When the door opens for more than the configured time, the door closes.

Step 4 Tap **Apply**.

4.6.3 Configuring Alarms

An alarm will be triggered when an abnormal access event occurs.

Procedure

- Step 1 Log in to the webpage.
Step 2 Select **More** > **Access Control** > **Alarm**.
Step 3 Configure alarm parameters, and then tap **Apply**.

Figure 4-23 Alarm settings

The screenshot displays the 'Alarm' configuration page. It features a list of settings, each with a label and a control element (toggle switch or dropdown). The 'Duress Alarm', 'Door Detector', and 'Excessive Attempts Alarm' are currently enabled (toggles are blue). 'Anti-passback', 'Intrusion Alarm', and 'Unlock Timeout Alarm' are disabled (toggles are grey). 'Door Detector Status' is set to 'NO' with a chevron indicating a dropdown menu. 'Unlock Timeout' is set to '60 s'. A blue 'Apply' button is located at the bottom of the settings list.

Table 4-8 Description of alarm parameters

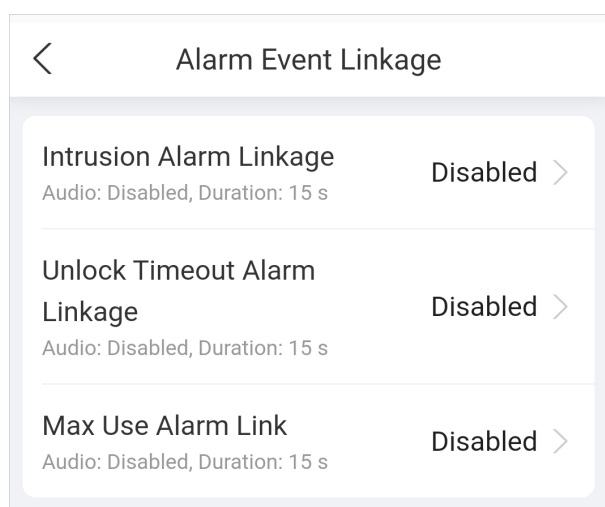
Parameter	Description
Duress Alarm	An alarm will be triggered when a duress card, duress password or duress fingerprint is used to unlock the door.
Door Detector	With the door detector wired to your device, alarm can be triggered when doors are opened or closed abnormally. The door detector includes 2 types, including NC detector and NO detector. ● NC: The sensor is in a shorted position when the door or window is closed. ● NO: An open circuit is created when the window or door is actually closed.
Intrusion Alarm	If the door is opened abnormally, an intrusion alarm will be triggered and last for a defined time.  The door detector and intrusion need to be enabled at the same time.
Unlock Timeout Alarm	When the door remains unlocked for longer than the defined timeout duration, the door timeout alarm will be triggered and last for the defined time.
Unlock Timeout	 The door detector and door timed out function need to be enabled at the same time.
Excessive Attempts Alarm	If the wrong password or card is used 5 times in a row within 60 seconds, the alarm for excessive use of illegal card will be triggered and lasts for a defined time.

4.6.4 Configuring Alarm Event Linkage

Procedure

- Step 1 Log in to the webpage.
- Step 2 Select **More** > **Access Control** > **Alarm Event Linkage**.

Figure 4-24 Alarm event linkage



Step 3 Click the linkage to configure the alarm linkage, and then click **OK**.

Table 4-9 Alarm event linkage

Parameter	Description
Intrusion Alarm Linkage	If the door is opened abnormally, an intrusion alarm will be triggered. Buzzer: The buzzer sounds when an intrusion alarm is triggered. You can configure the alarm duration.
Unlock Timeout Alarm Linkage	When the door remains unlocked for longer than the defined timeout duration, the door timeout alarm will be triggered and last for the defined time. Buzzer: The buzzer sounds when the unlock timeout alarm is triggered. You can configure the alarm duration.
Max Use Alarm Link	If the wrong password or card is used 5 times in a row within 60 seconds, the alarm for excessive use of illegal card will be triggered and lasts for a defined time. Buzzer: The buzzer sounds when the excessive use alarm is triggered. You can configure the alarm duration.

4.6.5 Configuring Card Settings

Background Information

Procedure

- Step 1** Log in to the webpage.
- Step 2** Select **More** > **Access Control** > **Card Settings**.
- Step 3** Configure the card parameters, and then tap **Apply**.

Table 4-10 Card parameters description

Parameter		Description
Card No. System	Card No. System	Select decimal format or hexadecimal format for the card number when Wiegand card reader is connected. The card No. system is the same for both card number input and output.

Step 4 Click **Apply**.

4.6.6 Configuring Screen Settings

Configure the screen always-on period and the device information that is displayed on the screen when the theme is configured to **General Mode**.

Procedure

Step 1 Log in to the webpage.

Step 2 Select **More** > **Access Control** > **Screen Settings**.

Step 3 Configure the always-on screen.

Always-On Config : The screen is always turned on during the configured time period.

1. Tap **Always-On Config**.
2. Enable the function, and then tap **OK**.
3. Tap the period, configure the start time and the end time, and then tap **OK**.
4. Tap **Apply**.



To help extend the lifespan of your screen, we recommend you limit the time it stays on to no more than 8 hours a day.

Figure 4-25 Display always on

Always-On Config

Display Always On ☒

To help extend the lifespan of your screen, we recommend you limit the time it stays on to no more than 8 hours a day.

Period1
08:00~18:00 >

Period2
00:00~00:00 >

Period3
00:00~00:00 >

Period4
00:00~00:00 >

Apply

4.7 Communication Settings

4.7.1 Configuring TCP/IP

You need to configure IP address of Device to make sure that it can communicate with other devices.

Procedure

- Step 1 Log in to the webpage.
- Step 2 Select **More** > **Communication Settings** > **Network Setting** > **TCP/IP**.
- Step 3 Configure the parameters, and then click **Apply**.

Figure 4-26 TCP/IP

The screenshot displays a 'TCP/IP' configuration window. At the top, there is a back arrow and the title 'TCP/IP'. Below this, the configuration is organized into sections. The first section shows 'NIC' set to 'NIC 1' with a chevron. The second section shows 'Mode' set to 'Static' with a chevron. The third section shows 'MAC Address' with a hexagonal input field. The fourth section shows 'IP Version' set to 'IPv4' with a chevron. Below this are five fields, each preceded by a red asterisk: '* IP Address', '* Subnet Mask', '* Default Gateway', '* Preferred DNS', and '* Alternate DNS'. Each field has a corresponding hexagonal input field. At the bottom of the configuration area, there is an 'MTU' field set to '1500'. A large blue 'Apply' button is located at the very bottom of the window.

Table 4-11 Description of TCP/IP

Parameter	Description
Mode	• Static: Manually enter IP address, subnet mask, and gateway. • DHCP: It stands for Dynamic Host Configuration Protocol. When DHCP is turned on, the Device will automatically be assigned with IP address, subnet mask, and gateway.
MAC Address	MAC address of the Device.
IP Version	IPv4 or IPv6.
IP Address	If you set the mode to Static , configure the IP address, subnet mask and gateway.
Subnet Mask	
Default Gateway	
	 • IPv6 address is represented in hexadecimal. • IPv6 version do not require setting subnet masks. • The IP address and default gateway must be in the same network segment.

Parameter	Description
Preferred DNS	Set IP address of the preferred DNS server.
Alternate DNS	Set IP address of the alternate DNS server.
MTU	MTU (Maximum Transmission Unit) refers to the maximum size of data that can be transmitted in a single network packet in computer networks. A larger MTU value can improve network transmission efficiency by reducing the number of packets and associated network overhead. If a device along the network path is unable to handle packets of a specific size, it can result in packet fragmentation or transmission errors. In Ethernet networks, the common MTU value is 1500 bytes. However, in certain cases such as using PPPoE or VPN, smaller MTU values may be required to accommodate the requirements of specific network protocols or services. The following are recommended MTU values for reference: • 1500: Maximum value for Ethernet packets, also the default value. This is a typical setting for network connections without PPPoE and VPN, some routers, network adapters, and switches. • 1492: Optimal value for PPPoE • 1468: Optimal value for DHCP. • 1450: Optimal value for VPN.

4.7.2 Configuring Wi-Fi

Procedure

- Step 1 Log in to the webpage.
- Step 2 Select **More** > **Communication Settings** > **Wi-Fi**.
- Step 3 Turn on Wi-Fi.

All available Wi-Fi are displayed.



- The Wi-Fi function is available on select models.
- The Wi-Fi and Wi-Fi AP cannot be enabled at the same time.

- Step 4 Click the Wi-Fi, and then enter the password.

The Wi-Fi is connected.

Related Operations

- DHCP: Select the **DHCP** mode and click **Apply**, the Device will automatically be assigned a Wi-Fi address.
- Static: Select the **Static** mode, manually enter a Wi-Fi address, and then click **Apply**, the Device will connect to the Wi-Fi.

4.7.3 Configuring Wi-Fi AP

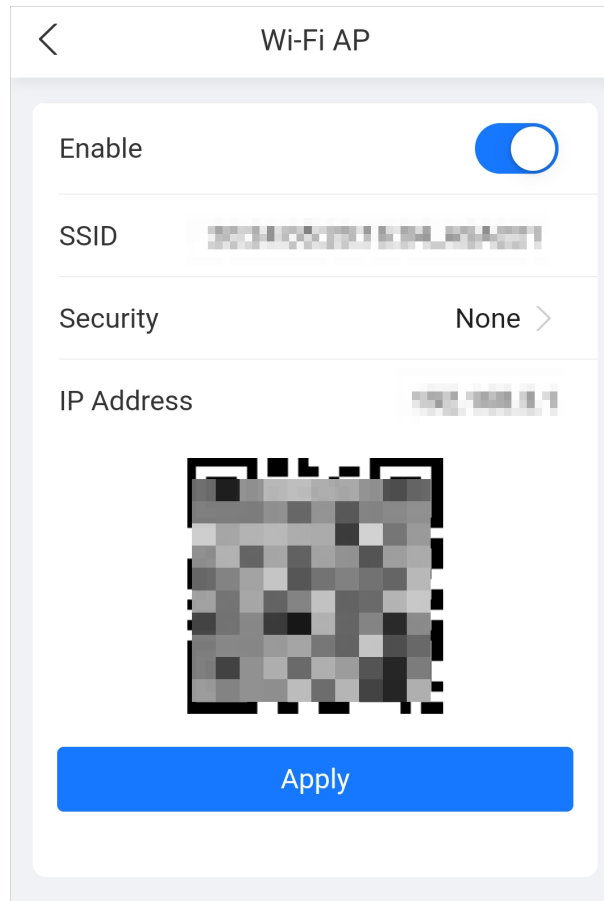


- The Wi-Fi function is available on select models.
- The Wi-Fi and Wi-Fi AP cannot be enabled at the same time.

Procedure

- Step 1 Log in to the webpage.
- Step 2 Select **More** > **Communication Settings** > **Wi-Fi AP**.
- Step 3 Enable the function, and then click **Apply**.

Figure 4-27 Wi-Fi AP



4.7.4 Configuring Cloud Service

Procedure

- Step 1 Log in to the webpage.
- Step 2 Select **More** > **Communication Settings** > **Cloud Service**.
- Step 3 Turn on the cloud service function.
The cloud service goes online if the P2P and PaaS are online.
- Step 4 Click **Apply**.

4.7.5 Configuring Auto Registration

Procedure

- Step 1 Log in to the webpage.
- Step 2 Select **More** > **Network Setting** > **Auto Registration**.
- Step 3 Enable the auto registration function, configure the parameters, and then click **Apply**.

Figure 4-28 Auto registration

Table 4-12 Automatic registration description

Parameter	Description
Status	Displays the connection status of auto registration.
Server Address	The IP address or the domain name of the server.
Port	The port of the server that is used for automatic registration.
Registration ID	The registration ID (user defined) of the device. Adding the device to the management by entering the registration ID on the platform.

4.8 Configuring Audio Prompts

Set audio prompts during identity verification.

Procedure

- Step 1 Log in to the webpage.
- Step 2 Select **More** > **Audio and Video Config** > **Audio**.
- Step 3 Configure the audio parameters, and then click **Apply**.

Table 4-13 Parameters description

Parameters	Description
Speaker Volume	Set the volume of the speaker.
Key Sound	When this function is enabled, the device will produce sound when pressing the button.

4.9 Viewing Logs

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

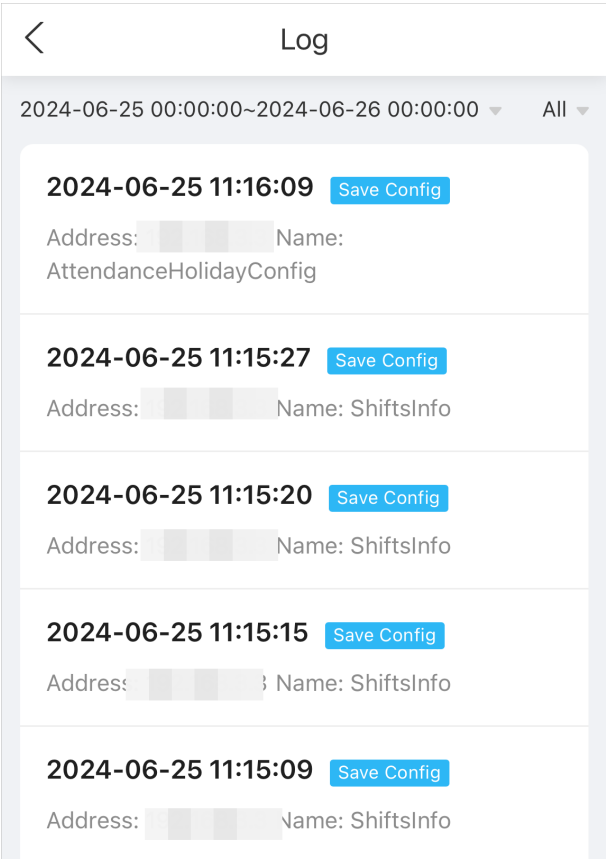
4.9.1 System Logs

View and search for system logs.

Procedure

- Step 1 Log in to the webpage.
- Step 2 Select **More** > **Log** > **Log**.

Figure 4-29 Logs



4.9.2 Unlock Records

Search for unlock records.

Procedure

- Step 1 Log in to the webpage.
- Step 2 Select **More** > **Log** > **Unlock Records**.
- Step 3 Click the record to view the details.

4.9.3 Alarm Logs

View alarm logs.

Procedure

- Step 1 Log in to the webpage.
- Step 2 Select **More** > **Log** > **Alarm Log**.

4.9.4 Attendance Logs

Procedure

- Step 1 Log in to the webpage.
- Step 2 Select **More** > **Log** > **Attendance Records**.
- Step 3 Tap the record to view the details.

5 SmartPSS Lite Operations

5.1 Installation

Contact technical support or go to the official website to get the SmartPSS Lite. If you get the software package of the SmartPSS Lite, install and run the software according to page instructions.

5.2 Initialization

Initialize SmartPSS Lite when you log in for the first time, including setting a password for login and security questions for resetting password.

Procedure

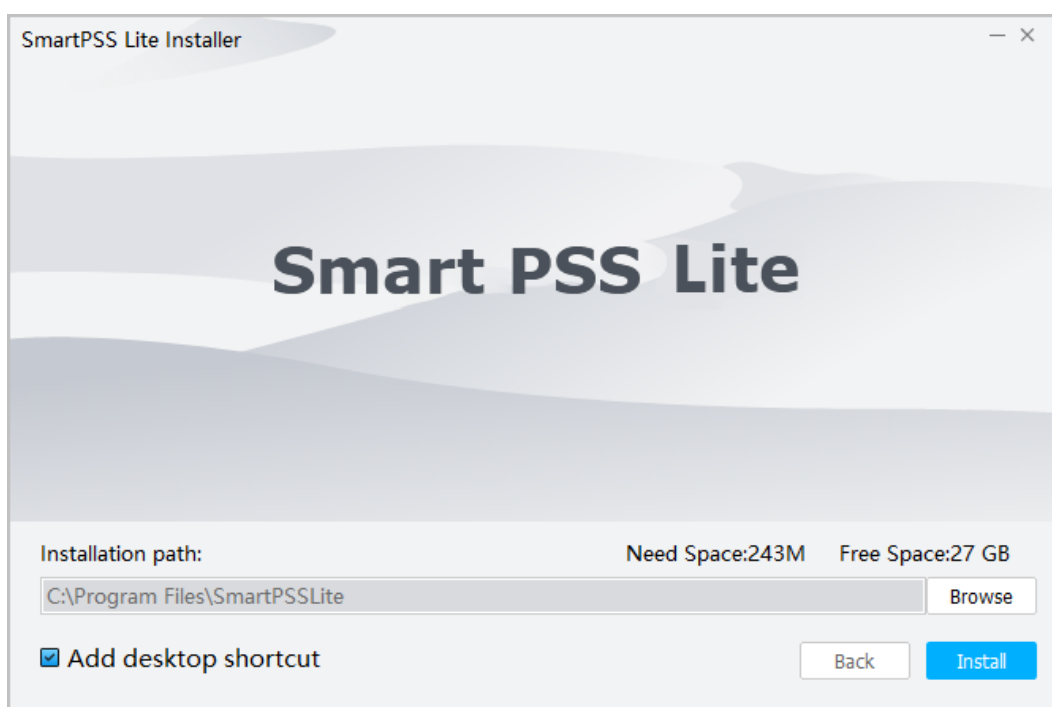
- Step 1 Double-click SmartPSSLite.exe.
- Step 2 Select the language from the drop-down list, select **I have read and agree the software agreement** , and then click **Next**.

Figure 5-1 Select language



- Step 3 Click **Browse** to select installation path, and then click **Install**.

Figure 5-2 Select installation path

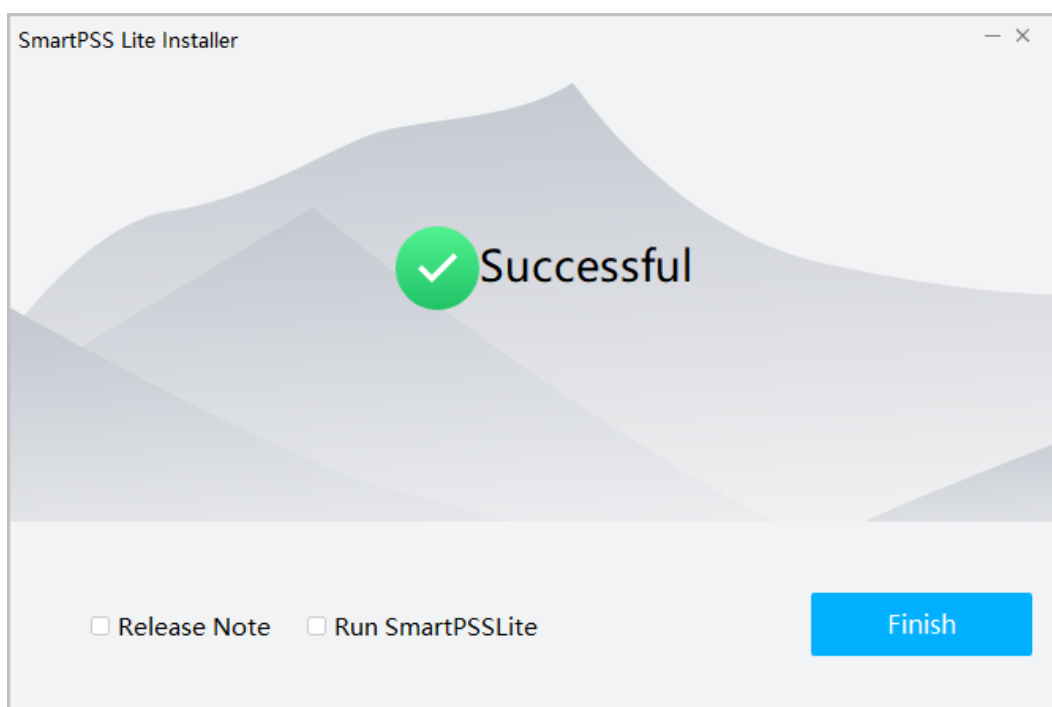


Step 4 Click **Finish** to complete the installation.



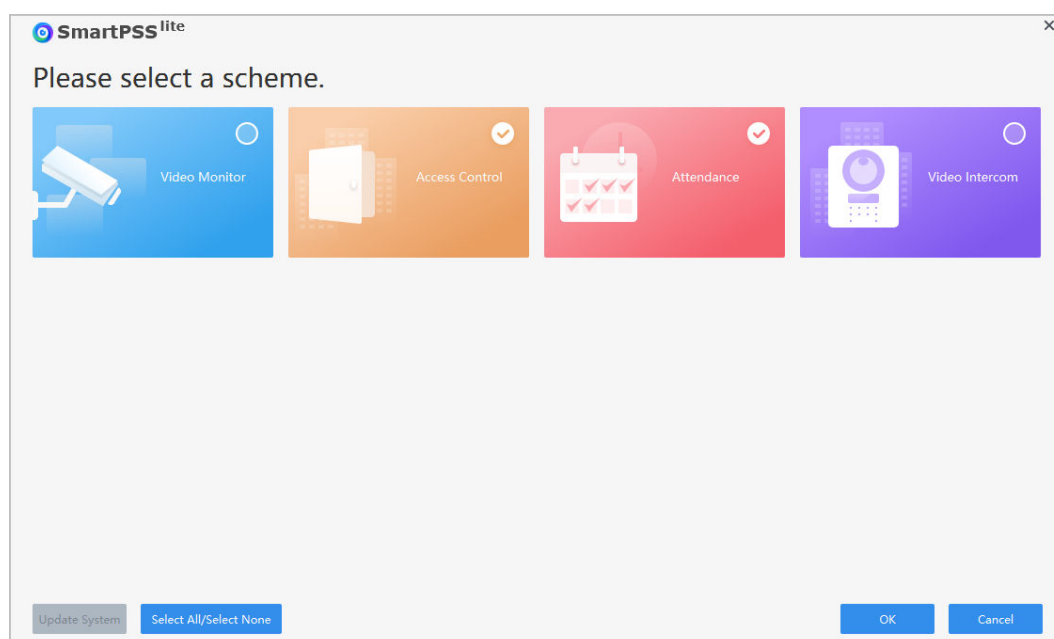
Select **Run SmartPSSLite** to start SmartPSS Lite.

Figure 5-3 Install complete



Step 5 Select the application scenes you want to add, and then click **OK**.

Figure 5-4 Select application scenes



Step 6 Click **Agree and Continue** to agree **Software License Agreement** and **Product Privacy Policy**.

Step 7 Set password on the **Initialization** page, and then click **Next**.

Figure 5-5 Set password

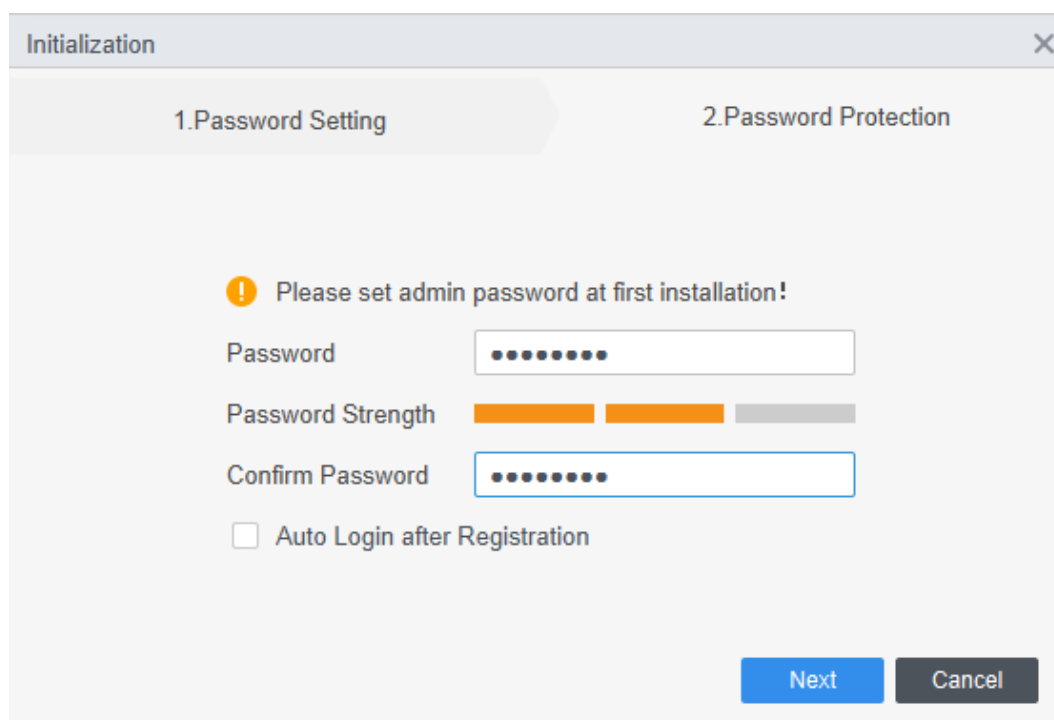


Table 5-1 Initialization parameters

Parameter	Description
Password	The password must consist of 8 to 32 non-blank characters and contain at least two types of characters among uppercase, lowercase, number, and special character (excluding ' " ; &).
Password Strength	Displays the effectiveness of a password against guessing or brute-force attacks. Green means the password is strong enough, and red means less strong. Set a password of high security level according to the password strength prompt.
Confirm Password	Enter the password again to confirm the password.
Auto Login after Registration	Enable Auto Login after Registration so that the SmartPSS Lite will log in automatically after initialization; otherwise the login page is displayed.

Step 8 Set security questions, and then click **Finish**.

Figure 5-6 Set security questions

The screenshot shows a window titled 'Initialization' with a close button (X) in the top right corner. Inside the window, there are two tabs: '1.Password Setting' and '2.Password Protection'. The '2.Password Protection' tab is active. Below the tabs, there is a yellow warning icon and the text 'Please set security questions!'. There are three sets of questions, each with a dropdown menu for the question and a text box for the answer. The questions are: 'What is your favorite children's book?', 'What was the first name of your first boss?', and 'What is the name of your favorite fruit?'. At the bottom right of the window, there is a blue button labeled 'Finish'.

5.3 Adding Devices

There are several methods available to add devices.

- Automatically search
- Manually adding
- Import in batches

5.3.1 Adding Device by Searching

You can add multiple devices by searching for them on the current network segment or other network segments.

Background Information



We recommend you add devices through searching when want to add multiple devices that are on the same network segment, or when you want to add devices with a known network segment but you do not know the exact IP address of the devices.

Procedure

Step 1 On the home page, click **Devices**.

Step 2 Select a search method.

- **Auto Search:** Enter the username and the password of the device. The system will automatically search for devices that are on the same network to your computer.
- **Device Network Segment:** Enter the username and the password of the device, and then define the start IP and the end IP. The system will automatically search for devices in this IP range.

Step 3 Click **Auto Search**.

Step 4 Enter a IP range, and then click **Search**.

The system automatically searches for devices in this IP range. You can also click **Auto Search** to automatically search for devices on the same network your computer is connected to.

Figure 5-7 Search for devices

No.	IP	Device Type	MAC Address	Port	Initialization Status
-----	----	-------------	-------------	------	-----------------------

Step 5 Select devices, and then click **Add**.

Step 6 Enter the login username and password of the selected devices, and then click **OK**.

Step 7 Enter the login user name and password, and then click **OK**.

The devices will be added to the platform.

Figure 5-8 Added devices

Total Devices										
☐	No.	Name	IP	Device Type	Device Model	Port	Number of Chann	Online Status	SN	Operation
☐	1	AC		Door Station		37777	2/0/10/2	Online		
☐	2	AC2		Access Controller		37777	2/0/0/0	Offline		

-  : Change the information of the device.
-  : Goes to the **Device Config** module in the platform.
-  : Goes to the webpage of the device.
-  : Log out of the device, and the status of the device will become **Offline**.
-  : Log in to the device, and the status of the device will become **Online**.
-  : Delete the device.

Related Operations

- Change IP one by one: Select a device, and then click **Change IP** to change the IP of the device.
- Change IP in batches: Select multiple devices, and then click **Change** to change their IP.



Enter the start IP, and the system will automatically assign IP to devices through increasing the IP by one based on the start IP. For example, if the start IP is 10.XX.XXX.52, and the following IP of devices will be 10.XX.XXX.53, 10.XX.XXX.54, and more.

- Initialize devices: Click **Initialize** to initialize devices.



Only support activating devices which are on the same network segment to your computer.

5.3.2 Adding Device One by One

If you already know the IP address of a device, you can manually add it to the platform.

Procedure

- Step 1 On the home page, click **Devices**.
- Step 2 Click **Add**, and then enter the device information.

Figure 5-9 Add devices

The 'Add Device' dialog box is shown with the following fields and controls:

- Device Name:** A text input field with a red asterisk indicating it is required.
- Add Mode:** A dropdown menu currently set to 'IP/Domain Name'.
- IP/Domain Name:** A text input field with a red asterisk indicating it is required.
- Port No.:** A text input field containing the value '37777' and a red asterisk indicating it is required.
- Username:** A text input field with a red asterisk indicating it is required.
- Password:** A text input field with a red asterisk indicating it is required.
- Buttons:** 'Add and Continue' (blue), 'Add' (blue), and 'Cancel' (grey).

Table 5-2 Parameters of IP adding

Parameter	Description
Device Name	The name of the device.
Add Mode	- IP/Domain Name: Add devices through IP Address. - SN (Available on devices that support P2P): Add devices through their serial number.
IP/Domain Name	Enter the IP address or domain name of the device.
Port No.	Enter the port number (80 by default).
Username	Enter the username and the password of the device.
Password	

Step 3 Click **Add**.

You can also click **Add and Continue** to add more devices.

5.3.3 Importing Device in Batches

You can export the device information, and then import it to another platform to add them in batches. We recommend you add devices by importing them when the devices are not on the same network segment.

Prerequisites

A .xml file of device information was exported. For details, see the corresponding user's manual.

Procedure

- Step 1 On the home page, click **Devices**.
- Step 2 Click **Import** to import the file the platform.



Devices will be logged in automatically after adding.

5.4 Adding Departments

Procedure

- Step 1 Select **Person** > **Person Management**.
- Step 2 In the department organization tree, click **+**.
- Step 3 Select a existing department, and then enter the name of the new department.
- Step 4 Click **OK**.

Figure 5-10 Add departments

The screenshot shows a dialog box titled "Add Department". It has a close button (X) in the top right corner. Inside the dialog, there are two input fields. The first is labeled "Department:" and has a dropdown menu currently showing "Default Company\HR" with a downward arrow. The second is labeled "Department Name:" and is an empty text box. At the bottom right of the dialog, there are two buttons: "OK" (blue) and "Cancel" (gray).

Related Operations

- Click  to delete the department.
- Click  to rename the department.

5.5 Adding Personnel

5.5.1 Adding Personnel One by One

Procedure

- Step 1 Select **Person** > **Person Management**, and then click **Add**.
- Step 2 Enter basic information of person.
1. Select **Basic Info**.
 2. Add basic information of personnel.
 3. Take snapshot or upload picture, and then click **Finish**.
 4. Configure identity verification methods.

- Set password

Click **Add** to add the password. For second-generation access controllers, set person passwords; for other devices, set card passwords. New passwords must consist of 6-8 digits.

- Configure card

- a. Click  to select **Device** or **Card issuer** as card reader.
- b. Add card.
- c. After adding, you can select the card as main card or duress card, or replace the card with a new one, or delete the card.
- d. Click  to display the QR code of the card.



Only 8-digit card number in hexadecimal mode can display the QR code of the card.

- Configure fingerprint

- a. Click  to select **Device** or **Fingerprint Scanner** as the fingerprint collector.
- b. Add fingerprint. Select **Add** > **Add Fingerprint**, and then press finger on the scanner for three times continuously.

- Configure feature codes

- a. Click , and then select a device.
- b. Click **Extract**, and then the device will extract the features of the face.

Figure 5-11 Add basic information

Add User

Basic Info

More Info

Person ID: *

Name: *

Department:

ult Company\HumanResource

Person Type:

Normal User

Effective Time:

2023/12/29 0:00:00

2023/12/29 23:59:59

3654 Day

Times Used:

Unlimited

Profile Picture

Take Snapshot

Upload Picture

Image size: 0-100 KB

Face1

Take Snapshot

Upload Picture

Image size: 0-100 KB

Face2

Take Snapshot

Upload Picture

Image size: 0-100 KB

Password

Add

For the second-generation access control device, it is the person password. Otherwise it is the card password.

Card

Add

The card number must be added if non-2nd generation access controller is used.

Fingerprint

+ Add

Delete

	Fingerprint Name	Operation
☐		

Add More

Complete

Cancel

Step 3 Click **More Info** tab to add extended information of the staff, and then click **Complete**.

Figure 5-12 Add more information

The 'Add User' dialog box has a title bar with a close button. It contains two tabs: 'Basic Info' and 'More Info'. The 'More Info' tab is active, showing a 'Details' section. The fields are arranged in two columns. The left column includes: Gender (radio buttons for Male and Female, with Male selected), Title (dropdown menu with 'Mr.' selected), Date of Birth (calendar icon, showing 1985/3/15), Phone No. (text input), Email (text input), Communication A... (text input), and Admin (toggle switch). The right column includes: Credential Type (dropdown menu with 'ID Card' selected), Credential No. (text input), Organization (text input), Occupation (text input), Employment Date (calendar icon, showing 2023/12/28 11:11:18), and Termination Date (calendar icon, showing 2033/12/29 11:11:18). At the bottom, there is a 'Remarks' text area. At the bottom right, there are three buttons: 'Add More' (blue), 'Complete' (blue), and 'Cancel' (grey).

Step 4 Click **Complete**.



After completing adding, you can click  to modify information or add details in the list of person.

Related Operations

- Click  to modify information or add details in the list of staff.
- Click  to delete all information of the person.
- Click  to freeze the card, and then the card cannot be used normally.

5.5.2 Adding Personnel in Batches

Procedure

- Step 1 Select **Person** > **Person Management**, and then click **Batch Add**.
- Step 2 Select the device type, set the start number, number of card.
- Step 3 Set the department, and the effective time and expiration time of card.
- Step 4 Click **Read Card No.**.
- Step 5 Place cards on the card issuer or the card reader.
The card number will be read automatically or filled in automatically.
- Step 6 Click **OK**.

Figure 5-13 Add personnel in batches

Batch Add

Device: Card Issuer

Start No.: 5

Quantity: 10

Department: Dropdown list

Validity Time: 2022/11/24 0:00:00

Expiration Time: 2032/11/24 23:59:59

Read C...

Issue Card

ID	Card No.
----	----------

OK Cancel

5.6 Permission Configuration

5.6.1 Adding Permission Areas

An area is a collection of door access permissions. Create an area, and then link users to the area so that they can gain access permissions set for the area.

Procedure

Step 1 Select **Access Control Config > Area Config**.

Step 2 Click **+** to add a permission area.



You can add up to 40 areas.

Step 3 Configure the permission area.

1. Enter area name and remark.
2. Select door channels, such as door 1.
3. Click **OK**.

Figure 5-14 Add permission area

Related Operations

- : Delete the permission area.
- : Modify the area information.

5.6.2 Assigning Permissions

The method to configure permission for department and for personnel is similar, and here uses department as an example.

Procedure

- Step 1** Select **Access Control Config** > **Permission Settings**.
- Step 2** Click  to add a permission rule.

Figure 5-15 Assign permissions rules

The screenshot shows the 'Add Permission Rule' dialog box. It has a title bar with a close button. Below the title bar, there's a search bar and a list of users. The 'Person Info' section has a search bar, a list of users, and a 'No data' message with an 'Add' button. The 'Area Info' section has a search bar, a list of areas, and a 'No data' message with an 'Add' button. The 'Add' buttons are highlighted with orange boxes and numbered 3 and 4 respectively. The dialog also features a 'Name' field, a 'Remarks' field, and a 'Select Data to be Sent' section with checkboxes for Card, Fingerprint, Password, and Face. The dialog is titled 'Add Permission Rule' and has a close button in the top right corner.

- Step 3** Enter the name of the permission rule, select the time plan and unlock methods.
- Step 4** In the **Person Info** area, click **Add** to select personnel, and then click **OK**.

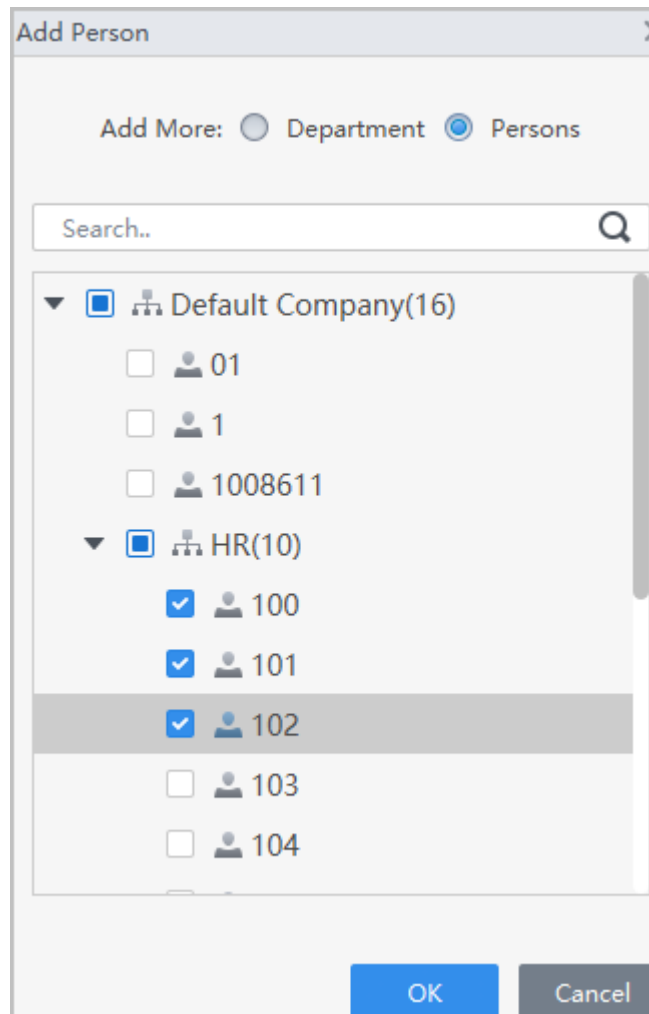
You can select personnel on the department or individual users.

- Dept: All personnel in the department will be assigned with access permissions.
- User: Only selected users will be assigned with access permissions.



When you want to assign permission to a new person or change access permissions for an existing person, you can simply add the user in a existing department or link them with a existing role, they will be automatically assigned access permissions set for the department or role.

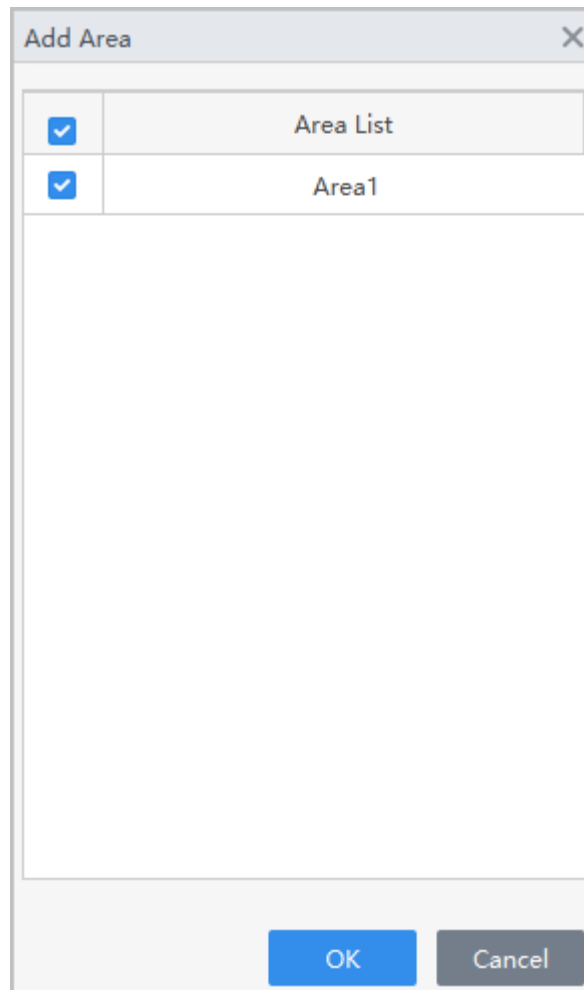
Figure 5-16 Add users



You can click **+** to create new permission areas. For details on creating permission areas, see the corresponding user's manual.

Step 5 In the **Area Info**, click **Add** to select an area, and then click **OK**.

Figure 5-17 Add area

A dialog box titled "Add Area" with a close button (X) in the top right corner. It contains a table with two columns: a checkbox column and an "Area List" column. The first row has a checked checkbox and the text "Area1". Below the table is a large empty rectangular area. At the bottom right are "OK" and "Cancel" buttons.

☒	Area List
☒	Area1

Step 6 Click **OK**.

Step 7 If authorization failed, click  in the list to view the possible reason.

Figure 5-18 Authorization progress

Permission Group	Device Name	Progress	Status	Result of Issuing	Operation
Permission Group3		1/1	Finished issuing	Successful: 1, Failed: 0	

5.7 Configuring Attendance Period

Set attendance schedules and attendance rules for fixed attendance mode or flexible attendance mode. Up to 32 attendance schedules can be added.

5.7.1 Configuring Fixed Attendance Schedules

Procedure

Step 1 Select **Attendance** > **Attendance Period**.

Step 2 Click **Add**, and then add an attendance schedule.

You can mark the attendance schedule in different color. When you arrange and apply shifts, the color will be displayed on the calendar.

Figure 5-19 Fixed attendance

Fixed Attendance Flexible Attendance

General Break

Basic Info

Period Name * Default Time Color: Blue

Attendance Period:

Working Time: 08:30 - 17:30 ! The time span must not exceed 24 hours.

Recorded: 540.0 minutes

Valid Check-in Time: 06:30 - Valid Check-out Time: 19:30

☒ Use First Check-In and Last Check-Out Only

☒ It overlaps with a holiday and is calculated as a holiday.

☒ Break Time Counted as Work Time

Attendance Rule:

☒ Valid work starts 60.00 minutes when the work day ends.

☒ Allowed to be 5.00 minutes late.

☒ Being late for more than 120.00 minutes is considered as absent.

☒ Allowed to leave 5.00 minutes early.

☒ Leaving early for more than 120.00 minutes is considered as absent.

Overtime Rule ☒

☒ The minimum overtime is 60.00 minutes. If it is insufficient, it will be recorded as n...

☒ The maximum overtime is 300.00 minutes

Table 5-3 Fixed attendance parameters

Item	Parameter	Description
Attendance period	Period Name	Enter the period name. You can mark the attendance schedule in different color. When you arrange and apply shifts, the color will be displayed on the calendar.

Item	Parameter	Description
	Working time	The start time and the end time of a workday.  The time span must not exceed 24 hours.
	Valid check-in time- Valid check-out time	Specify a time range when people can clock in and clock out for the workday.
	Use First Check-In and Last Check-Out Only	If a person clocks in and out multiple times in a day, the earliest and latest times will be valid.
	It overlaps with a holiday and is calculated as a holiday.	If the employee is scheduled to work on a holiday, and then the total worked hours = The actual worked hours * Holiday work rate. For how to set holiday work rate, see the corresponding user's manual.
	Break Time Counted as Work Time	The rest time is not deducted from the total work time.
Attendance Rule	Valid work starts "N" minutes when the work day ends	The defined time period will not be included in the total hours worked. For example, if the "N" is set to 60 minutes and the specified clock-out time is 17:00, when you clock out at 19:00, only one extra hour will be added to your total hours worked.
	Allowed to be "N" minutes late	A "tolerance time" is given if employee's clock-in is late by the set time, For example, if the "N" is set to 5 minutes and the clock-in time for the beginning of the work days is 8:00, when you clock in at 8:05, it will not be considered late.
	Being late for more than "N" minutes is considered as absent	If the person clocks in after the time limit, they will be considered as absent. For example, if "N" is set as 30 minutes, and the clock-in time for the beginning of the work day is 9:00, when a person clocks in at 9:40, they will be considered as absent for one day.
	Allowed to leave "N" minutes early	A "tolerance time" is offered so that when employees clock out earlier than the time set to end the work day, and they will not be considered as leaving too early. For example, if "N" is set as 5 minutes, and the clock-out time for the end of the work day is 17:00, if a person clocks out at 16:55, they will not be considered as clocking out too early.
	Leaving early for more than "N" minutes is considered as absent	If the person clocks in before the time limit, they will be considered as absent. For example, if "N" is set as 30 minutes, and the clock-out time for the end of the work day is 17:00, when a person clocks out at 16:20, they will be considered as absent for one day.

Item	Parameter	Description
Overtime Rule	The minimum overtime is "N" minutes. If it is insufficient, it will be recorded as no overtime.	If the time a employee's overtime is less than the defined time, they will not be considered as working overtime.
	The maximum overtime is "N" minutes	The upper limit of overtime. For example, if "N" is set as 300 minutes, when an employee has 500 minutes of overtime worked, the overtime will still be recorded as 300 minutes.

Step 3 Configure break periods.

For the fixed attendance mode, you can add up to 7 break periods.

1. Click **Break** tab, and the click **Management**.
2. Click **Add**, enter the name of the break, and then set the start time and the end time of the rest.

During this time a break may be taken.

3. Select the break rule.
 - **Auto Deduction:** The defined break time is automatically deducted from an employee's total hours worked.
 - **Must Check In/Out:** The actual break time is calculated according to the time the employee clocks in and out.
 - ◇ **Validity Start Time/Validity End Time:** Set a time period when employees can clock out for the break time, and clock back in for the end of the break.
 - ◇ **Convert Unused Break Time to Work Time:** If employees only rest 30 minutes out of the defined 1 hour break period, the remaining 30 minutes will be added to their total hours worked.
 - ◇ **Break that last longer than "N" Minutes will be recorded as:** If the break time exceeds the defined limit, it is recorded as late for late, left early or absent.
4. Click **OK**.

Figure 5-20 Add break periods

The screenshot shows a 'Management' window with a sidebar containing '+ Add' and 'Delete' icons. The main area contains the following fields and options:

- Break Name:** A text input field with a red asterisk indicating it is required.
- Start Time:** A time picker set to 00:00.
- End Time:** A time picker set to 00:00.
- Break Period:** A spinner set to 0.00 minutes.
- Radio Buttons:** 'Auto Deduction' (unselected) and 'Must Check In/Out' (selected).
- Valid Start Time:** A time picker set to 00:00.
- Valid End Time:** A time picker set to 00:00.
- Convert Unused Break Time to Work Time:** An unchecked checkbox.
- Breaks that last longer th...:** A checkbox (unchecked) followed by a spinner set to 120.00 minutes and a dropdown menu set to 'Late'.
- Buttons:** 'OK' (blue) and 'Cancel' (grey) at the bottom right.

Step 4 Click **Select** to select a break schedule.

Step 5 Click **OK**.

5.7.2 Configuring Flexible Attendance Schedules

Flexible attendance means the attendance time are not fixed for a workday.

Procedure

Step 1 Select **Attendance** > **Attendance Period**.

Step 2 Click **Flexible Attendance**, click **Add**, and then add an attendance schedule.

You can mark the attendance schedule with colors. When you arrange and apply shifts, the color will be displayed on the calendar.

Figure 5-21 Flexible attendance

Fixed Attendance
Flexible Attendance

Basic Info

Period Name
* Default Time
Color:
Blue

Required work hours
480.0
minutes

Following Day Check In/Out Time
00:00
?

☒ Use First Check-In and Last Check-Out Only

Overtime Rule

☒ The minimum overtime is
60.00
minutes. If it is insufficient, it will be recorded as no overtime.

☒ The maximum overtime is
300.00
minutes

Table 5-4 Fixed attendance parameters

Item	Parameter	Description
Basic Info	Period Name	Enter the period name. You can mark the attendance schedule in different color. When you arrange and apply shifts, the color will be displayed on the calendar.
	Required work hours	The minimum set of hours required to complete a work day. The time to clock in and out are not fixed.
	Following Day Check In/Out Time	The period for people to clock in and out. For example, if the time for following day check in/out time is to 11:00, then another work day begins at 11:00 and ends at 10:59, and employee much clock in and clock out during this period.
	Use First Check-In and Last Check-Out Only	If a person clocks in and out multiple times in a day, the earliest and latest times will be valid.
Overtime Rule	The minimum overtime is "N" minutes. If it is insufficient, it will be recorded as no overtime.	If the time a employee's overtime is less than the defined time, they will not be considered as working overtime.

Item	Parameter	Description
	The maximum overtime is "N" minutes	The upper limit of overtime. For example, if "N" is set as 300 minutes, when an employee has 500 minutes of overtime worked, the overtime will still be recorded as 300 minutes.

Step 3 Click **Save**.

5.8 Adding Attendance Shifts

You can arrange shift by day or week. Here uses the weekly shift as an example.

Prerequisites

Make sure that you have configured attendance periods before managing the attendance shifts.

Procedure

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

Step 2 Click **Add** on the upper-left corner of page.

Step 3 Set the shift name, start date, loop mode and cycle period, and then drag the period to the calendar to arrange the shift.



The existing period will be overwritten if the newly configured period is in conflict with it.

You can assign up to 3 attendance periods for one person in a day.

Click **Clear All** to clear all the settings.

Figure 5-22 Set attendance shift

Basic Info

Shift Name: * Shift pp

Start Time: 2024-04-24

Loop Mode: Day Week

Number of Cycles: 7

Period (Drag to the calendar to arrange the schedule)

		14:30-17:00	Shift 2
		08:30-12:30	default period
		21:30-23:30	Shift 3

Schedule Image (Right-click to clear shifts)

Clear All

	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23
2024-04-24 (Wed)																								
2024-04-25 (Thu)																								
2024-04-26 (Fri)																								
2024-04-27 (Sat)																								
2024-04-28 (Sun)																								
2024-04-29 (Mon)																								

Save Cancel

Step 4 Click **Save** , and then click **OK** to confirm operation.

5.9 Configuring Shift Schedules

5.9.1 Configuring Shift Schedules for Department

Procedure

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

Step 2 Select a shift.

Step 3 Select the start time and the end time.

The shift will repeat during this period.

Step 4 Click **Assign to Department**, and then select a department.

Step 5 Click **OK**.

The shift will be assigned to the personnel automatically.

Figure 5-23 Assign shifts to department

Shift: 1
Default Shift

Start Time: 2
2024-01-15

End Time: 2024-01-18

Assign to Person

Assign to Department 3

Assign to Department

Search... 4

Default Company

HR

OK 5 Cancel

Step 6 Select **By Shift** or **By Person**, and click  to save the settings.

- By Shift: Select a shift, view the personnel that the current shift was assigned to.
- By Person: Select a person, view the shifts that was assigned to the current person.

Figure 5-24 By shift

By Shift		By Person						
Schedule ...		Config Details						
☐	Shift Name	Shift	Department	Person ID	Person Name	Start Time	End Time	Operation
☒	Default Shift	Default Shift	HR	100	100	2024-01-15	2024-01-18	 
☐	111	Default Shift	HR	101	101	2024-01-15	2024-01-18	 

Figure 5-25 By person

By Shift		By Person						
Department		Config Details						
Search...		Shift	Department	Person ID	Person Name	Start Time	End Time	Operation
▼ Default Company		Default Shift	HR	100	100	2024-01-15	2024-01-18	
☐ 01		Default Shift	HR	101	101	2024-01-15	2024-01-18	
▼ HR								
☒ 100								
101								

Related Operations

- : Delete the current shift.
- : Select a shift, and then click **Clear** to clear all shifts that were assigned to personnel.

5.9.2 Configuring Shifting Schedules for Personnel

Procedure

- Step 1 **Attendance > Shift Schedule**
- Step 2 Select a shift.
- Step 3 Select the start time and the end time.
 The shift will repeat during this period.
- Step 4 Click **Assign to Person**, and select personnel.
- Step 5 Click **OK**.
 The shift will be assigned to the personnel automatically.

Figure 5-26 Assign shifts to person

Step 6 Select **By Shift** or **By Person**, and click  to save the settings.

- By Shift: Select a shift, view the personnel that the current shift was assigned to.
- By Person: Select a person, view the shifts that was assigned to the current person.

Figure 5-27 By shift

By Shift		By Person						
Schedule ...		Config Details						
☐	Shift Name	Shift	Department	Person ID	Person Name	Start Time	End Time	Operation
☒	Default Shift	Default Shift	HR	100	100	2024-01-15	2024-01-18	
☐	111	Default Shift	HR	101	101	2024-01-15	2024-01-18	

Figure 5-28 By person

By Shift		By Person						
Department	Config Details							Clear
Search...	Shift	Department	Person ID	Person Name	Start Time	End Time	Operation	
Default Company 01 HR 100 101	Default Shift	HR	100	100	2024-01-15	2024-01-18		
	Default Shift	HR	101	101	2024-01-15	2024-01-18		

Related Operations

- : Delete the current shift.
- : Select a shift, and then click **Clear** to clear all shifts that were assigned to personnel.

Appendix 1 Important Points of Fingerprint Registration Instructions

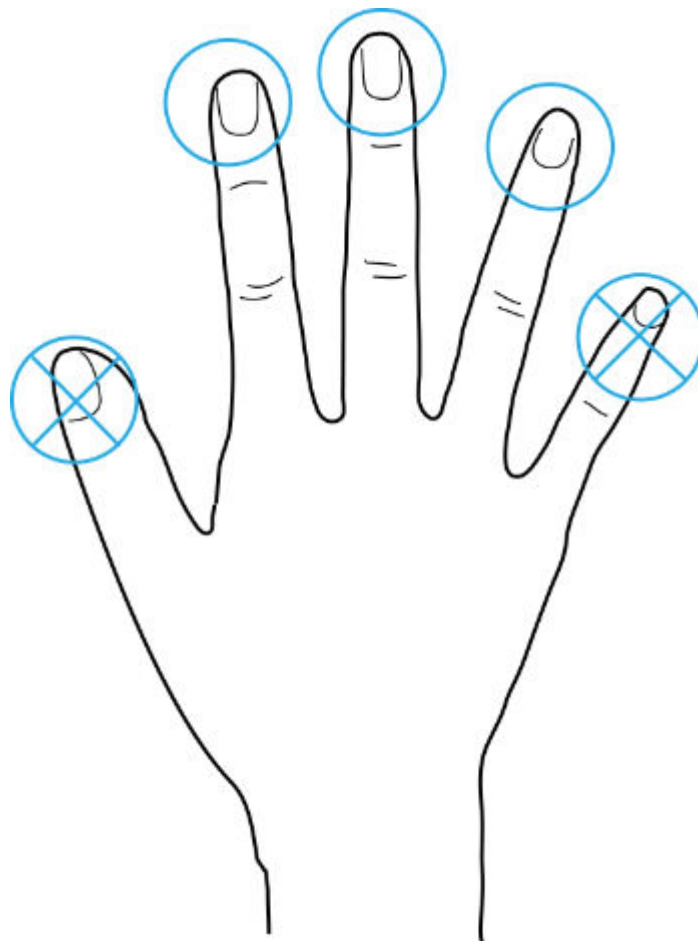
When you register the fingerprint, pay attention to the following points:

- Make sure that your fingers and the scanner surface are clean and dry.
- Press your finger on the center of the fingerprint scanner.
- Do not put the fingerprint sensor in a place with intense light, high temperature, and high humidity.
- If your fingerprints are unclear, use other unlocking methods.

Fingers Recommended

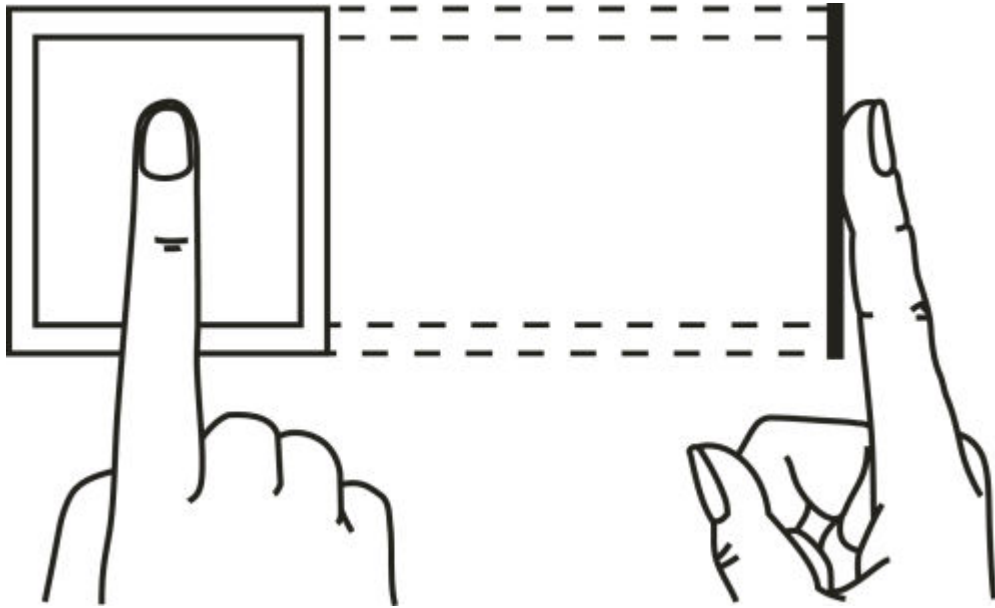
Forefingers, middle fingers, and ring fingers are recommended. Thumbs and little fingers cannot be put at the recording center easily.

Appendix Figure 1-1 Recommended fingers

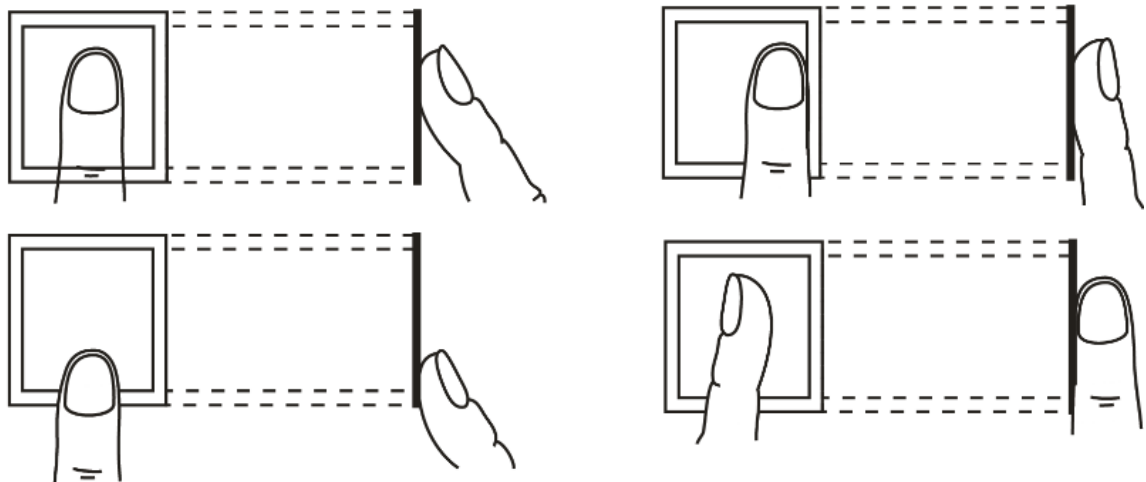


How to Press Your Fingerprint on the Scanner

Appendix Figure 1-2 Correct placement



Appendix Figure 1-3 Wrong placement



Appendix 2 FAQ

- Q: The Device prompts me to do it again after I have placed my finger on the sensor.
A: Check if your fingerprints have been registered.
- Q: The bell does not ring.
A: Check if bell ring is set successfully and the broadcast volume switch is on.
- Q: I cannot update the Device through the USB.
A: Check if the Device is successfully recognized by the Device, and check the update file name.
- Q: Failed to export by USB flash drive.
A: Use USB in FAT32 format.
- Q: I forget administrator password.
A: Contact the manufacturer.
- Q: How to search for user attendance record?
A: On the standby screen, tap #, and then place your finger on the fingerprint sensor, or enter the user ID and password, or swipe the card.

Appendix 3 Security Recommendation

Account Management

1. Use complex 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: 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 repeating characters, such as 111, aaa, etc.

2. Change passwords periodically

It is recommended to periodically change the device password to reduce the risk of being guessed or cracked.

3. Allocate accounts and permissions appropriately

Appropriately add users based on service and management requirements and assign minimum permission sets to users.

4. Enable account logout function

The account logout function is enabled by default. You are advised to keep it enabled to protect account security. After multiple failed password attempts, the corresponding account and source IP address will be locked.

5. Set and update password reset information in a timely manner

The device supports password reset function. To reduce the risk of this function being used by threat actors, if there is any change in the information, please modify it in time. When setting security questions, it is recommended not to use easily guessed answers.

Service Configuration

1. Enable HTTPS

It is recommended that you enable HTTPS to access web services through secure channels.

2. Encrypted transmission of audio and video

If your audio and video data contents are very important or sensitive, it is recommended to use encrypted transmission function in order to reduce the risk of your audio and video data being eavesdropped during transmission.

3. Turn off non-essential services and use safe mode

If not needed, it is recommended to turn off some services such as SSH, SNMP, SMTP, UPnP, AP hotspot etc., to reduce the attack surfaces.

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

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

4. Change HTTP and other default service ports

It is recommended that you change the default port of HTTP and other services to any port between 1024 and 65535 to reduce the risk of being guessed by threat actors.

Network Configuration

1. **Enable Allowlist**

It is recommended that you turn on the allowlist function, and only allow IP in the allowlist to access the device. Therefore, please be sure to add your computer IP address and supporting device IP address to the allowlist.

2. **MAC address binding**

It is recommended that you bind the IP address of the gateway to the MAC address on the device to reduce the risk of ARP spoofing.

3. **Build a secure network environment**

In order to better ensure the security of devices and reduce potential cyber risks, the following are recommended:

- Disable the port mapping function of the router to avoid direct access to the intranet devices from external network;
- According to the actual network needs, partition the network: if there is no communication demand between the two subnets, it is recommended to use VLAN, gateway and other methods to partition the network to achieve network isolation;
- Establish 802.1x access authentication system to reduce the risk of illegal terminal access to the private network.

Security Auditing

1. **Check online users**

It is recommended to check online users regularly to identify illegal users.

2. **Check device log**

By viewing logs, you can learn about the IP addresses that attempt to log in to the device and key operations of the logged users.

3. **Configure network log**

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

Software Security

1. **Update firmware in time**

According to the industry standard operating specifications, the firmware of devices needs to be updated to the latest version in time in order to ensure that the device has the latest functions and security. If the device is connected to the public network, it is recommended to enable the online upgrade automatic detection function, so as to obtain the firmware update information released by the manufacturer in a timely manner.

2. **Update client software in time**

It is recommended to download and use the latest client software.

Physical Protection

It is recommended that you carry out physical protection for devices (especially storage devices), such as placing the device in a dedicated machine room and cabinet, and having access control

and key management in place to prevent unauthorized personnel from damaging hardware and other peripheral equipment (e.g. USB flash disk, serial port).