



User Manual

Bio-1

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
V1.0.0	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, 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.....	3
2.3 Powering On.....	4
2.4 Unlocking Methods.....	4
2.4.1 Unlocking by Cards.....	4
2.4.2 Unlocking by Fingerprints.....	4
2.4.3 Unlocking by User Password.....	4
2.5 Creating Administrator Account.....	5
2.6 Logging In.....	5
2.7 User Management.....	6
2.7.1 Adding Users.....	6
2.7.2 Viewing User Information.....	8
2.7.3 Configuring the Admin Unlock Password.....	9
2.8 Access Control Management.....	9
2.8.1 Configuring Unlock Combinations.....	10
2.8.2 Configuring Alarms.....	10
2.8.3 Configuring the Door Status.....	11
2.8.4 Configuring the Verification Time Interval.....	12
2.9 Attendance Management.....	12
2.9.1 Configuring Departments.....	12
2.9.2 Configuring Shifts.....	12
2.9.3 Configuring Holiday.....	14
2.9.4 Configuring Work Schedules.....	14
2.9.5 Configuring Attendance Modes.....	16
2.10 Communication Settings.....	17
2.10.1 Configuring the IP Address.....	17
2.10.2 Configuring Wi-Fi.....	18
2.10.3 Configuring Wi-Fi AP.....	19
2.11 System Settings.....	19
2.11.1 Configuring Time.....	20
2.11.2 Configuring the Volume.....	20
2.11.3 Configuring the Language.....	21
2.11.4 Configuring Screen Parameters.....	21
2.11.5 Configuring Ringtone.....	22

2.11.6 Restoring Factory Defaults.....	22
2.11.7 Restarting the Device.....	22
2.12 USB Management.....	23
2.12.1 Exporting to USB.....	23
2.12.2 Importing from USB.....	23
2.12.3 Updating the System.....	24
2.13 Record Management.....	24
2.14 System Information.....	24
2.14.1 Viewing Data Capacity.....	24
2.14.2 Viewing Device Version.....	24
3 Webpage Operations.....	25
3.1 Initialization.....	25
3.2 Resetting the Password.....	25
3.3 Home Page.....	26
3.4 Person Management.....	27
3.5 Configuring Attendance.....	31
3.5.1 Configuring Departments.....	31
3.5.2 Configuring Shifts.....	31
3.5.3 Configuring Holiday.....	34
3.5.4 Configuring Work Schedules.....	35
3.5.5 Configuring Attendance Mode.....	37
3.6 Configuring Access Control.....	39
3.6.1 Configuring Access Control Parameters.....	39
3.6.2 Configuring Alarms.....	42
3.6.3 Configuring Alarm Event Linkage.....	43
3.6.4 Configuring Card Settings.....	44
3.6.5 Configuring Periods.....	46
3.7 Access Monitoring.....	49
3.8 Configuring Audio.....	50
3.9 Communication Settings.....	51
3.9.1 Configuring TCP/IP.....	51
3.9.2 Configuring Wi-Fi.....	53
3.9.3 Configuring Wi-Fi AP.....	54
3.9.4 Configuring Port.....	55
3.9.5 Configuring Basic Service.....	56
3.9.6 Configuring Cloud Service.....	58
3.9.7 Configuring Auto Registration.....	59
3.9.8 Configuring CGI Auto Registration.....	60
3.9.9 Configuring Auto Upload.....	61
3.10 Configuring the System.....	62

3.10.1 User Management.....	62
3.10.2 Viewing Online Users.....	65
3.10.3 Configuring Time.....	65
3.10.4 Configuring Ringtone.....	67
3.11 Maintenance Center.....	67
 3.11.1 One-click Diagnosis.....	67
 3.11.2 System Information.....	68
 3.11.3 Data Capacity.....	68
 3.11.4 Viewing Logs.....	68
 3.11.5 Maintenance Management.....	70
 3.11.6 Updating the System.....	71
 3.11.7 Advanced Maintenance.....	72
3.12 Security Settings (Optional)	73
 3.12.1 Security Status.....	73
 3.12.2 Configuring System Service.....	74
 3.12.3 Attack Defense.....	74
 3.12.4 Installing Device Certificate.....	77
 3.12.5 Installing the Trusted CA Certificate.....	80
 3.12.6 Security Warning.....	81
 3.12.7 Security Authentication.....	82
4 Phone Operations.....	83
 4.1 Logging in to the Webpage.....	83
 4.2 Home Page.....	84
 4.3 Person Management.....	86
 4.4 Configuring the System.....	89
 4.4.1 Viewing Version Information.....	90
 4.4.2 Maintenance.....	90
 4.4.3 Configuring Time.....	90
 4.4.4 Data Capacity.....	92
 4.4.5 Configuring Ringtone.....	92
 4.5 Configuring Attendance.....	93
 4.5.1 Configuring Departments.....	93
 4.5.2 Configuring Shifts.....	95
 4.5.3 Configuring Holiday.....	98
 4.5.4 Configuring Work Schedules.....	98
 4.5.5 Configuring Attendance Mode.....	100
 4.6 Configuring Access Control.....	101
 4.6.1 Configuring Unlock Methods.....	101
 4.6.2 Configuring Access Control Parameters.....	102
 4.6.3 Configuring Alarms.....	104



4.6.4 Configuring Alarm Event Linkage.....	106
4.6.5 Configuring Card Settings.....	107
4.7 Communication Settings.....	108
4.7.1 Configuring TCP/IP.....	108
4.7.2 Configuring Wi-Fi.....	110
4.7.3 Configuring Wi-Fi AP.....	110
4.7.4 Configuring Cloud Service.....	111
4.7.5 Configuring Auto Registration.....	111
4.8 Configuring Audio Prompts.....	112
4.9 Viewing Logs.....	113
4.9.1 System Logs.....	113
4.9.2 Unlock Records.....	113
Appendix 1 Important Points of Fingerprint Registration Instructions.....	115
Appendix 2 FAQ.....	117
Appendix 3 Security Recommendation.....	118



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 on other modes, see "2.9.5 Configuring Attendance Modes".

Table 2-1 Button description

Button	Description
0-9	<ul style="list-style-type: none"> 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 0 for 3 seconds, and use the administrator password to open the door. The attendance function in this situation is invalid.
ESC/F1	<ul style="list-style-type: none"> Exit or go to the previous screen. Press it on the standby screen to configure the check in mode.

Button	Description
↖/F2	<ul style="list-style-type: none"> Press it on the standby screen to configure the break out mode. Press to go up the options.
↘/F3	<ul style="list-style-type: none"> Press it on the standby screen to configure the break in mode. Press it to go down through the options.
OK/F4	<ul style="list-style-type: none"> Confirm your settings. Press it on the standby screen to configure the check out mode.
#	<ul style="list-style-type: none"> 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.
✉ * ∅	<ul style="list-style-type: none"> 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. <p></p> <p>Only administrators can enter the main menu.</p> <ul style="list-style-type: none"> Press it to change the input types (numbers, letters and symbols).

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 ↘ 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 '' ;:&).

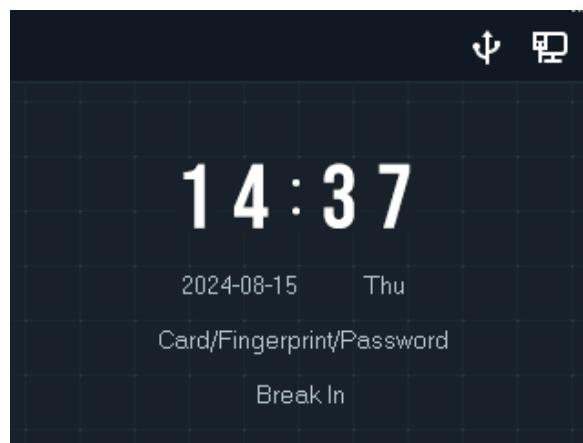
- Step 4 Press ↘ to select **Confirm Password**, and then press OK.

- 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.

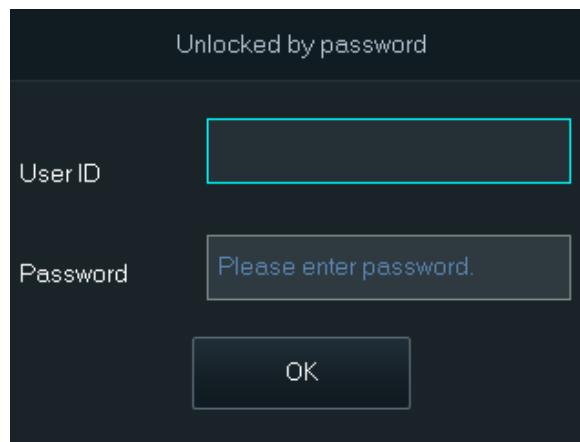
2.4.3 Unlocking by User Password

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.

2.5 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 2-2 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	<p>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.</p> <p></p> <ul style="list-style-type: none"> ● 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	<p>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.</p> <p>You can enable the Duress Card function. An alarm will be triggered if a duress card is used to unlock the door.</p> <p></p> <p>One user can only set one duress card.</p>
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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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. <p></p> <p>The delay time is not available for remote verification methods.</p> <ul style="list-style-type: none"> Custom User 1/Custom User 2 : Same with general users.
Department	Select departments, which is useful when configuring department schedules.
Schedule Mode	<ul style="list-style-type: none"> Department Schedule: Apply department schedules to the user. Personal Schedule: Apply personal schedules to the user. <p></p> <p>◊ 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.</p>

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

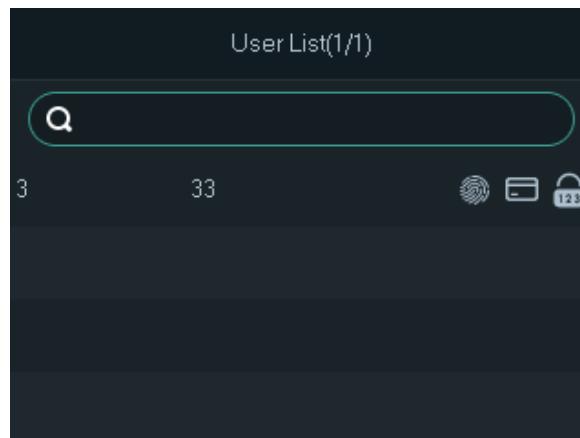
2.7.2 Viewing User Information

View the user or administrator information. You can edit or delete the user and administrator information.

Procedure

- Step 1 On the **Main Menu**, select **Users**.
- Step 2 Select **User List**, or select **Admin List**.
 - The user list displays all the user information in the Device.
 - The admin list displays all the administrator information in the device.
- Step 3 View all added users or admin accounts.
 - : Unlock through password.
 - : Unlock through swiping card.
 - : Unlock through fingerprint.

Figure 2-4 User list



Related Operations

- Search for users or administrators: Press \wedge or \vee to select the search box, enter the user number, user name, administrator number or the administrator name, and then press OK.
- Edit users or administrators: Press \wedge or \vee to select the user or the administrator, and then press OK.
- Delete users or administrators
 - ◊ Delete one by one:
 1. On the user list or the admin list screen, press \wedge or \vee to select the user or the administrator, and then press OK.
 2. Press \wedge to select , and then press OK.
 3. Press OK to delete the user.
 - ◊ Delete all the users: On the **Person Management** screen, select **Delete All Users**, press OK, and then press OK again to delete all the users, including the administrators.

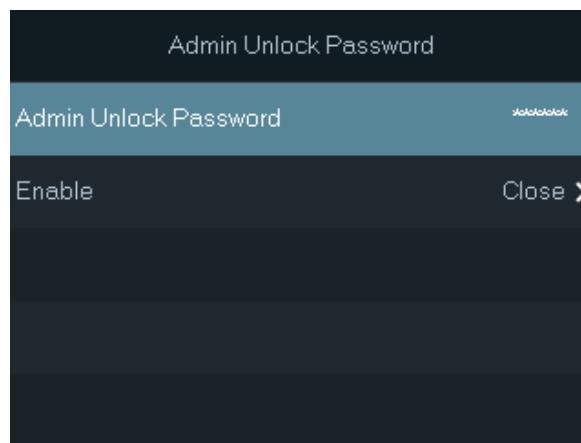
2.7.3 Configuring the Admin Unlock Password

You can unlock the door by only entering the admin password. This password is not limited by user types. Only one admin unlock password is allowed for one device.

Procedure

- Step 1 On the **Main Menu** screen, select **Users > Admin Unlock Password**.
- Step 2 Enter the password, and then press OK.

Figure 2-5 Admin unlock password

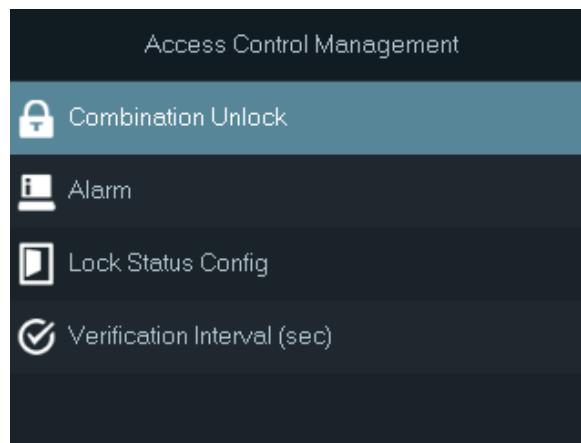


- Step 3 Select **Enable**, and then press OK to enable this function.

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 2-6 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 2-3 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.
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. <ul style="list-style-type: none"> ● 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.

Parameter	Description
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 the Door Status

Procedure

Step 1 On the **Main Menu** screen, select **Access Control > Lock Status Config**.

Step 2 Configure the parameters.

Figure 2-7 Lock status



Table 2-4 Parameters description

Parameter	Description
Door Status	<ul style="list-style-type: none"> ● NO : The door remains unlocked all the time. ● NC : The door remains locked all the time. ● Normal : If Normal is selected, the door will be locked and unlocked according to your settings.
Unlock Duration	After a person is granted access, the door will remain unlocked for a defined time for them to pass through.

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**.

2.9 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 2-5 Shift parameters description

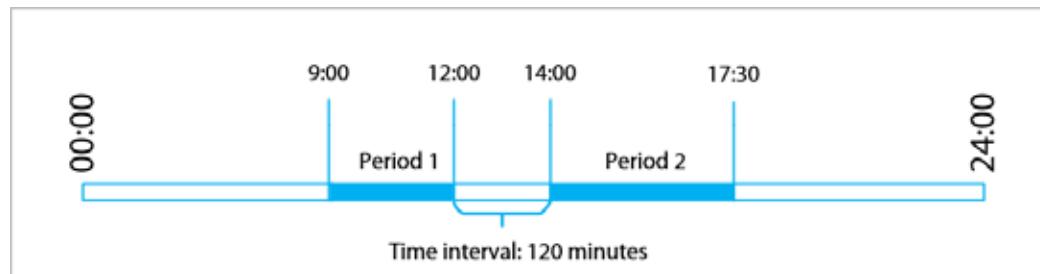
Parameter	Description
Shift Name	Enter the name of the shift.



Parameter	Description
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 2-8 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.

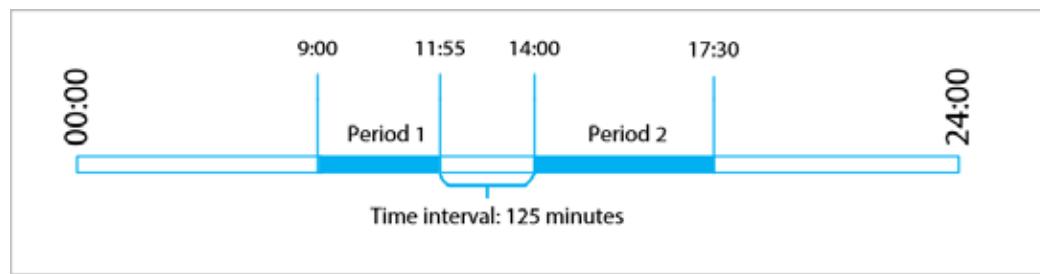


If a person clocks out multiple times during period 1, the latest time will be valid, and if they clock in multiple times during period 2, the earliest time will be valid.

- 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 2-9 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 2-6 Parameters description

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

Step 4 Press Esc to save the configurations.

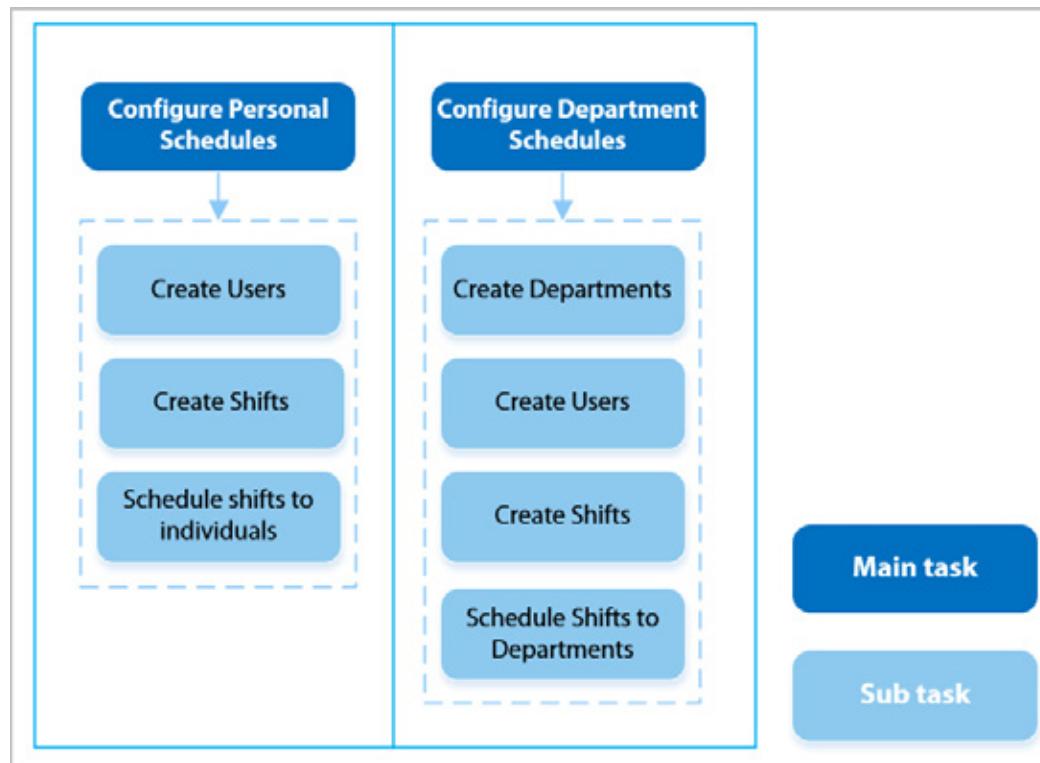
2.9.4 Configuring Work Schedules

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 2-10 Configuring work schedules



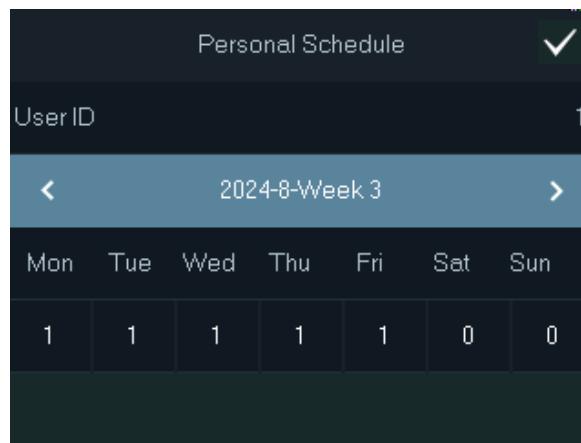
Procedure

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

Step 2 Set work schedules for individuals.

1. Select **Personal Schedule**.

Figure 2-11 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 Attendance Modes

Prerequisites

Make sure that you have enabled **Local Attendance** on the **Attendance** screen

Procedure

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

Step 2 Configure attendance mode.



Table 2-7 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.	<ul style="list-style-type: none"> 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.	<ul style="list-style-type: none"> Overtime check in: Clock in when your overtime period starts. Overtime check out: Clock out when your overtime period ends.
Manual Mode	<ul style="list-style-type: none"> 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. <p></p> <p>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.</p>	<ul style="list-style-type: none"> 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.
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.

2.10 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 2-12 IP settings

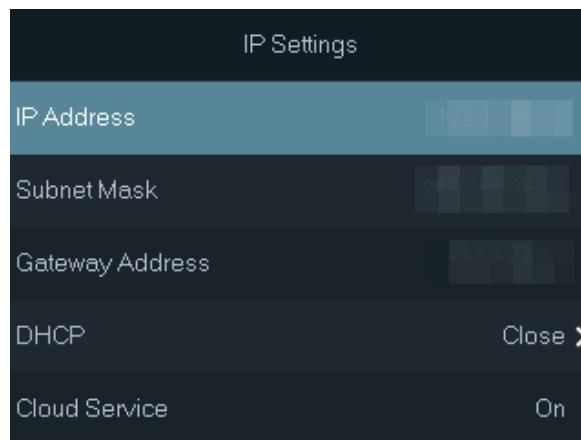


Table 2-8 IP configuration parameters

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**.

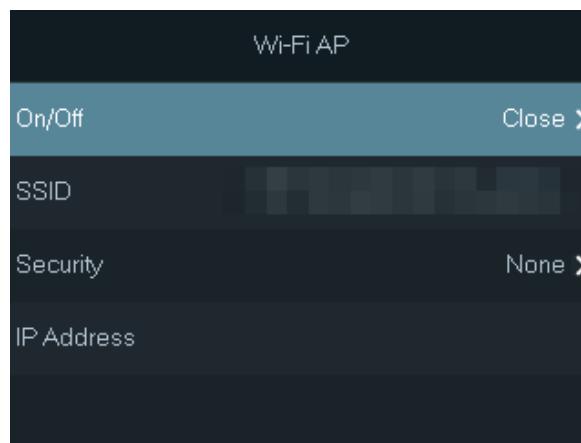
Step 2 Turn on Wi-Fi AP.

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 2-13 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 2-14 Time settings

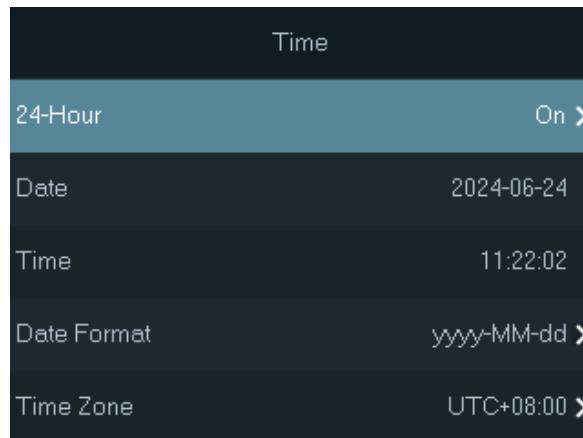


Table 2-9 Description of time parameters

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 2-10 Parameters description

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

Configure when the display should turn off and the logout time.

Procedure

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

Figure 2-15 Screen settings

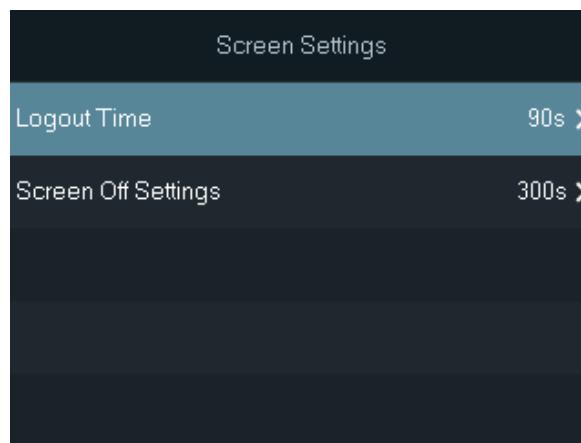


Table 2-11 Parameters description

Parameters	Description
Logout Time	Press OK to select the time. The system goes back to the standby screen after a defined time of inactivity. The value ranges from 15 seconds to 90 seconds.
Screen Off Settings	The system goes back to the standby screen and then the screen turns off after a defined time of inactivity. The value ranges from 30 seconds to 300 seconds.



Example

For example, if the logout time is set to 15 seconds, and the screen off time is set to 30 seconds, the system goes back to the standby screen after 15 seconds, and then the screen will turn off after another 15 seconds.



The logout time must be less than the screen off 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 2-12 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 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.

2.11.7 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 2-16 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

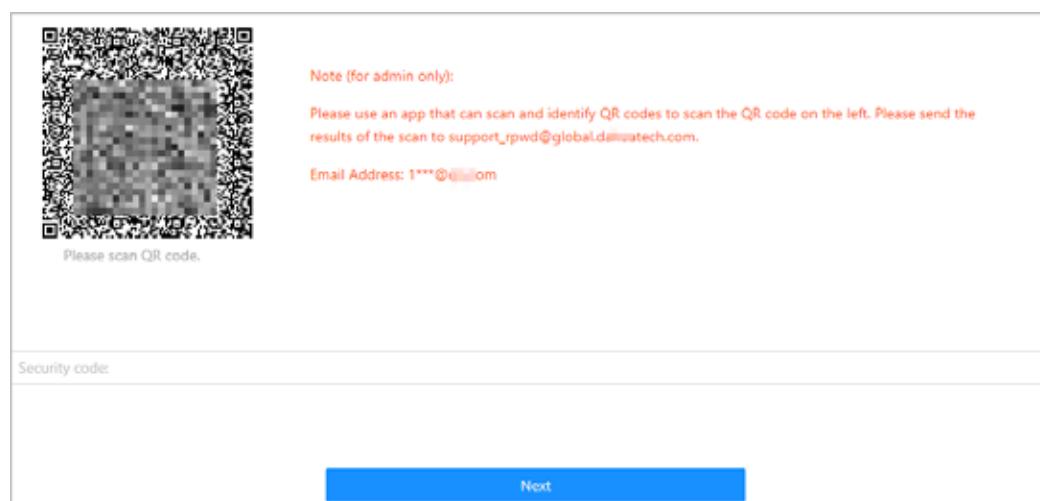
Step 1 On the login page, click **Forgot password**.

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



- 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

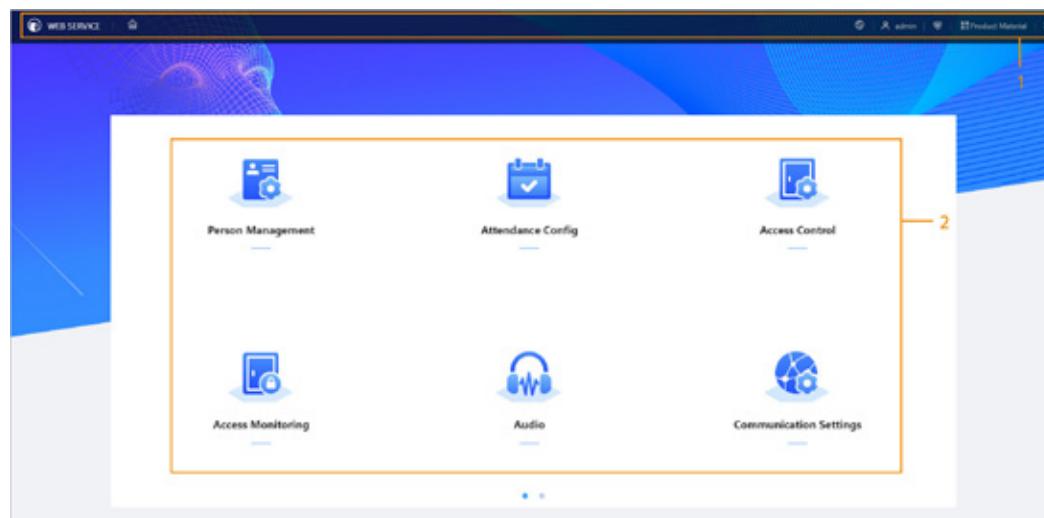


Table 3-1 Home page description

No.	Description
1	<ul style="list-style-type: none"> ● 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 Person Management

Procedure

- Step 1 On the home page, select **Person Management**, and then click **Add**.
Step 2 Configure user information.

Figure 3-3 Add users

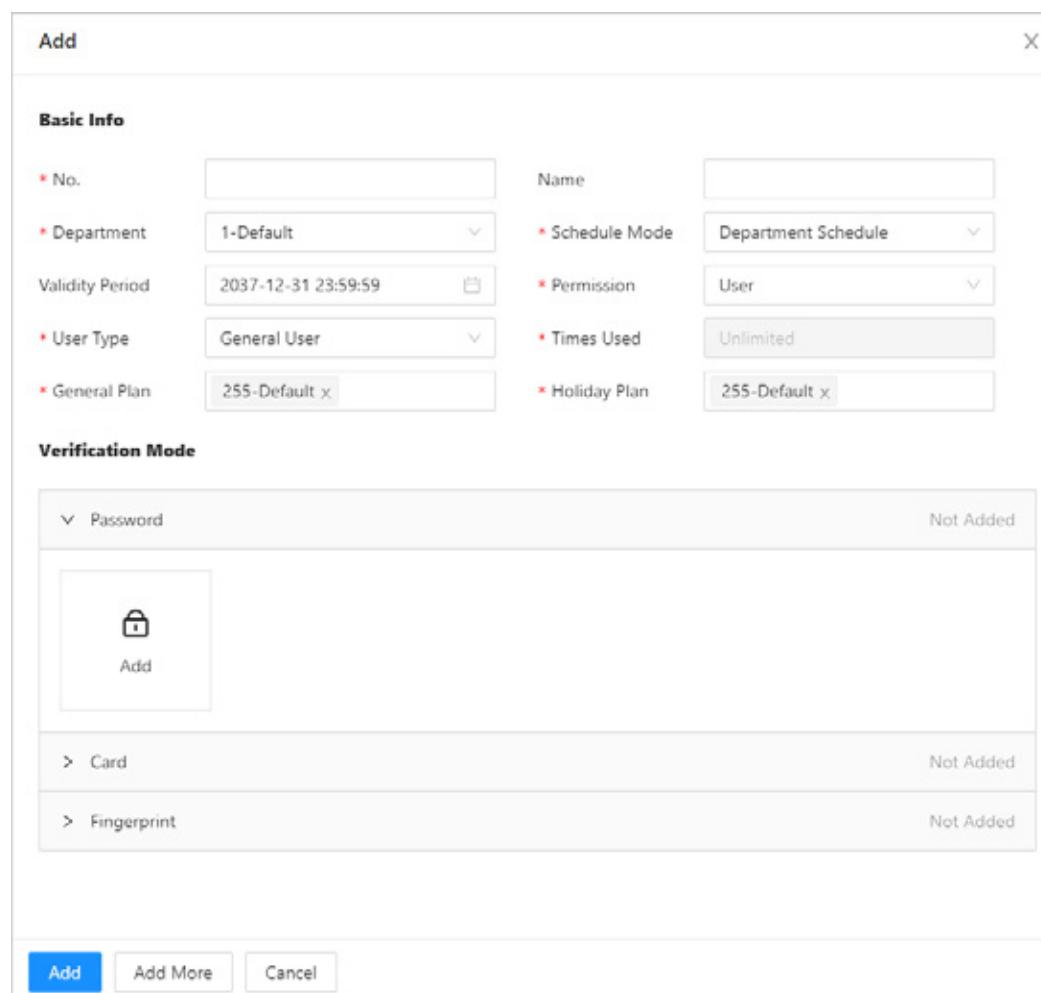


Table 3-2 Parameters description

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).
Department	Add users to a department. If a department schedule is assigned to the person, they will follow the established department schedule. <ul style="list-style-type: none"> ● Department Schedule: Assign department schedule to the user. ● Personal Schedule: Assign personal schedule to the user.
Schedule Mode	 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.

Parameter	Description
Validity Period	Set a date on which the door access and attendance permissions of the person will be expired.
Permission	<ul style="list-style-type: none"> ● User : Users only have door access or time attendance permissions. ● Admin : Administrators can configure the Device besides door access and attendance permissions.
User Type	<ul style="list-style-type: none"> ● 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	<p>People can unlock the door or take attendance during the defined period.</p>  <p>You can select more than one plan.</p>
Holiday Plan	<p>People can unlock the door or take attendance during the defined holiday.</p>  <p>You can select more than one holiday.</p>
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	<ul style="list-style-type: none"> 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. <p>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.</p> <ul style="list-style-type: none"> Click Add. <p>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.</p> <p>You can enable the Duress Card function. An alarm will be triggered if a duress card is used to unlock the door.</p> <ul style="list-style-type: none"> Set duress card. Change card number. <p></p> <p>One user can only set one duress card.</p>
Fingerprint	<p>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.</p> <p>Enroll fingerprints through an enrollment reader or the Device.</p> <ul style="list-style-type: none"> 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. <p></p> <ul style="list-style-type: none"> 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.

3.5 Configuring Attendance

3.5.1 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 3-4 Create departments

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.

3.5.2 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 Select **Attendance Config > Shift Config**.

Step 2 Click  to configure the shift.



Figure 3-5 Create shifts

Edit Shift

X

* Shift No.	1
* Shift Name	Default
* Period 1	08:00 → 17:00 (Clock icon)
* Period 2	00:00 → 00:00 (Clock icon)
* Overtime Period	00:00 → 00:00 (Clock icon)
* Limit for Arriving Late	3 min (0-99)
* Limit for Leaving Early	5 min (0-99)

Table 3-3 Shift parameters description

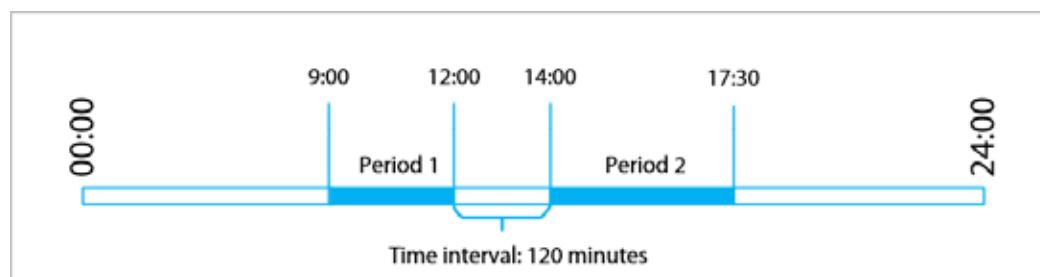
Parameter	Description
Shift Name	Enter the name of the shift.
Period 1	Specify a time range when people can clock in and clock out for the workday. If you only set one attendance period, employees need to clock in and out by the designated times to avoid an anomaly appearing on their attendance record. For example, if you set 08:00 to 17:00, employees must clock in by 08:00 and clock out from 17:00 onwards.
Period 2	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.



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 3-6 Time interval (even number)



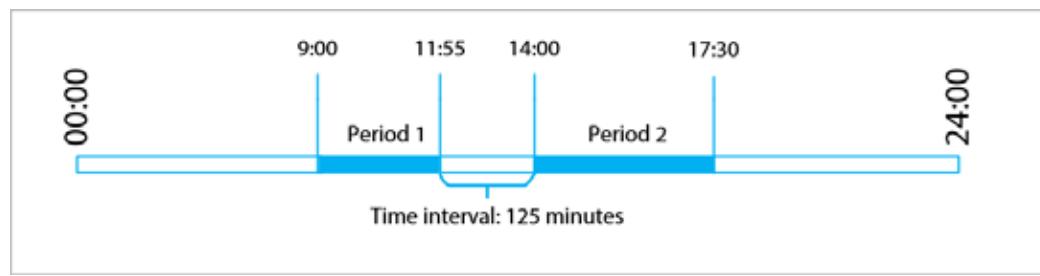
For example: If the interval is 120 minutes, then the clock-out time for period 1 is from 12:00 to 12:59, and the clock-in time for period 2 is from 13:00 to 14:00.



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 3-7 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.

3.5.3 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 3-8 Create holiday plans

The screenshot shows a modal dialog titled "Add Attendance Holiday". It contains three input fields: "Attendance Holiday No." with value "1", "Attendance Holiday" with value "Attendance Holiday for October", and "Time" with start date "2024-10-01" and end date "2024-10-07". At the bottom are "OK" and "Cancel" buttons.

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**.



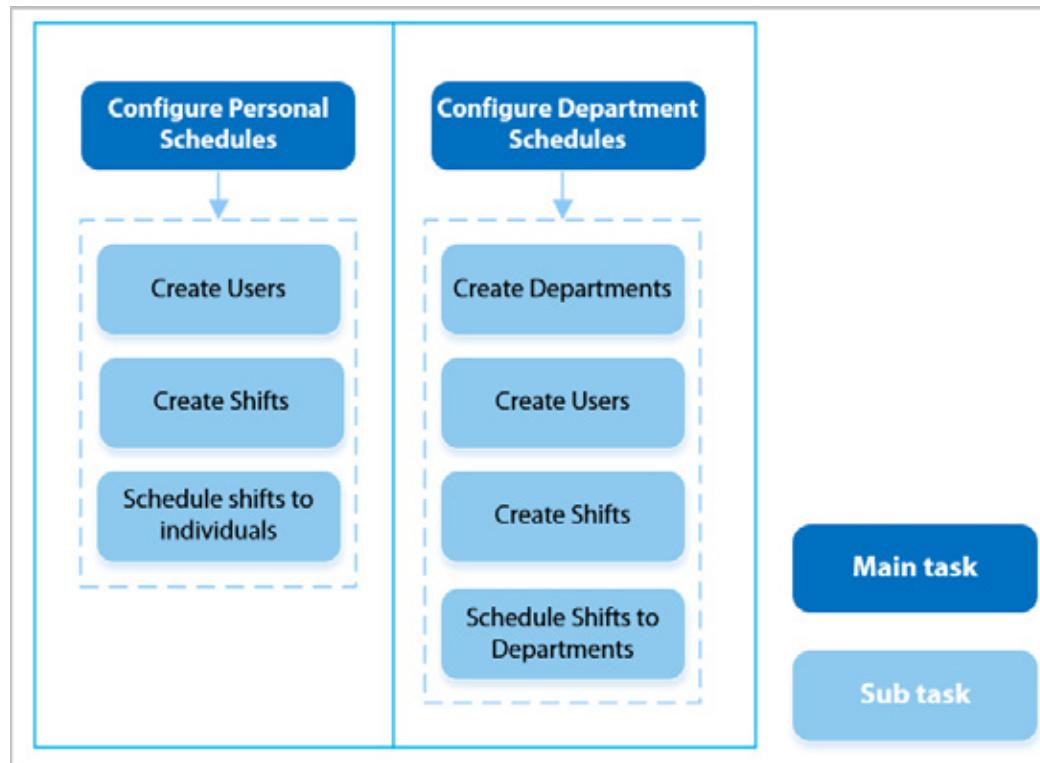
3.5.4 Configuring Work Schedules

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 3-9 Configuring work schedules



Procedure

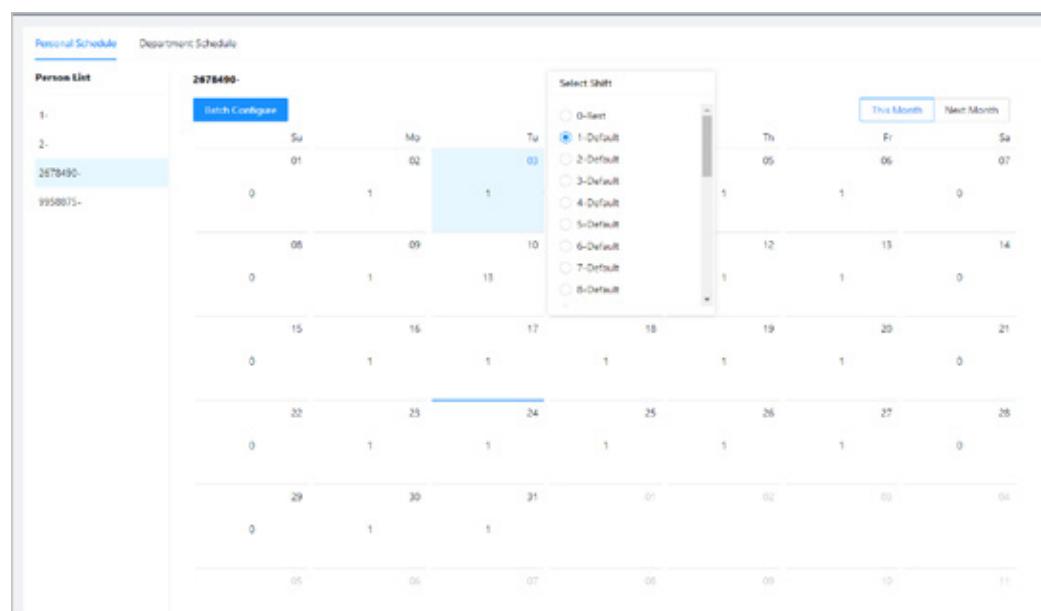
Step 1 Select **Attendance Config > Schedule Config**.

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 3-10 Personal schedule



You can only set work schedules for the current month and the next month.

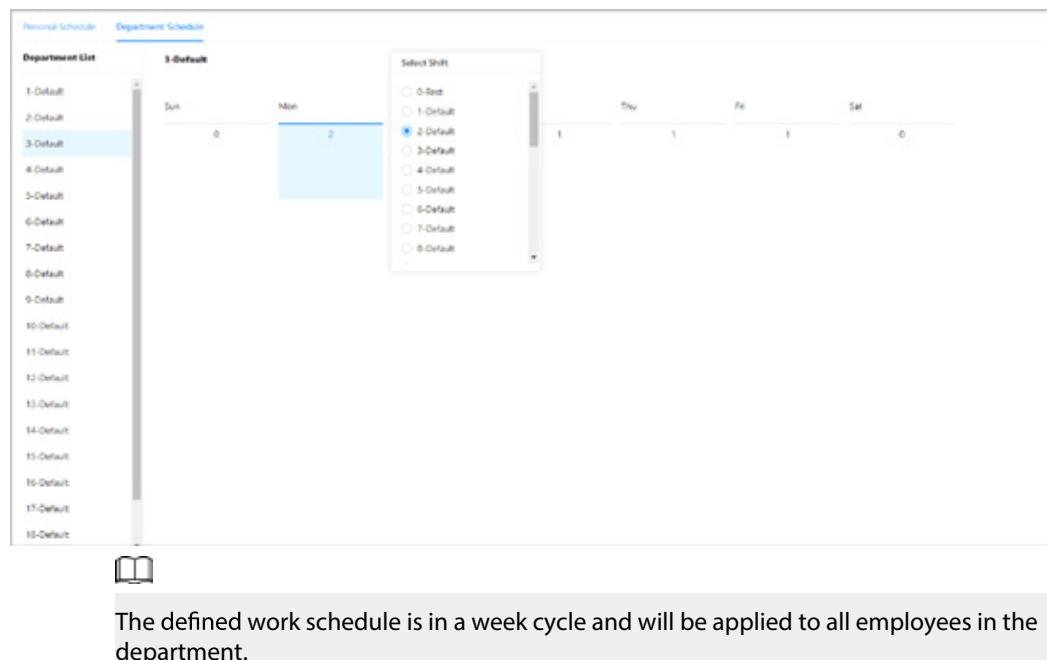
- 0 indicates break.
- 1 to 24 indicates the number of the per-defined shifts.
- 25 indicates business trip.
- 26 indicates leave of absence.

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 3-11 Schedule shifts to a department

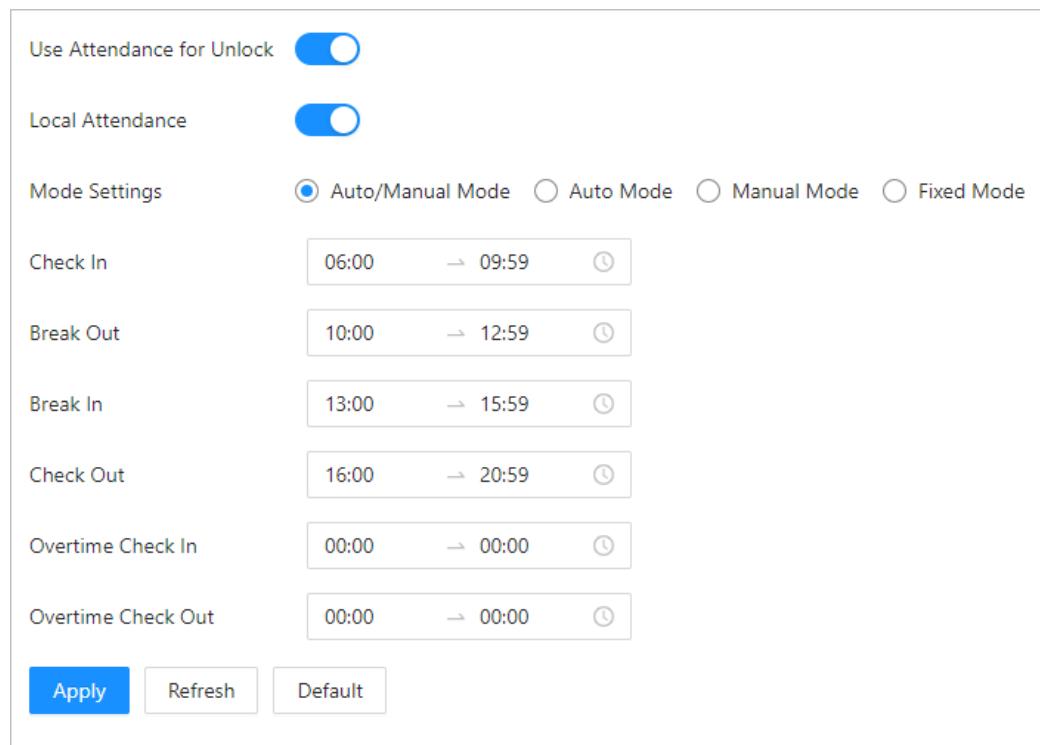


3.5.5 Configuring Attendance Mode

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 3-12 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	

Buttons:

- 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.	<ul style="list-style-type: none"> 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.	<ul style="list-style-type: none"> 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.



Parameter	Description	Attendance Mode
Manual Mode	<ul style="list-style-type: none"> 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. <p></p> <p>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.</p>	
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.

3.6 Configuring Access Control

3.6.1 Configuring Access Control Parameters

3.6.1.1 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 3-13 Basic parameters

Table 3-6 Basic parameters description

Parameter	Description
Name	The name of the door.



Parameter	Description
Door Status	<p>Set the door status.</p> <ul style="list-style-type: none"> 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	<p>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 "3.6.5 Configuring Periods".</p>
Normally Closed Period	<p></p> <ul style="list-style-type: none"> 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.
Verification Interval	<p>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.</p>
Admin Unlock Password	<p>You can configure one administrator password for opening the door. The password must contain 1 to 8 numbers.</p>

Step 3 Click **Apply**.

3.6.1.2 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

- Select **Combination Unlock** from the **Unlock Method** list.
- 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.
- Select unlock methods, and then configure other parameters.



Figure 3-14 Unlock settings

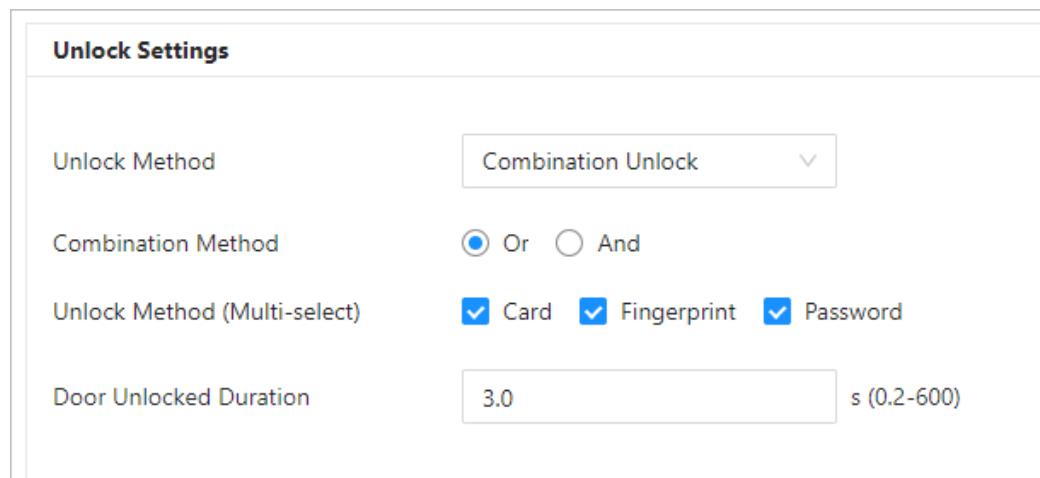


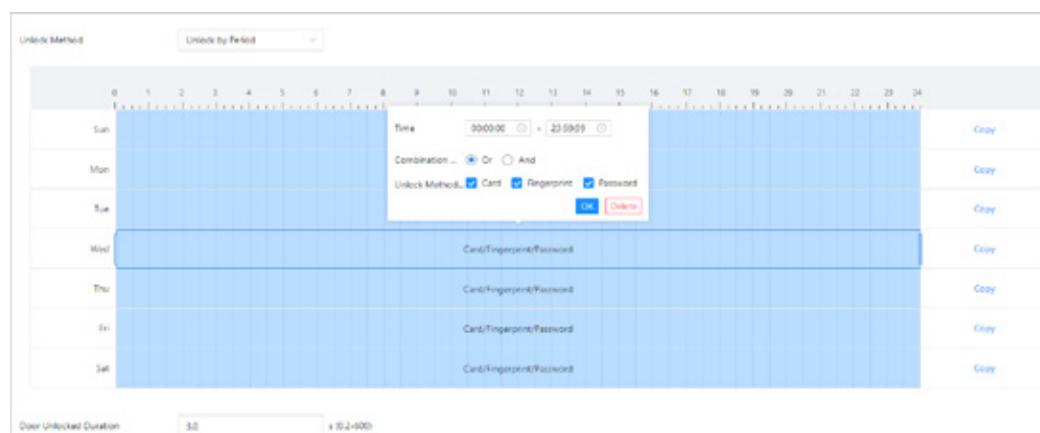
Table 3-7 Unlock settings description

Parameter	Description
Unlock Method (Multi-select)	Unlock methods might differ depending on the models of product.
Door Unlock Duration	After a person is granted access, the door will remain unlocked for a defined time for them 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 3-15 Unlock by period



- **Unlock by multiple users.**

1. In the **Unlock Method** list, select **Unlock by multiple users**.
2. Click **Add** to add groups.
3. Select unlock method, valid number and users.



The valid number indicates the number of people who need to verify their identities on the Device before the door unlocks.

Step 3 Click **Apply**.

3.6.2 Configuring Alarms

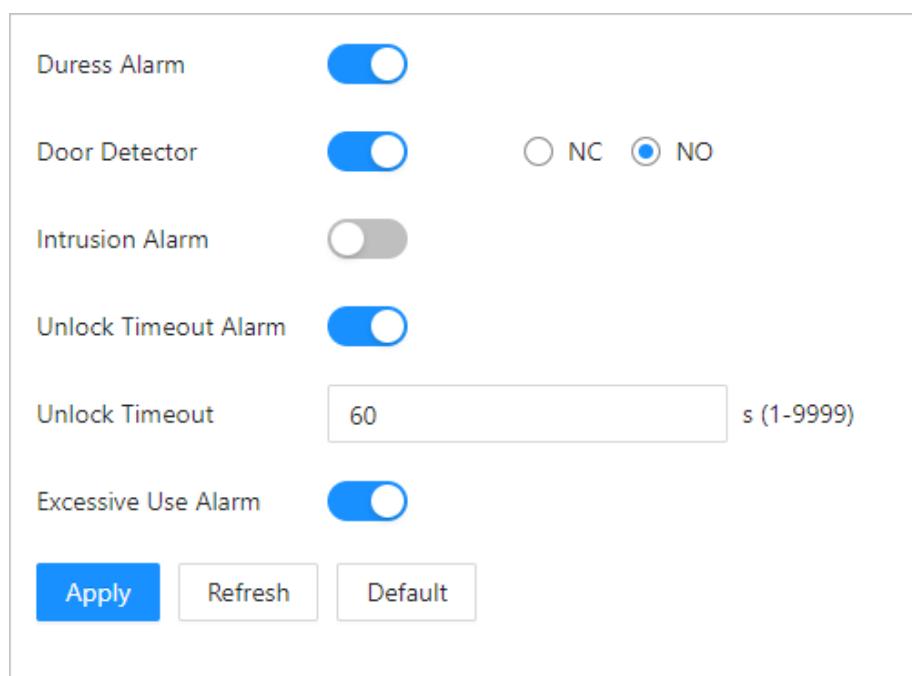
An alarm will be triggered when an abnormal access event occurs.

Procedure

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

Step 2 Configure alarm parameters.

Figure 3-16 Alarm



Duress Alarm

Door Detector NC NO

Intrusion Alarm

Unlock Timeout Alarm

Unlock Timeout 60 s (1-9999)

Excessive Use Alarm

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.

Parameter	Description
Door Detector	<p>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.</p> <ul style="list-style-type: none"> ● 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	<p>If the door is opened abnormally, an intrusion alarm will be triggered and last for a defined time.</p>  <p>The door detector and intrusion need to be enabled at the same time.</p>
Unlock Timeout Alarm	<p>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.</p> 
Unlock Timeout	<p>The door detector and door timed out function need to be enabled at the same time.</p> 
Excessive Use Alarm	<p>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.</p>

Step 3 Click **Apply**.

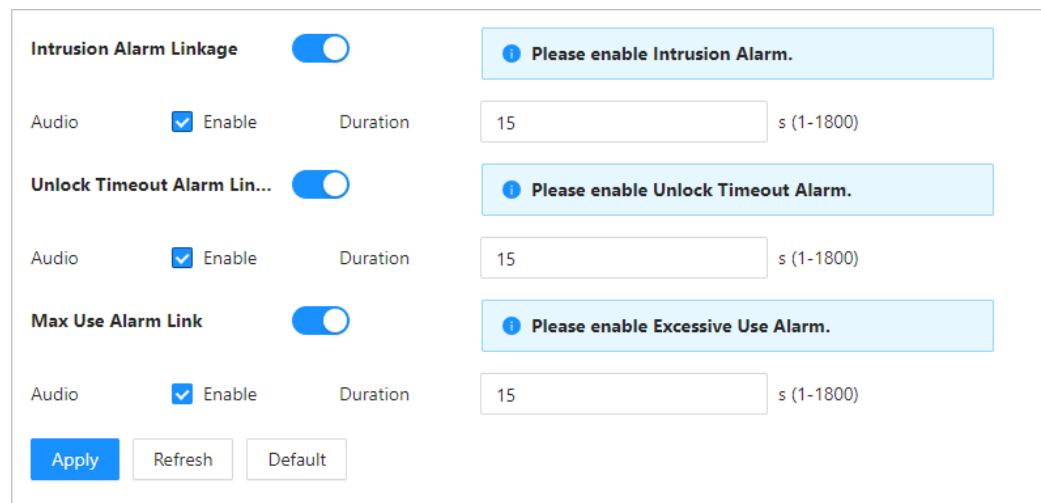
3.6.3 Configuring Alarm Event Linkage

Procedure

- Step 1 On the **Main Menu**, select **Access Control > Alarm > Alarm Event Linkage**.
- Step 2 Configure alarm event linkages.



Figure 3-17 Alarm event linkage



Intrusion Alarm Linkage Please enable Intrusion Alarm.

Audio Enable Duration 15 s (1-1800)

Unlock Timeout Alarm Linkage Please enable Unlock Timeout Alarm.

Audio Enable Duration 15 s (1-1800)

Max Use Alarm Linkage Please enable Excessive Use Alarm.

Audio Enable Duration 15 s (1-1800)

Buttons: Apply, Refresh, Default

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.
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**.

3.6.4 Configuring Card Settings

Background Information



This function is only available on select models.

Procedure

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



Figure 3-18 Card parameters

Card Settings

IC Card

IC Card Encryption & Verification

Block NFC Cards

Apply Refresh Default

Card No. System

After the number system is changed, the card numbers will become invalid.

Card No. System Hexadecimal Decimal

Apply Refresh Default

Table 3-10 Card parameters description

Parameter	Description	
Card Settings	IC Card	<p>The IC card can be read when this function is enabled.</p>  <p>This function is only available on select models.</p>
	IC Card Encryption & Verification	<p>The encrypted card can be read when this function is enabled.</p>  <p>Make sure IC Card is enabled.</p>

Parameter	Description
	<p>Block NFC Cards</p> <p>Prevent unlocking through duplicated NFC card after this function is enabled.</p>  <ul style="list-style-type: none"> • This function is only available on models that support IC cards. • Make sure IC Card is enabled. • NFC function is only available on select models of phones.
Card No. System	<p>Card No. System</p> <p>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.</p>

Step 4 Click **Apply**.

3.6.5 Configuring Periods

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

3.6.5.1 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.

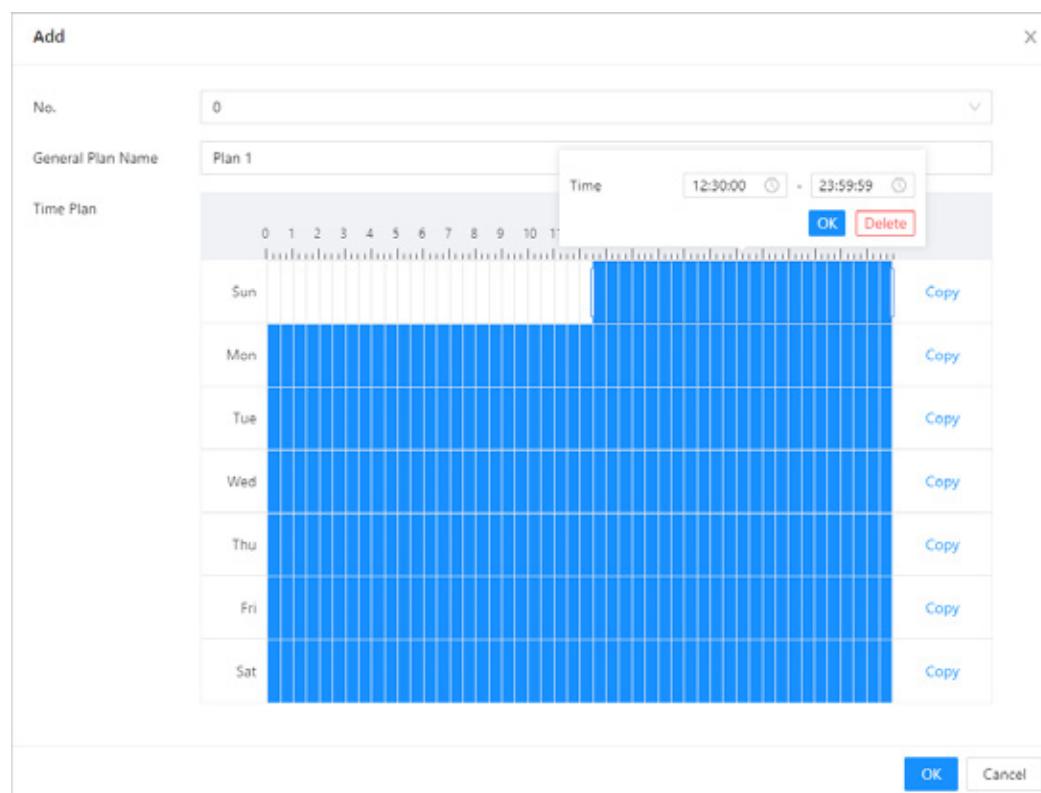
Step 2 Select **Access Control > Period Config > General Plan**.

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 3-19 Configure general plan



Step 4 Click **OK**.

3.6.5.2 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

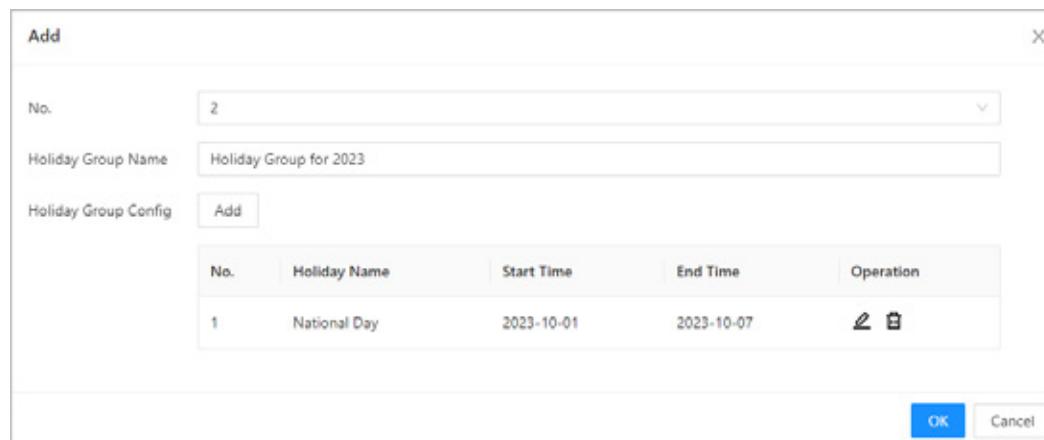
Step 1 Log in to the webpage.

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 3-20 Add a holiday group



No. 2

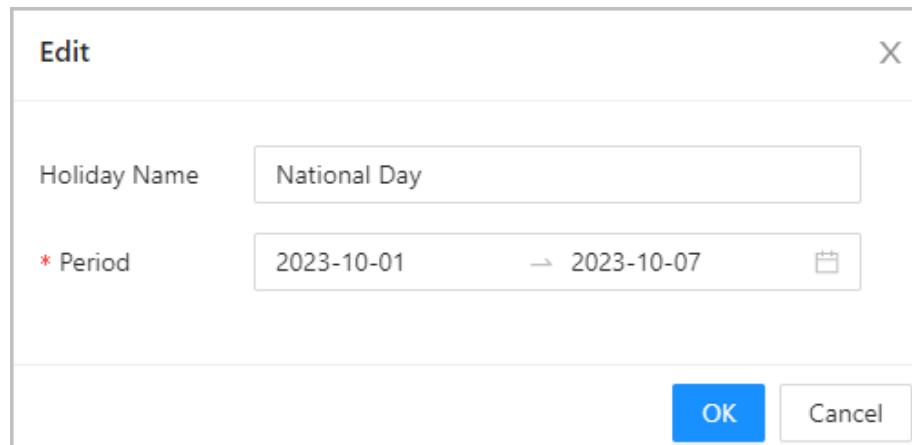
Holiday Group Name: Holiday Group for 2023

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

OK Cancel

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

Figure 3-21 Add a holiday to a holiday group



Holiday Name: National Day

* Period: 2023-10-01 → 2023-10-07

OK Cancel

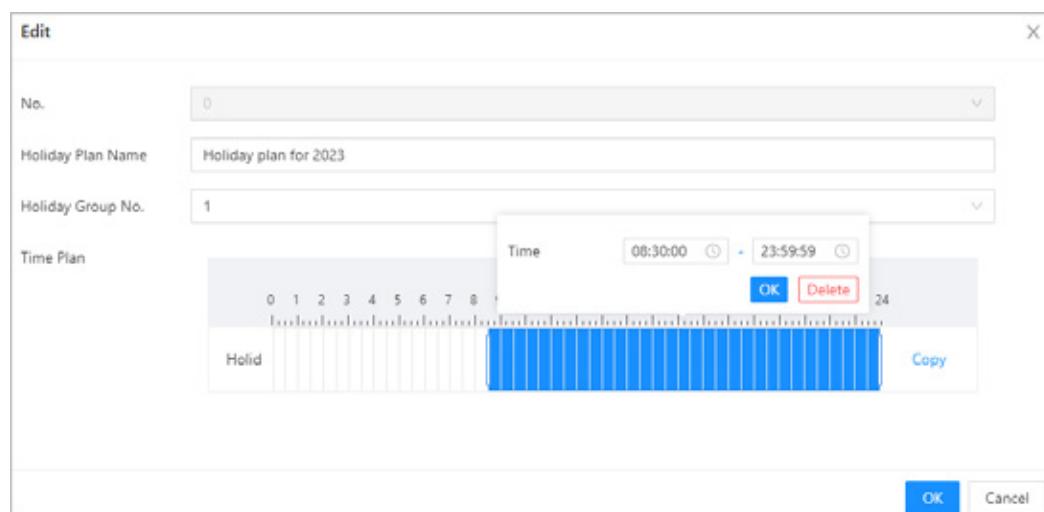
Step 4 Click **OK**.

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

- Select a number for the holiday plan, and then enter a name for it.
- 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 3-22 Add holiday plan



Step 6 Click **OK**.

3.7 Access Monitoring

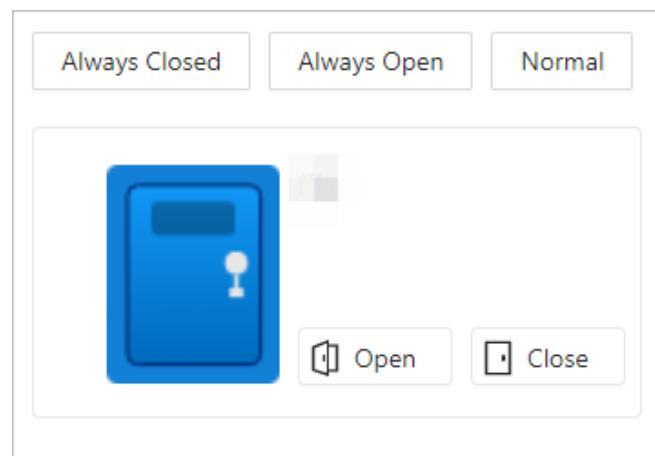
Log in to the webpage, select **Access Monitoring**, and all the connected doors are displayed.

Operations to control the door

- Click **Open** or **Close** to remotely control the door.
- Click **Always Open** or **Always Closed** to remotely control the door.

The door will remain open or closed all the time. You can click **Normal** to restore access control to its normal status, and the door will be open or closed based on the configured verification methods.

Figure 3-23 Operations to control the door



Event information

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

Figure 3-24 Event information

Event Info		<input checked="" type="checkbox"/> Select All	<input checked="" type="checkbox"/> Alarm	<input checked="" type="checkbox"/> Abnormal	<input checked="" type="checkbox"/> Normal	
Time	Camera Name	Event Info			Description	
2024-07-30 00:32:00	Door1					Unlock Timeout Alarm
2024-07-30 00:32:00	Door1					Unlock Timeout Alarm

Details

The details of the Device is displayed. You can view the IP address, device type and the device model here.

3.8 Configuring Audio

Set the speaker volume and audio prompts during identity verification.

Procedure

- Step 1 Log in to the webpage.
- Step 2 Select **Audio**.
- Step 3 Configure the audio parameters.

Figure 3-25 Configure audio parameters

Speaker Volume	30	(0-100)	
Key Sound			
Only supports MP3 files that are less than 20 KB with a sampling rate of 16K.			
Audio File	Audio Type	Audio File	Modify
Successfully verified.			
Failed to verify.			
Apply	Refresh	Default	

Table 3-11 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.



Parameters	Description
Audio File	<p>Click  to upload audio files to platform for each audio type.</p> <p></p> <p>Only supports MP3 files that are less than 20 KB with a sampling rate of 16K.</p>

Step 4 Click **Apply**.

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 3-26 TCP/IP

NIC: NIC 1

Mode: DHCP Static

MAC Address:

IP Version: IPv4

IP Address:

Subnet Mask:

Default Gateway:

Preferred DNS:

Alternate DNS:

MTU: 1500

Apply **Refresh** **Default**

Table 3-12 Description of TCP/IP

Parameter	Description
Mode	<ul style="list-style-type: none"> 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.

Parameter	Description
IP Address	If you set the mode to Static , configure the IP address, subnet mask and gateway.
Subnet Mask	
Default Gateway	<p></p> <ul style="list-style-type: none"> • 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	<p>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:</p> <ul style="list-style-type: none"> • 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 3-27 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 3-28 Wi-Fi AP



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.

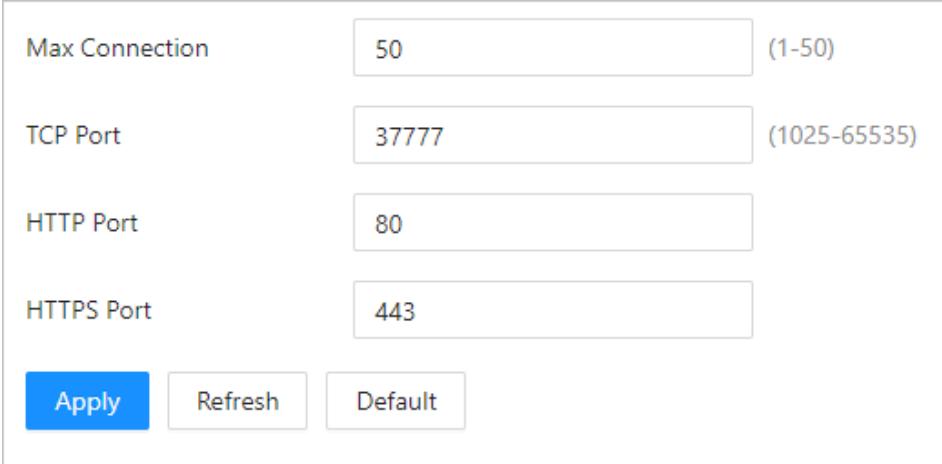
3.9.4 Configuring Port

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 3-29 Configure ports



Max Connection	50	(1-50)
TCP Port	37777	(1025-65535)
HTTP Port	80	
HTTPS Port	443	
<input type="button" value="Apply"/> <input type="button" value="Refresh"/> <input type="button" value="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 3-30 Basic service

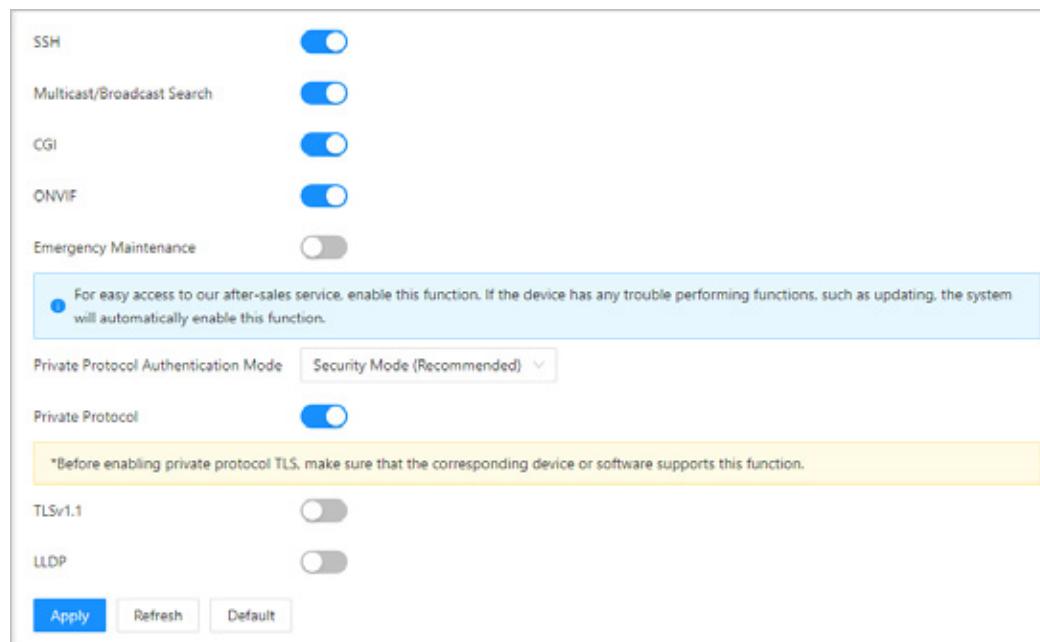


Table 3-14 Basic service parameter description

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	<p>Set the authentication mode, including safe mode and compatibility mode. It is recommended to choose Security Mode.</p> <ul style="list-style-type: none"> ● 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	<p>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.</p> <p></p> <p>Security risks might present when TLSv1.1 is enabled. Please be advised.</p>
LLDP	<p>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.</p>

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

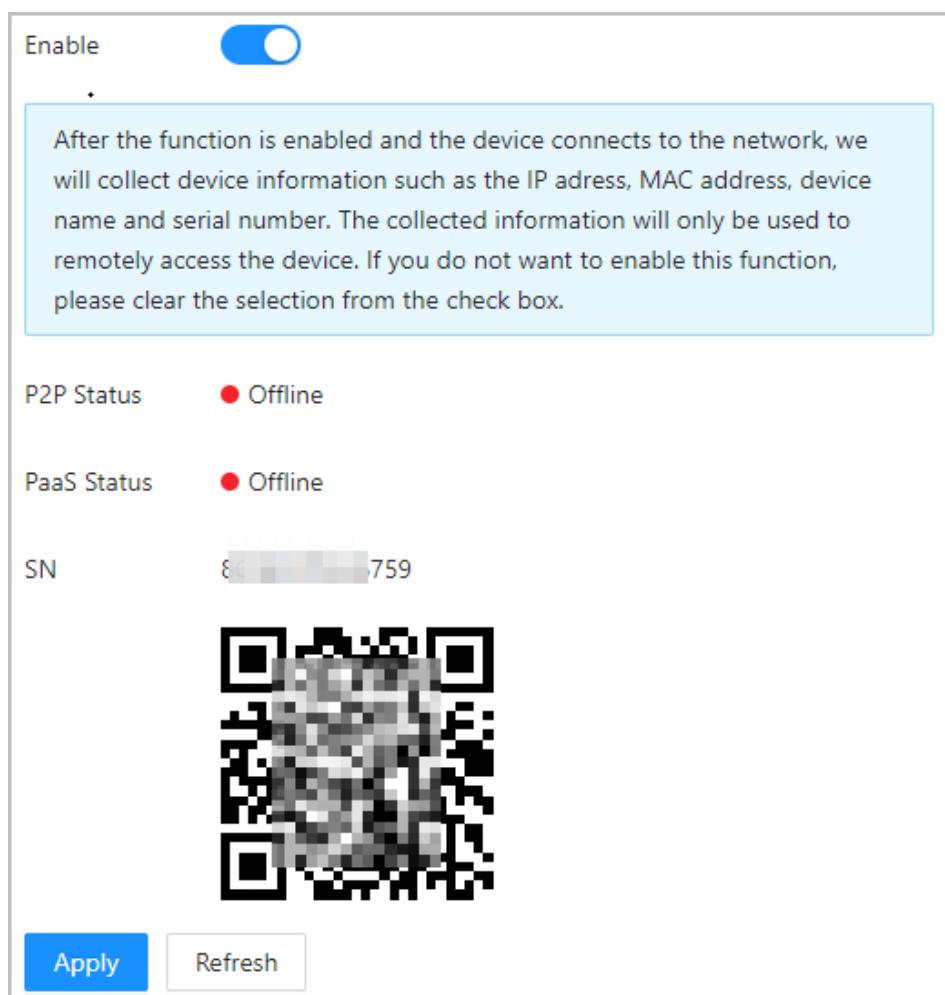
Step 1 On the home page, select **Communication Settings > Network Setting > Cloud Service**.

Step 2 Turn on the cloud service function.

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



Figure 3-31 Cloud service



Step 3 Click **Apply**.

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

3.9.7 Configuring 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 > Auto Registration**.

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

Figure 3-32 Auto Registration

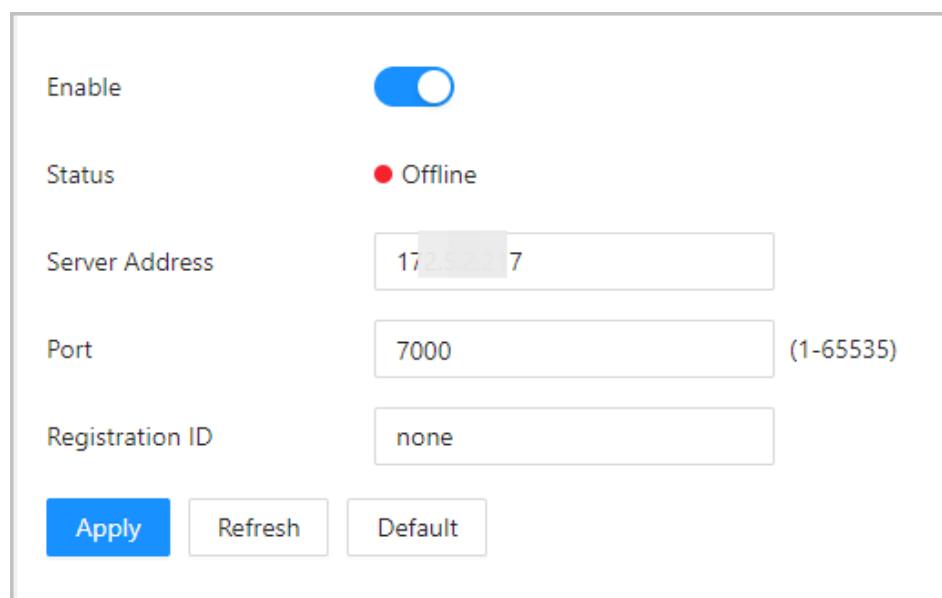


Table 3-15 Automatic registration description

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	<ul style="list-style-type: none"> ● Host IP: Enter the IP address of the third-party platform.
Domain Name	<ul style="list-style-type: none"> ● Domain Name: Enter the domain name of the third-party platform.
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 3-33 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	<p>Select the type of event that will be pushed to the management platform.</p> <p></p> <ul style="list-style-type: none"> • 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.

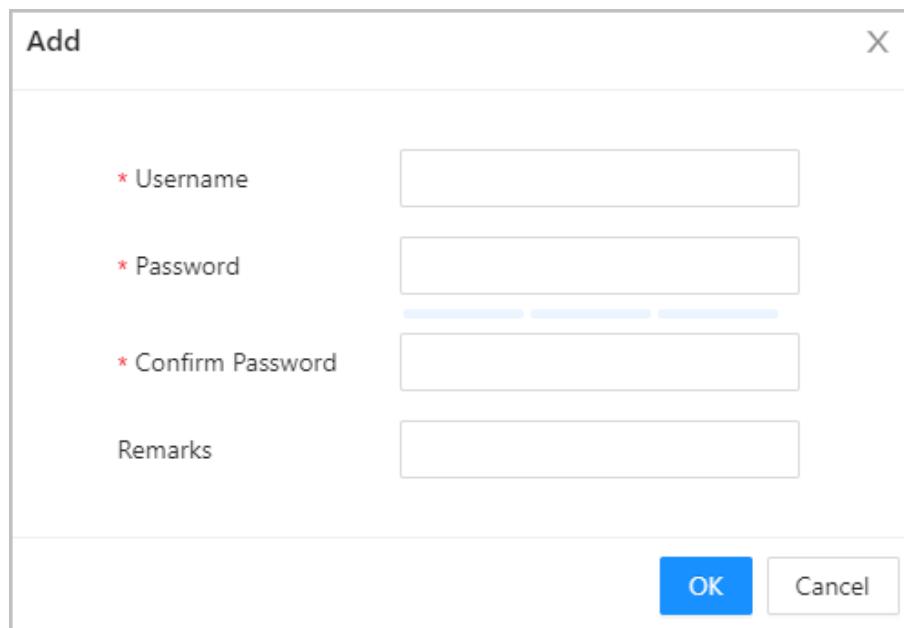


- The username cannot be the same with existing account. The username consists of up to 31 characters and only allows for numbers, letters, underscores, midlines, dots, or @.
- The password must consist of 8 to 32 non-blank characters and contain at least two types of the following characters: Upper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

Set a high-security password by following the password strength prompt.



Figure 3-34 Add administrators



The screenshot shows a modal dialog box titled "Add". It contains four input fields: "Username" (marked with a red asterisk), "Password" (marked with a red asterisk), "Confirm Password" (marked with a red asterisk), and "Remarks". Below the fields are two buttons: "OK" (blue) and "Cancel".

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 manufacturers. ONVIF users have their identities verified through ONVIF protocol. The default ONVIF user is admin.

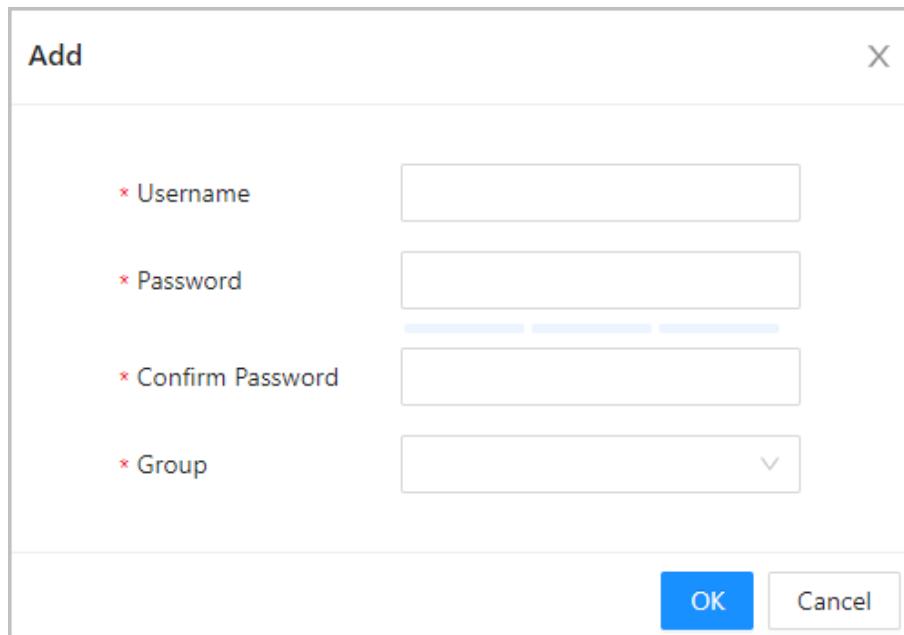
Procedure

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

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



Figure 3-35 Add ONVIF user



The screenshot shows a modal dialog box titled 'Add'. It has four input fields with validation stars: 'Username', 'Password', 'Confirm Password', and 'Group'. Below the 'Group' field is a dropdown arrow. At the bottom right are 'OK' and 'Cancel' buttons.

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	<p>There three permission groups which represents different permission levels.</p> <ul style="list-style-type: none"> ● 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 3-36 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 3-37 Date settings

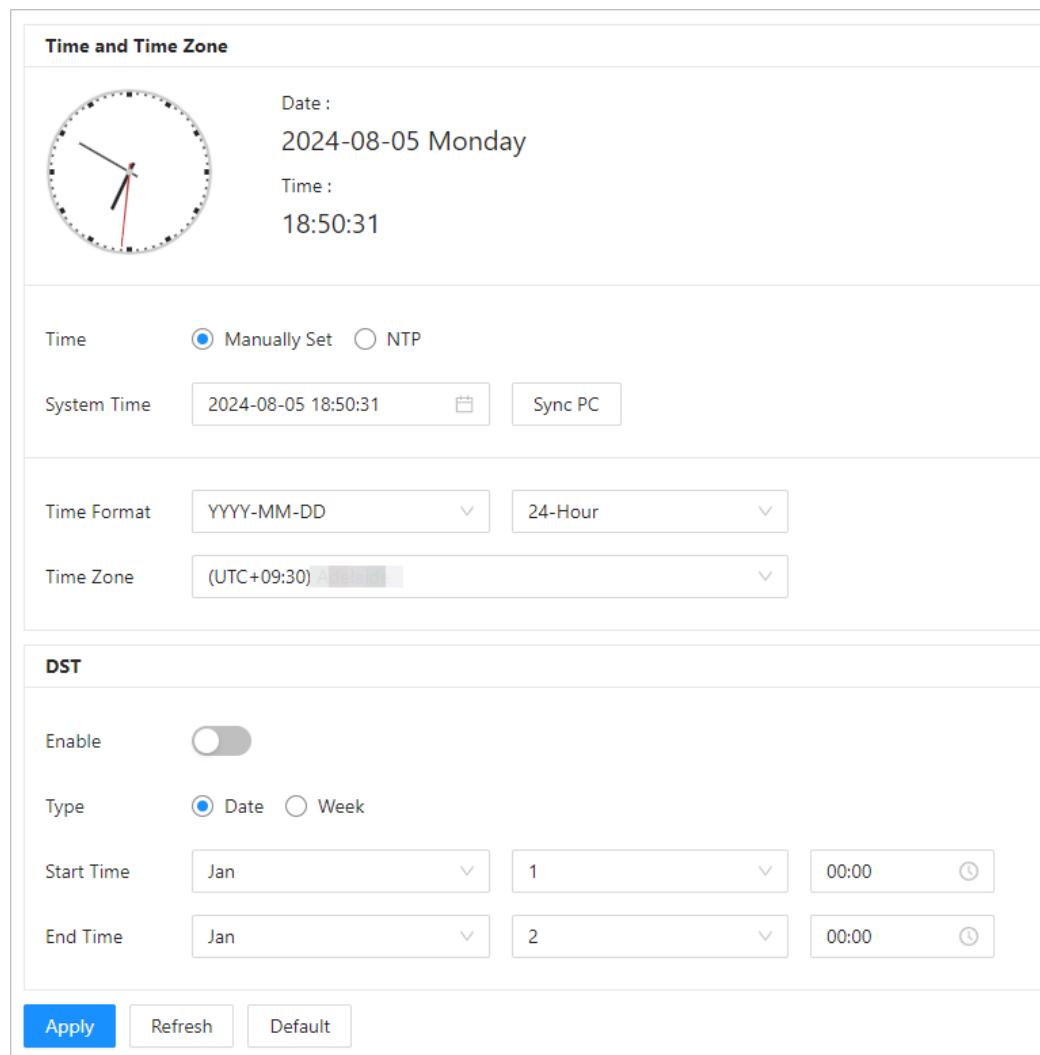


Table 3-19 Time settings description

Parameter	Description
Time	<ul style="list-style-type: none"> ● 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. <ul style="list-style-type: none"> ◊ 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.

3.11 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 3-38 One-click diagnosis



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 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**.

3.11.4.4 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.

3.11.4.5 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

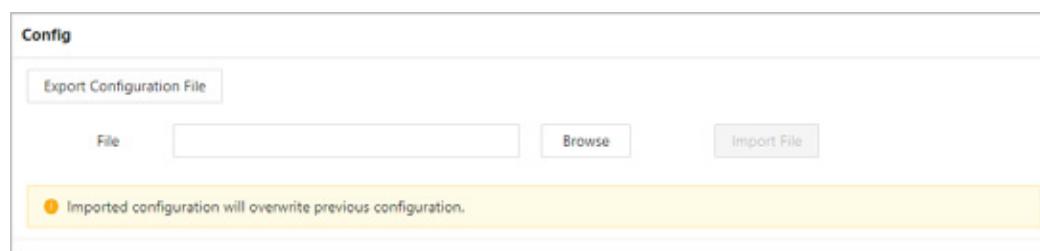
You can import and export the configuration file for the Device. When you want to apply the same configurations to multiple devices, you can import the configuration file to them.

Procedure

Step 1 Log in to the webpage.

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

Figure 3-39 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.

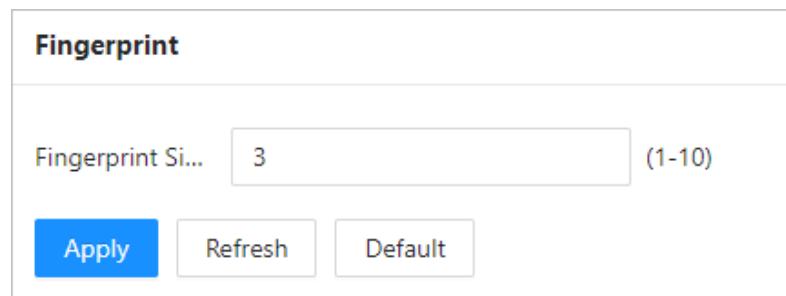
Step 2 Select **Maintenance Center > Maintenance Management > Config.**

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 3-40 Fingerprint similarity threshold



Fingerprint		
Fingerprint Si...	3	(1-10)
Apply	Refresh	Default

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 3-41 Packet Capture

Packet Capture						
NIC	Device Address	IP 1: Port 1		IP 2: Port 2		Packet Sniffer Size
eth0	192.168.1.166	Optional	[Optional]	Optional	[Optional]	500KB
eth1	192.168.1.101	Optional	[Optional]	Optional	[Optional]	500KB



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

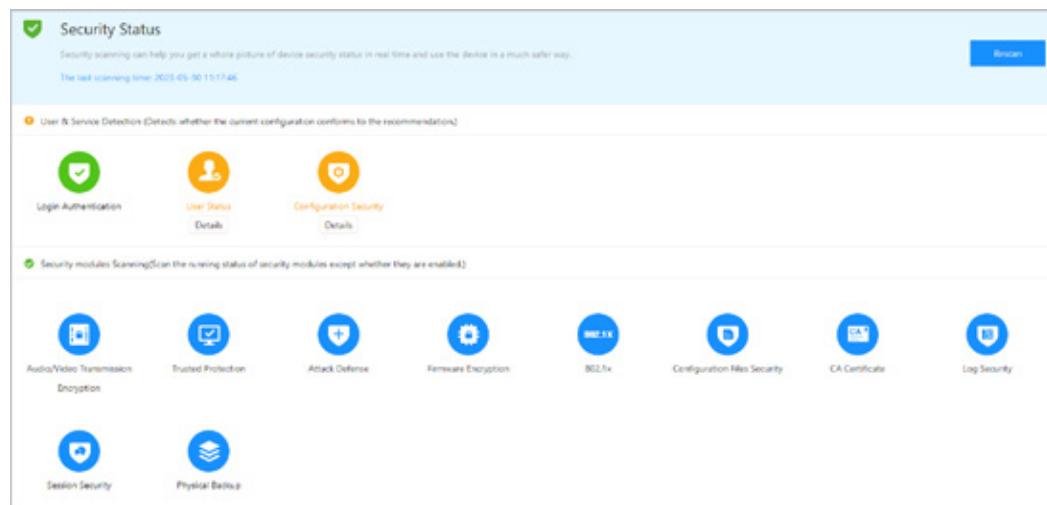
Step 1 Select  > **Security Status**.

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 3-42 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.



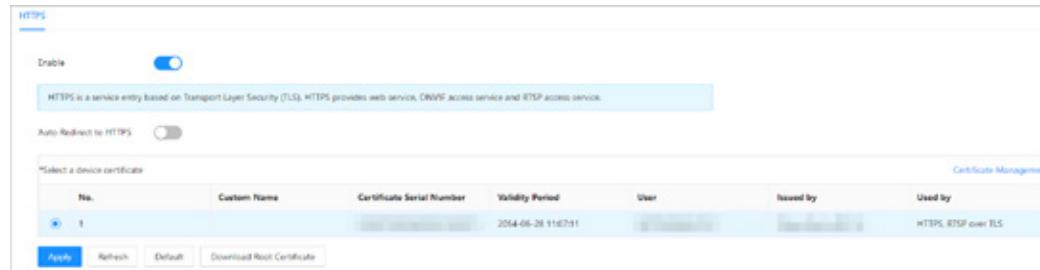
If you turn on the compatible with TLS v1.1 and earlier versions, security risks might occur. Please be advised.

Step 3 Select the certificate.



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

Figure 3-43 System service



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.

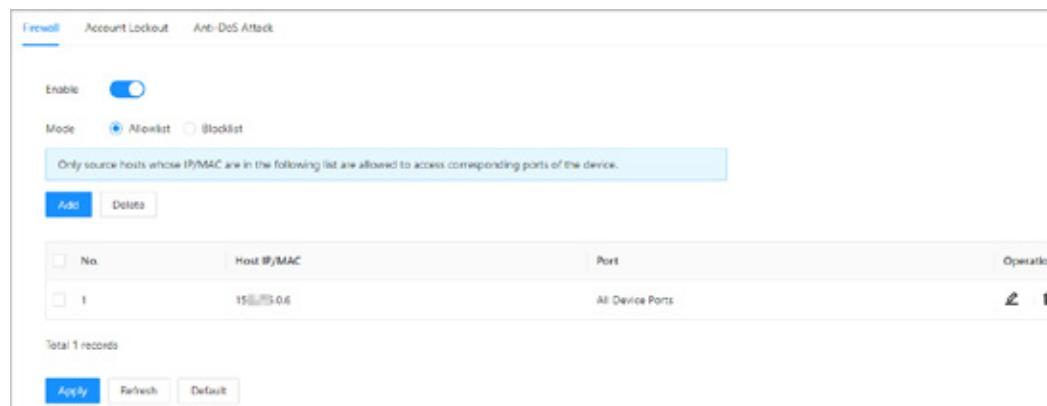
Procedure

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

Step 2 Click  to enable the firewall function.



Figure 3-44 Firewall



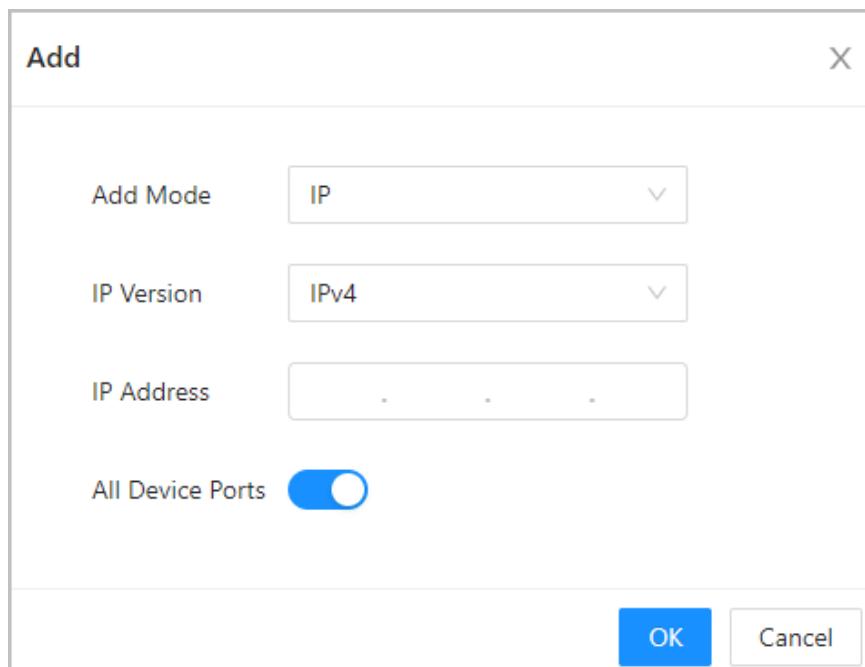
No.	Host IP/MAC	Port	Operations
1	192.168.3.0/24	All Device Ports	

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 3-45 Add IP information



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 3-46 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**.

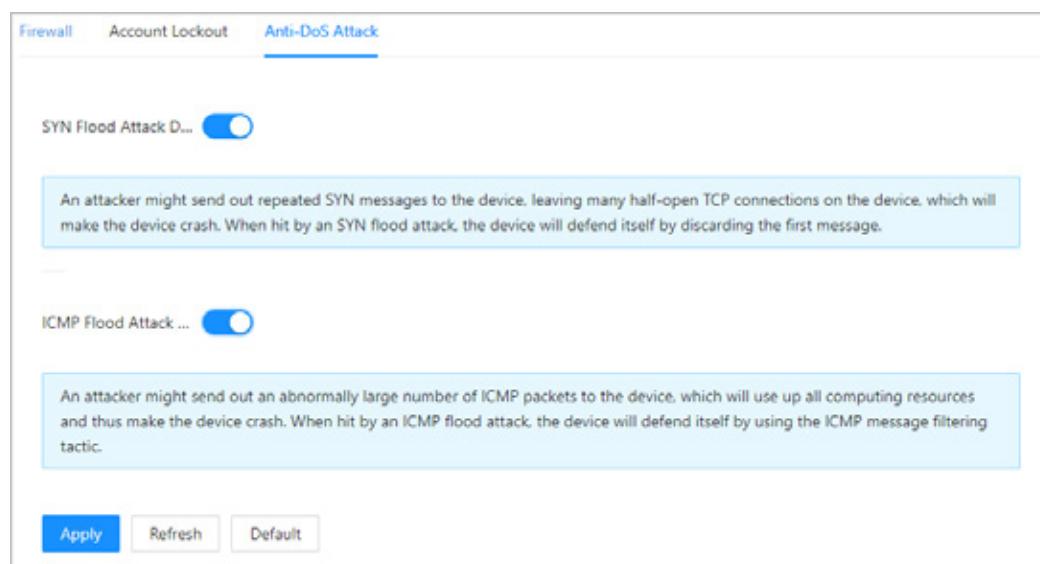
3.12.3.3 Configuring Anti-DoS Attack

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 3-47 Anti-DoS attack



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 3-48 Certificate information

Step 2: Fill in certificate information.

Custom Name	<input type="text"/>
* IP/Domain Name	<input type="text"/> 103
Organization Unit	<input type="text"/>
Organization	<input type="text"/>
* Validity Period	<input type="text"/> Days (1~5000)
* Region	<input type="text"/>
Province	<input type="text"/>
City Name	<input type="text"/>

[Back](#) [Create and install certificate](#) [Cancel](#)



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 **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 3-49 Certificate information (2)

Step 2: Fill in certificate information.

* IP/Domain Name	172.17.0.3
Organization Unit	
Organization	
* Region	
Province	
City Name	

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 **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.

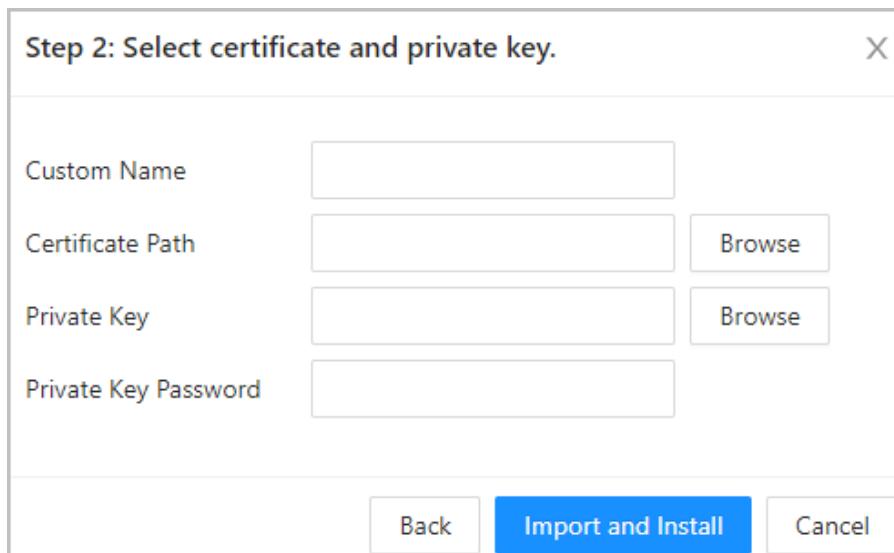
Procedure

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 3-50 Certificate and private key



Step 2: Select certificate and private key.

Custom Name

Certificate Path [Browse](#)

Private Key [Browse](#)

Private Key Password

[Back](#) [Import and Install](#) [Cancel](#)

- 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 **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.

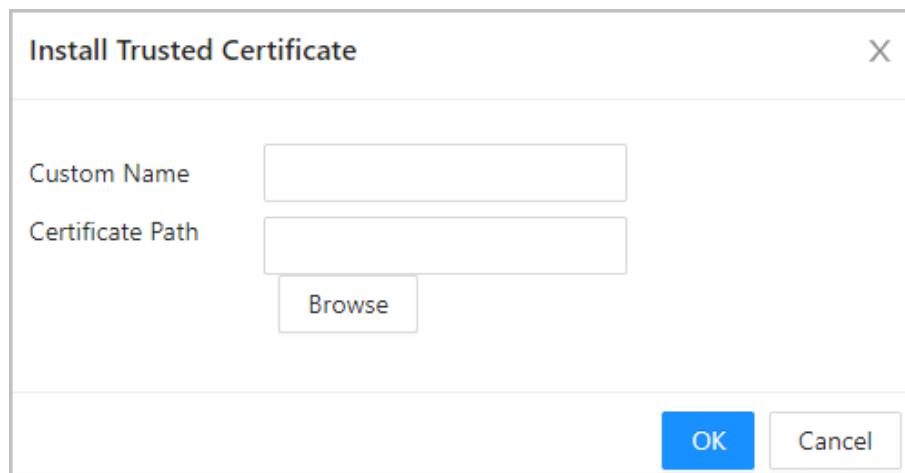
Background Information

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 3-51 Install the trusted certificate



Step 4 Click **OK**.

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

Related Operations

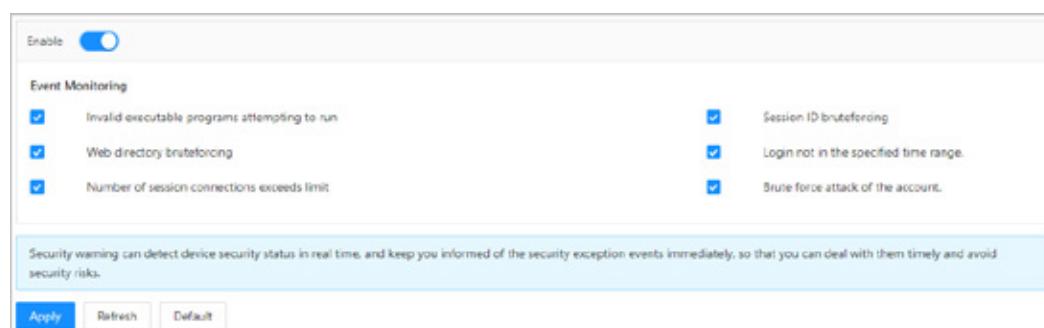
- Click **Edit Mode** on the **Device Certificate** page to edit the name of the certificate.
- Click  to download the certificate.
- Click  to delete the certificate.

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 3-52 Security warning



Step 4 Click **Apply**.

3.12.7 Security Authentication

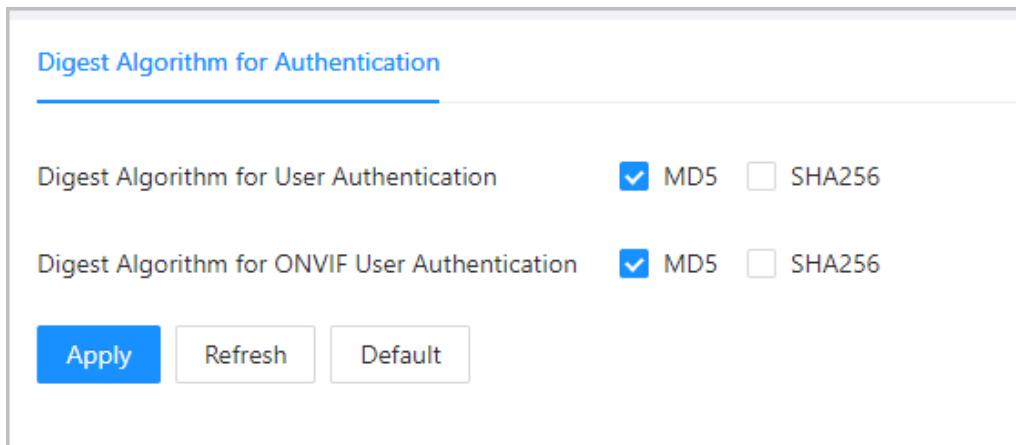
Procedure

Step 1 Select **Security > Security Authentication**.

Step 2 Select a message digest algorithm.

Step 3 Click **Apply**.

Figure 3-53 Security authentication



The screenshot shows a configuration interface titled "Digest Algorithm for Authentication". It contains two sections: "Digest Algorithm for User Authentication" and "Digest Algorithm for ONVIF User Authentication". In both sections, the "MD5" checkbox is checked and "SHA256" is unchecked. At the bottom are three buttons: "Apply" (blue), "Refresh" (white), and "Default" (white).

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

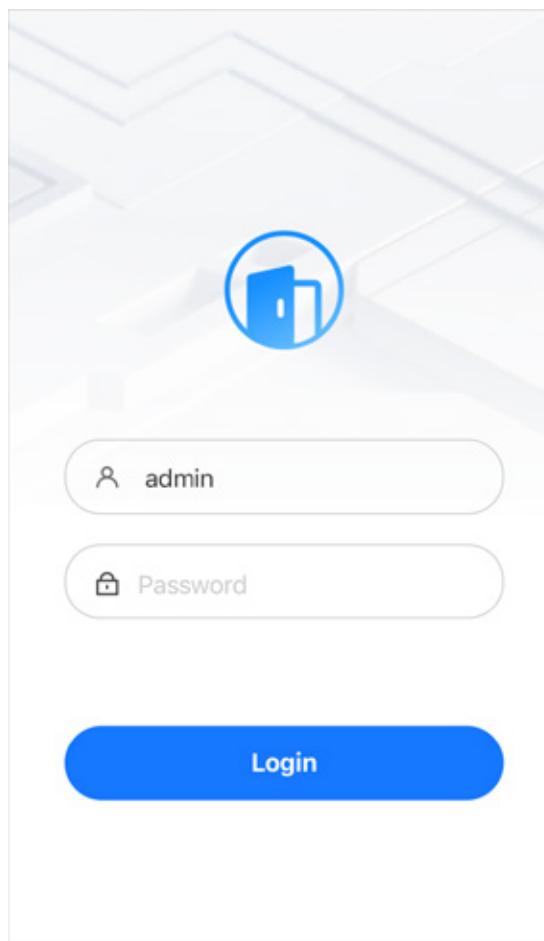
Step 1 Open a browser, and then enter to the IP address of the Device.

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



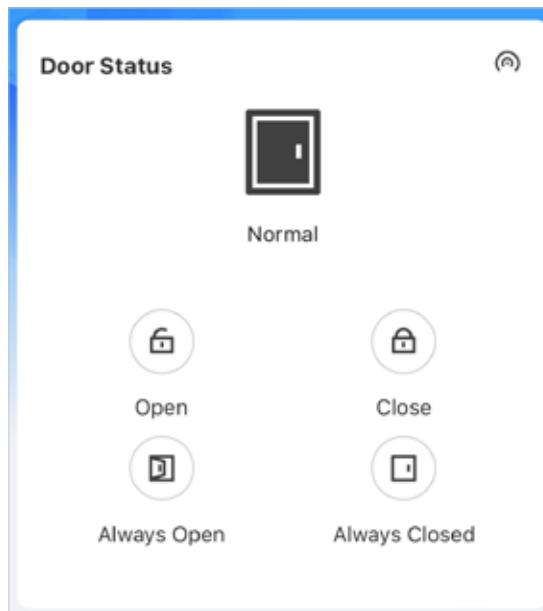
Step 3 Click **Login**.

4.2 Home Page

The home page is displayed after you successfully log in.

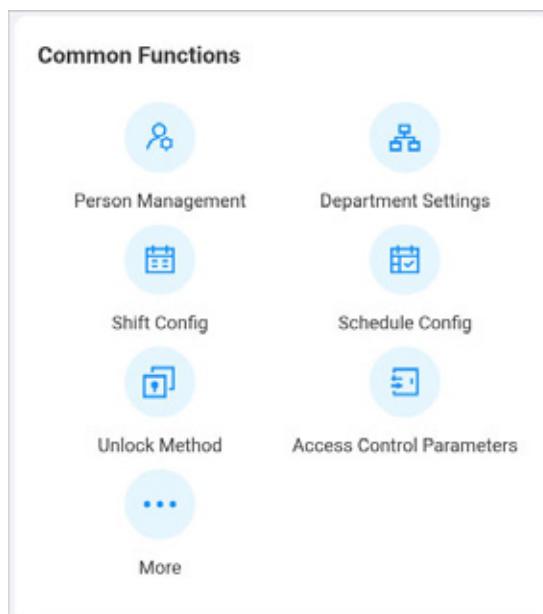
- The **Door Status** area displays the status of the door. You can remotely open or close the door. You can also configure the door status as **Always Open** or **Always Closed**.

Figure 4-2 Door status



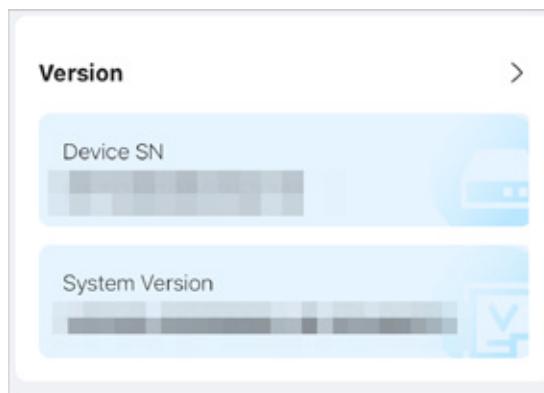
- The **Common Function** area displays the configuration menu of the Device. Click **More** to view all the configuration menus.

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



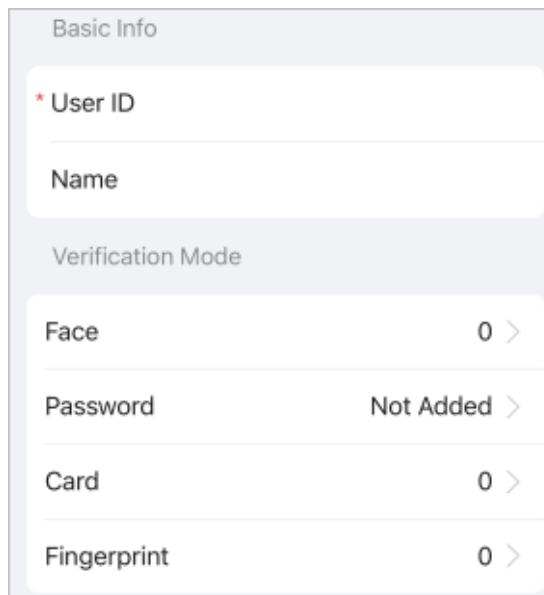
4.3 Person Management

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)



Basic Info	
* User ID	
Name	
Verification Mode	
Face	0 >
Password	Not Added >
Card	0 >
Fingerprint	0 >

Figure 4-6 Add the person (2)

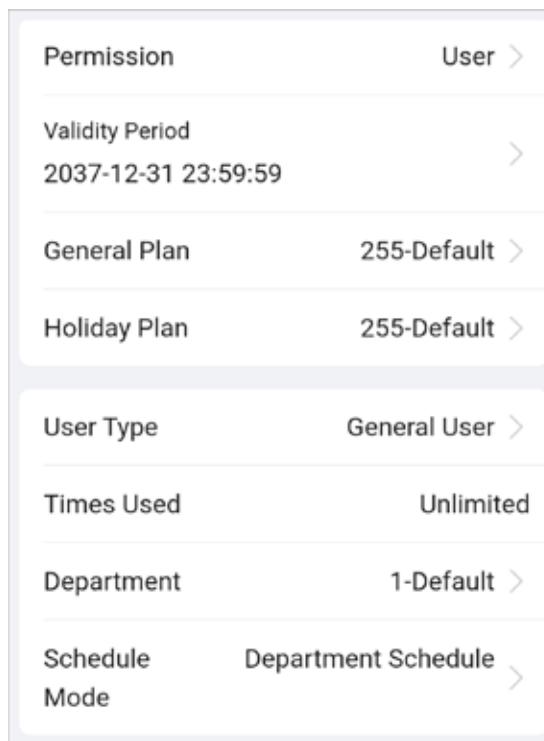


Table 4-1 Parameters description

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	<ul style="list-style-type: none"> Enter the card number manually. <p>1. Click Add. 2. Enter the card number, and then click Add.</p> <ul style="list-style-type: none"> Read the number automatically through the Device. <p>1. Click Add. 2. 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.</p> <p>3. Click OK.</p> <p>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.</p> <p>You can enable the Duress Card function. An alarm will be triggered if a duress card is used to unlock the door.</p> <ul style="list-style-type: none"> ● Duress Card : Click to set duress card. ● Change Card No. : Click to change the card number.  <p>One user can only set one duress card.</p>
Fingerprint	<p>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.</p> <p>Enroll fingerprints through an enrollment reader or the Device.</p> <p>1. Click Add. 2. Press finger on the scanner according to the on-screen instructions. 3. Click OK.</p>  <ul style="list-style-type: none"> ● 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	<ul style="list-style-type: none"> ● 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	<p>People can unlock the door or take attendance during the defined period.</p>  <p>You can select more than one plan.</p>
Holiday Plan	<p>People can unlock the door or take attendance during the defined holiday.</p>  <p>You can select more than one holiday.</p>
User Type	<ul style="list-style-type: none"> ● 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	<p>Set an unlock limit for guest users. After the unlock times run out, they cannot unlock the door.</p>
Department	<p>Add users to a department. If a department schedule is assigned to the person, they will follow the established department schedule.</p> <ul style="list-style-type: none"> ● Department Schedule: Assign department schedule to the user. ● Personal Schedule: Assign personal schedule to the user.
Schedule Mode	 <p>◊ This function is only available on select models.</p> <p>◊ 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.</p>

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.

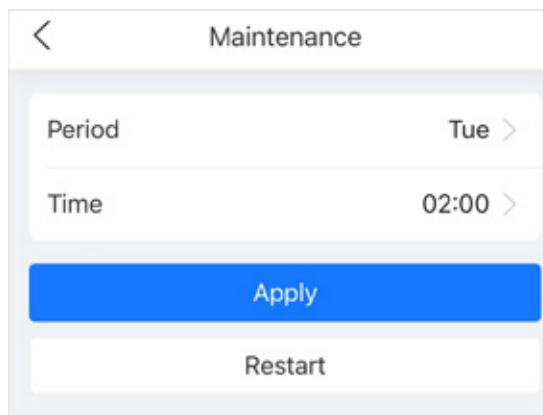
4.4.2 Maintenance

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



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

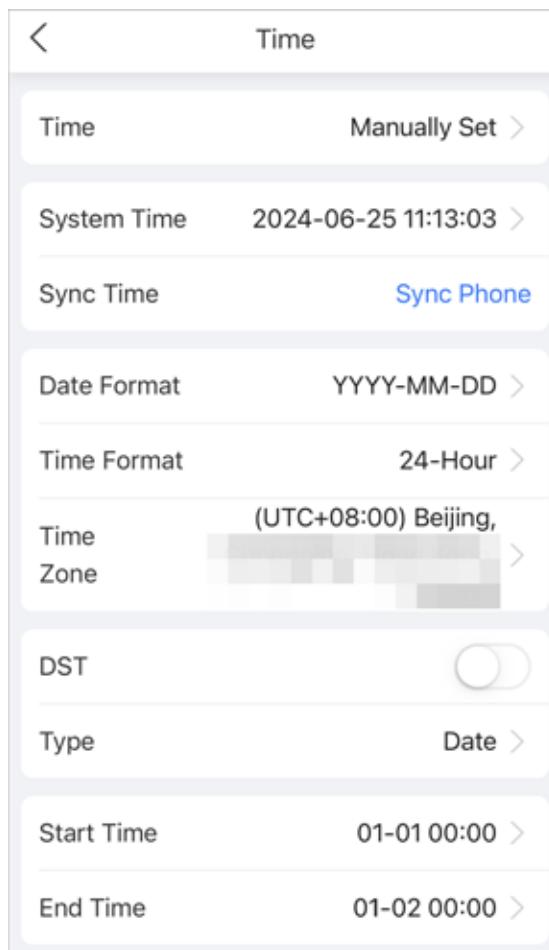


Table 4-2 Time settings description

Parameter	Description
Time	<ul style="list-style-type: none"> 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. <ul style="list-style-type: none"> 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	<ol style="list-style-type: none"> (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

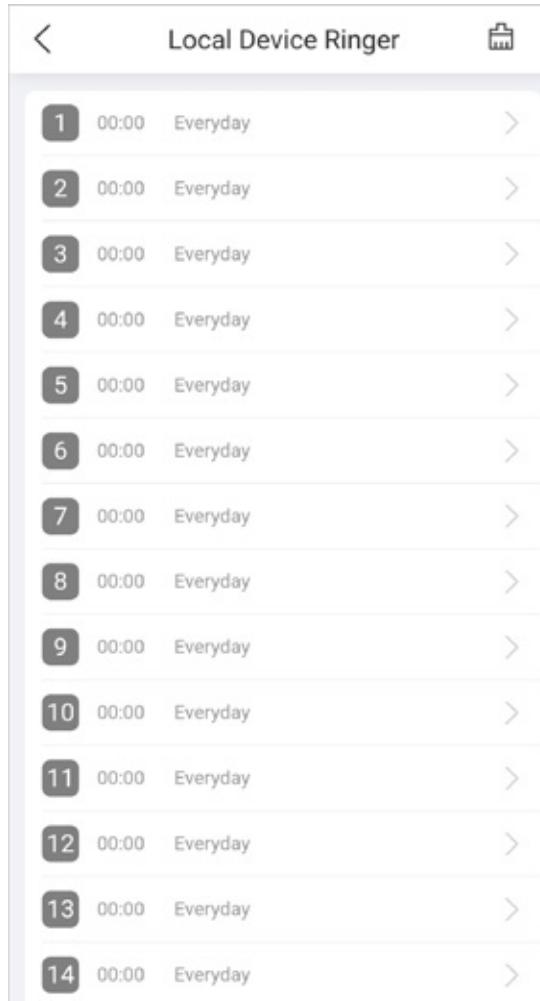
Configure the time when the bell rings as a reminder.

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

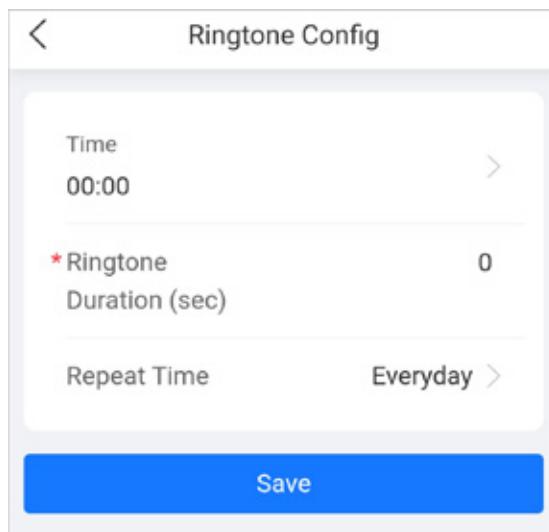


Table 4-3 Parameters description

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.

4.5 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**.

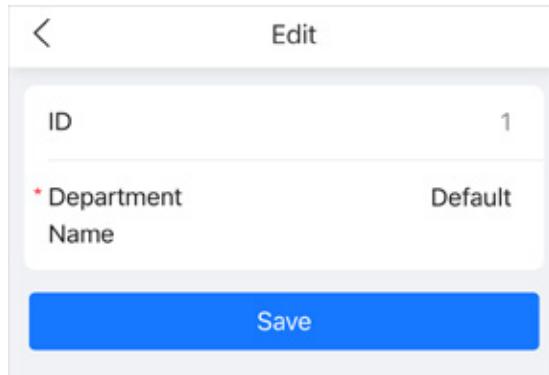
Figure 4-11 Department settings



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



ID	1
* Department Name	Default

Save

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

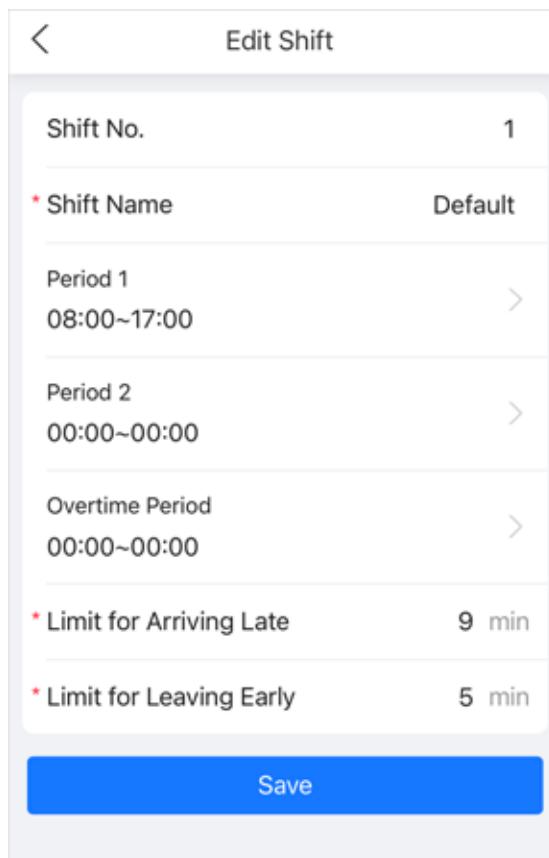
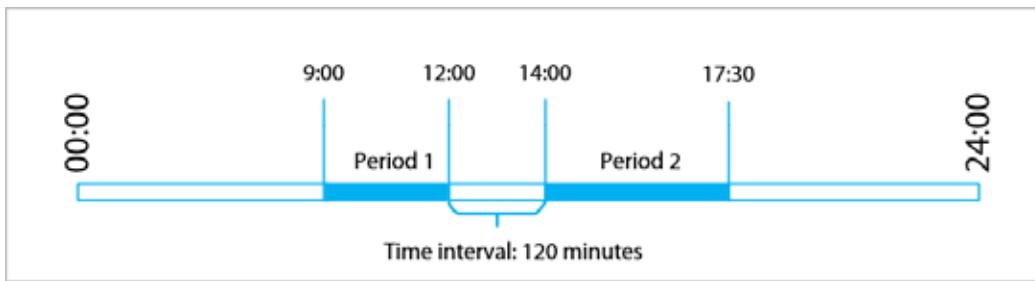


Table 4-4 Shift parameters description

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. 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.
Period 2	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)



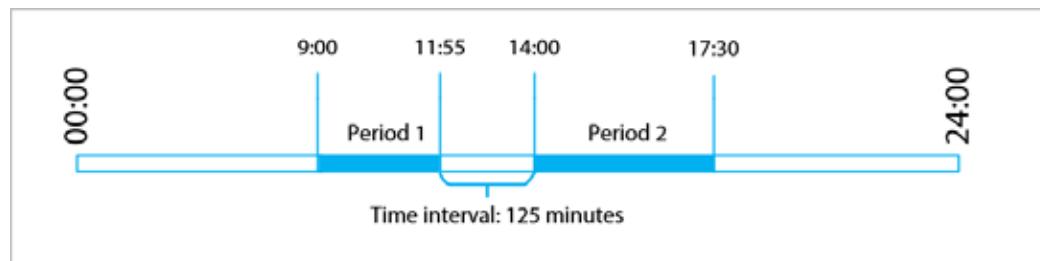
For example: If the interval is 120 minutes, then the clock-out time for period 1 is from 12:00 to 12:59, and the clock-in time for period 2 is from 13:00 to 14:00.



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

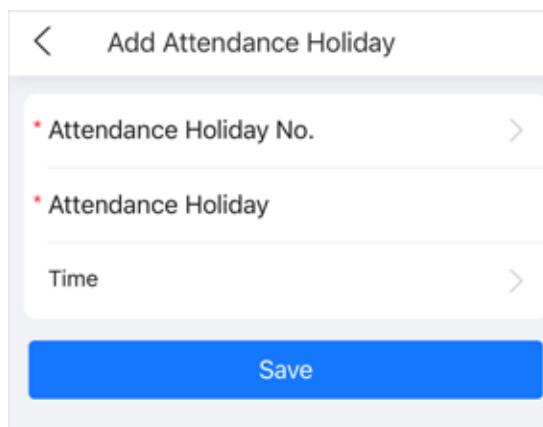


Table 4-5 Parameters description

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

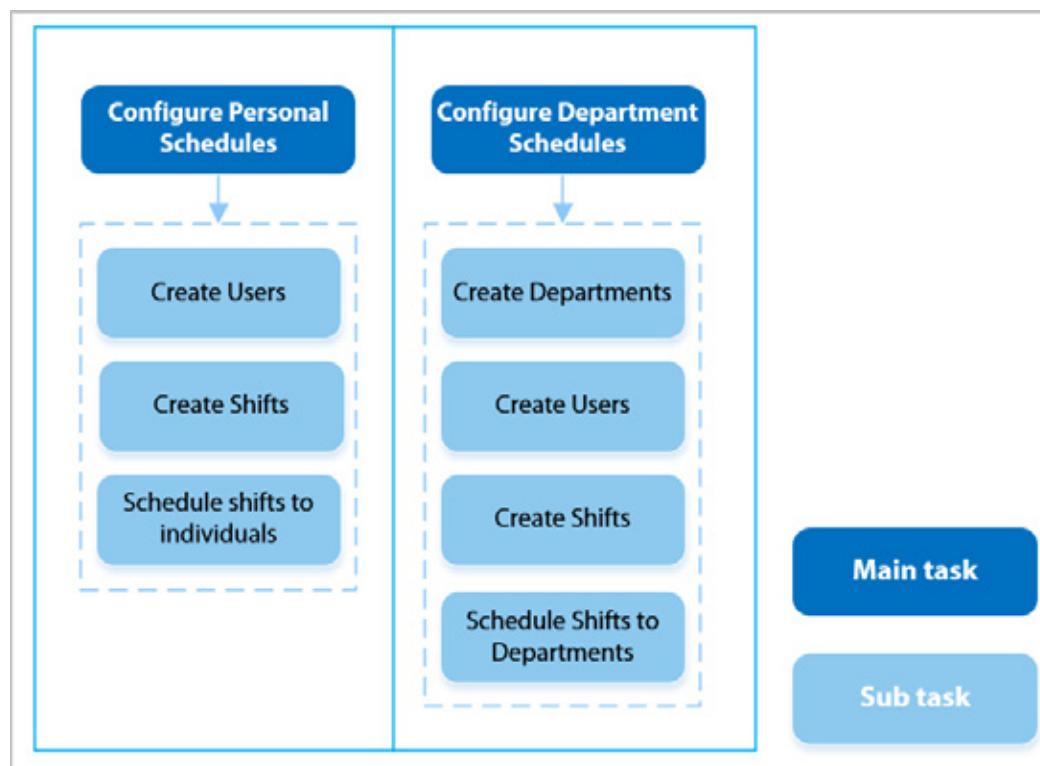
A work schedule generally refers to the days per month and the hours per day that an employee is expected to be at their job. You can create different types of work schedules based on different individuals or departments, and then employees must follow the established work schedules.

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.



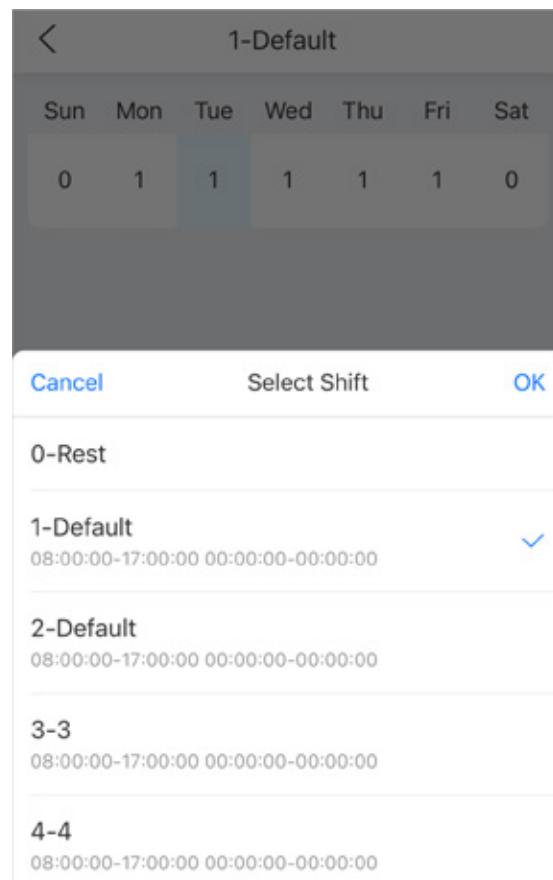
You can only set work schedules for the current month and the next month.

- 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



- 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.	<ul style="list-style-type: none"> 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.	<ul style="list-style-type: none"> Overtime check in: Clock in when your overtime period starts. Overtime check out: Clock out when your overtime period ends.
Manual Mode	<ul style="list-style-type: none"> 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. <p></p> <p>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.</p>	<ul style="list-style-type: none"> Overtime check in: Clock in when your overtime period starts. Overtime check out: Clock out when your overtime period ends.
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.

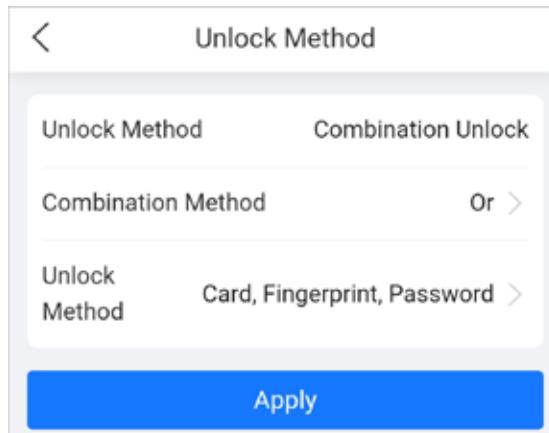
Procedure

- 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



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 click **Apply**.

Figure 4-21 Access control parameters (1)

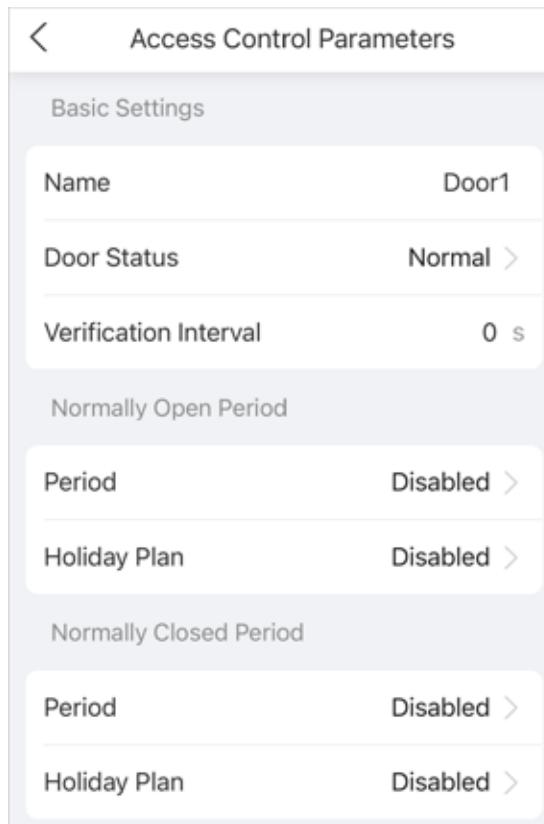


Figure 4-22 Access control parameters (2)

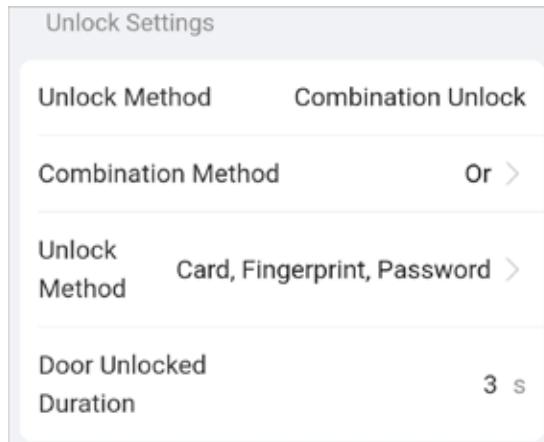


Table 4-7 Description of access control parameters

Parameter	Description	
Basic Settings	Name	The name of the door.

Parameter	Description
Door Status	<p>Set the door status.</p> <ul style="list-style-type: none"> 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.
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. 
Normally Closed Period	<ul style="list-style-type: none"> 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.
	Combination Method <ul style="list-style-type: none"> 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 Click **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 click **Apply**.



Figure 4-23 Alarm settings

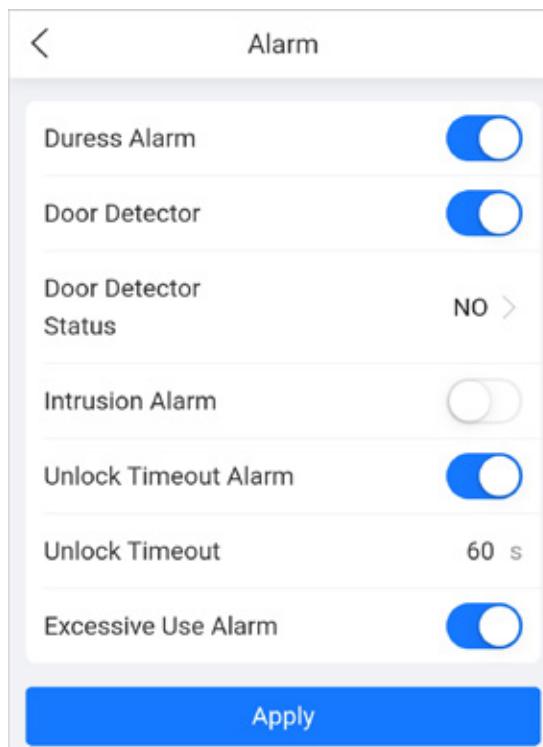


Table 4-8 Description of alarm parameters

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	<p>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.</p> <ul style="list-style-type: none"> ● 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	<p>If the door is opened abnormally, an intrusion alarm will be triggered and last for a defined time.</p> <p></p> <p>The door detector and intrusion need to be enabled at the same time.</p>

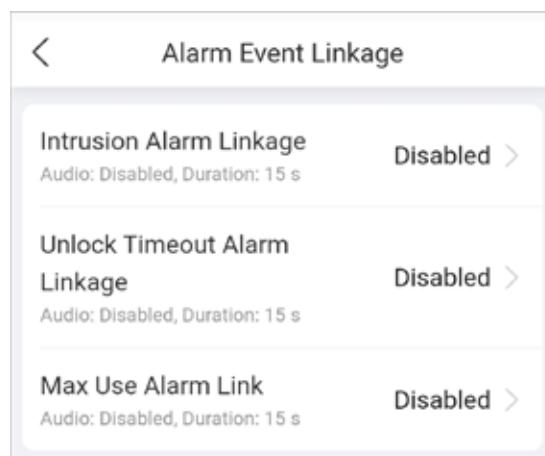
Parameter	Description
Unlock Timeout Alarm	When the door remains unlocked for longer than the defined timeout duration, the door timeout alarm will be triggered and last for the defined time.
Unlock Timeout	 The door detector and door timed out function need to be enabled at the same time.
Excessive 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.

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.

Parameter	Description
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 click **Apply**.

Figure 4-25 Card settings

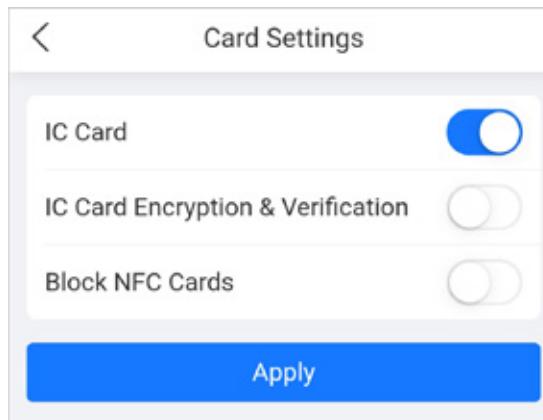


Table 4-10 Card parameters description

Parameter	Description	
Card Settings	IC Card	The IC card can be read when this function is enabled.  This function is only available on select models.
	IC Card Encryption & Verification	The encrypted card can be read when this function is enabled.  Make sure IC Card is enabled.

Parameter	Description
	<p>Block NFC Cards</p> <p>Prevent unlocking through duplicated NFC card after this function is enabled.</p>  <ul style="list-style-type: none"> • This function is only available on models that support IC cards. • Make sure IC Card is enabled. • NFC function is only available on select models of phones.
Card No. System	<p>Card No. System</p> <p>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.</p>

Step 4 Click **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

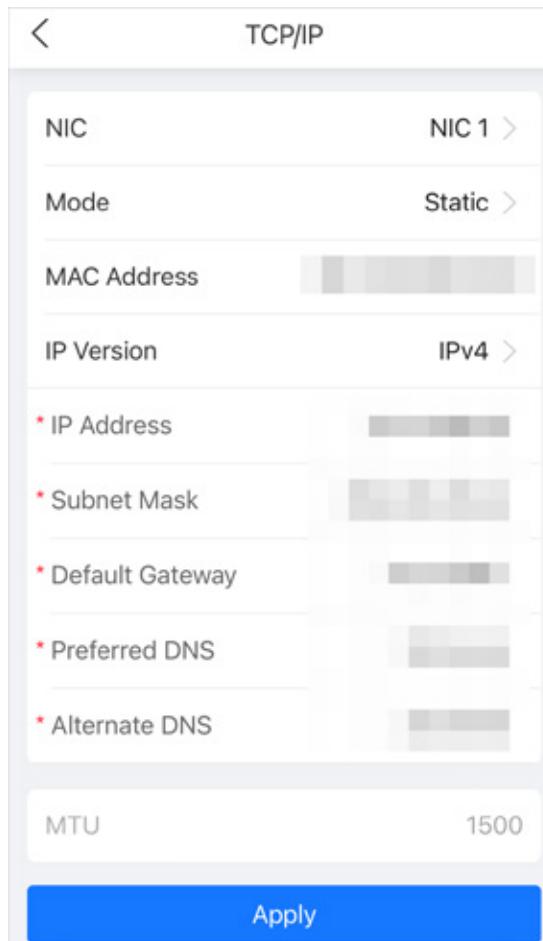


Table 4-11 Description of TCP/IP

Parameter	Description
Mode	<ul style="list-style-type: none"> 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	<p></p> <ul style="list-style-type: none"> 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	<p>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:</p> <ul style="list-style-type: none"> • 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

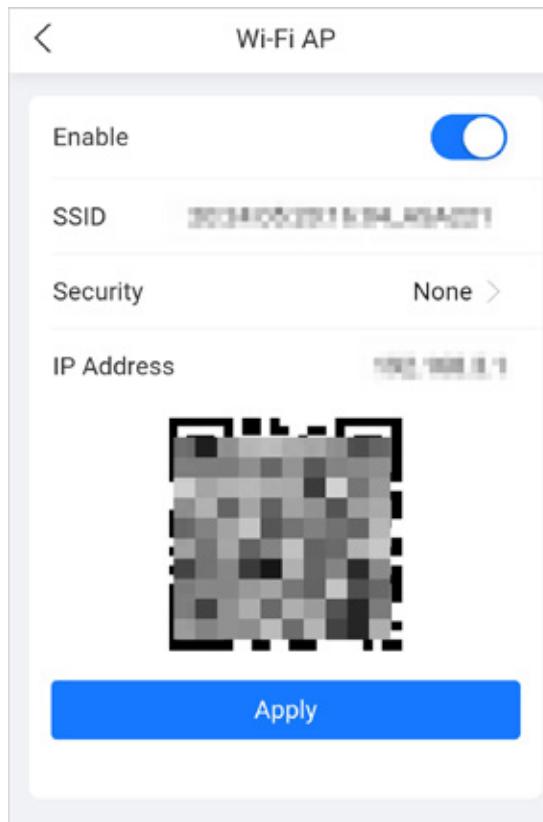


- The Wi-Fi function is available on select models.
- The Wi-Fi and Wi-Fi AP cannot be enabled at the same time.

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

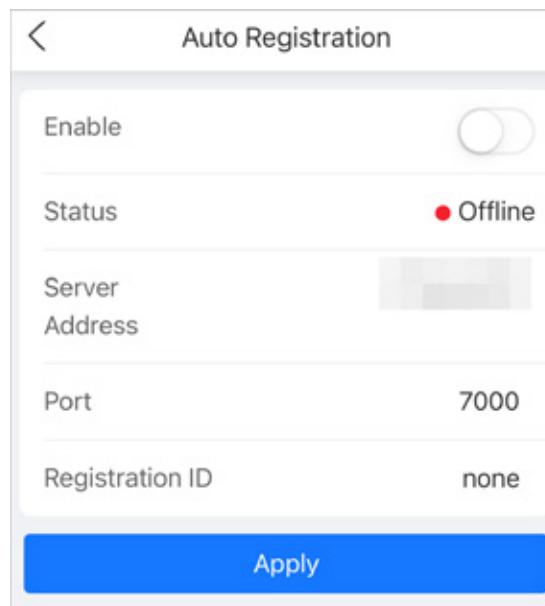


Table 4-12 Automatic registration description

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.

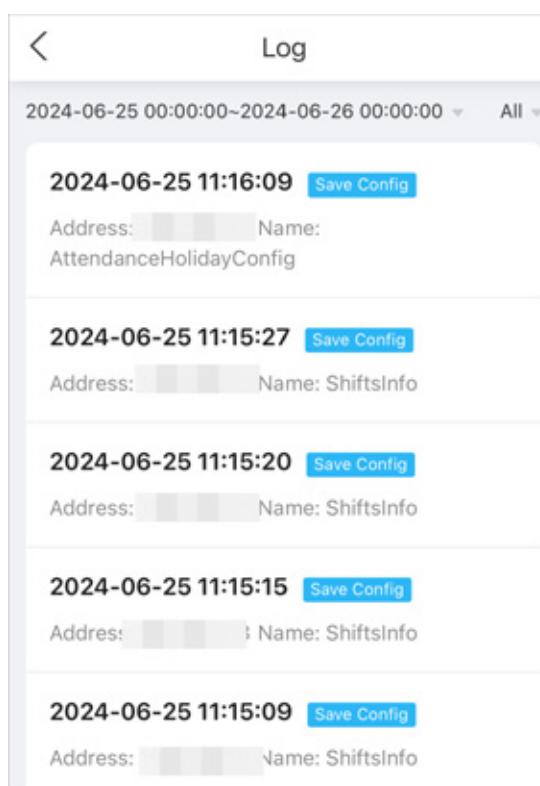
4.9.1 System Logs

View and search for system logs.

Procedure

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

Figure 4-29 Logs



Date	Time	Action
2024-06-25	11:16:09	Save Config Address: [REDACTED] Name: AttendanceHolidayConfig
2024-06-25	11:15:27	Save Config Address: [REDACTED] Name: ShiftsInfo
2024-06-25	11:15:20	Save Config Address: [REDACTED] Name: ShiftsInfo
2024-06-25	11:15:15	Save Config Address: [REDACTED] Name: ShiftsInfo
2024-06-25	11:15:09	Save Config Address: [REDACTED] Name: ShiftsInfo

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**.



Appendix 1 Important Points of Fingerprint Registration Instructions

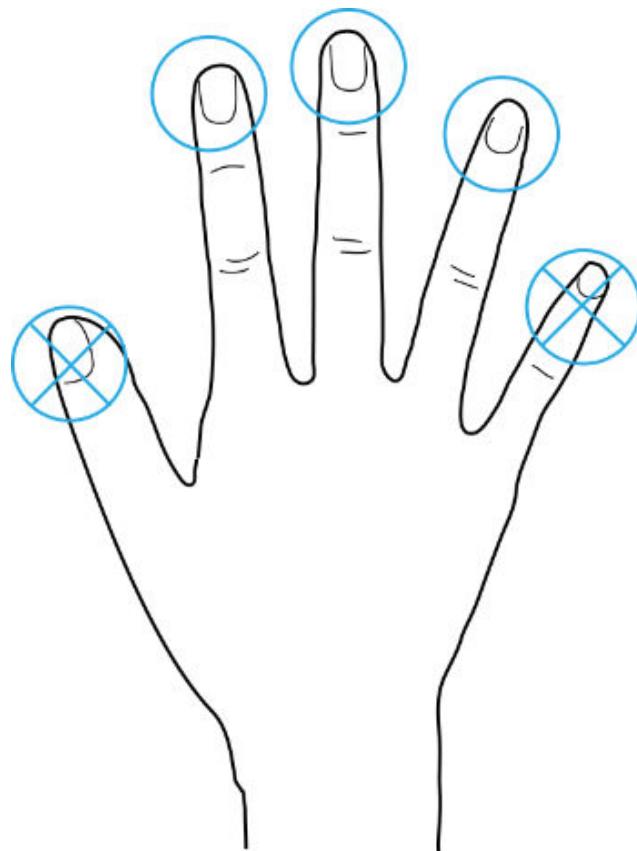
When you register the fingerprint, pay attention to the following points:

- 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

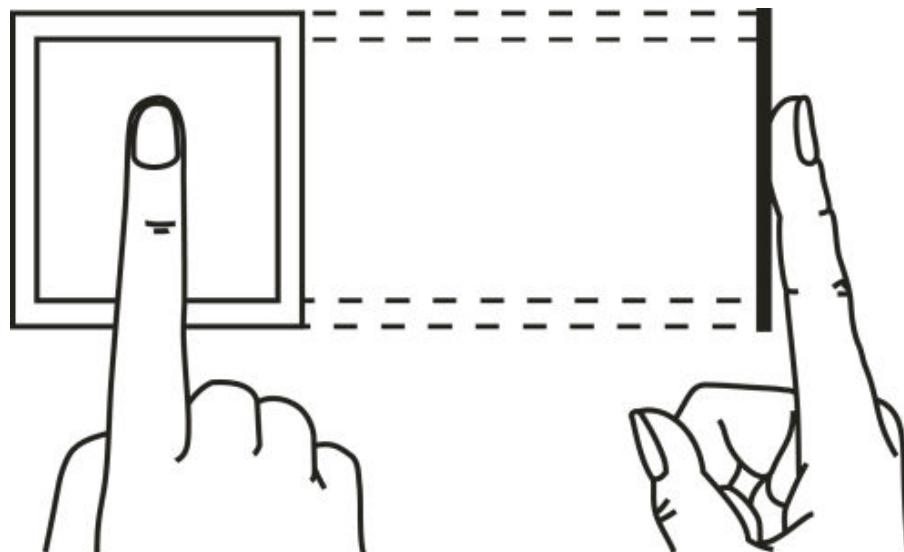
Forefingers, middle fingers, and ring fingers are recommended. Thumbs and little fingers cannot be put at the recording center easily.

Appendix Figure 1-1 Recommended fingers

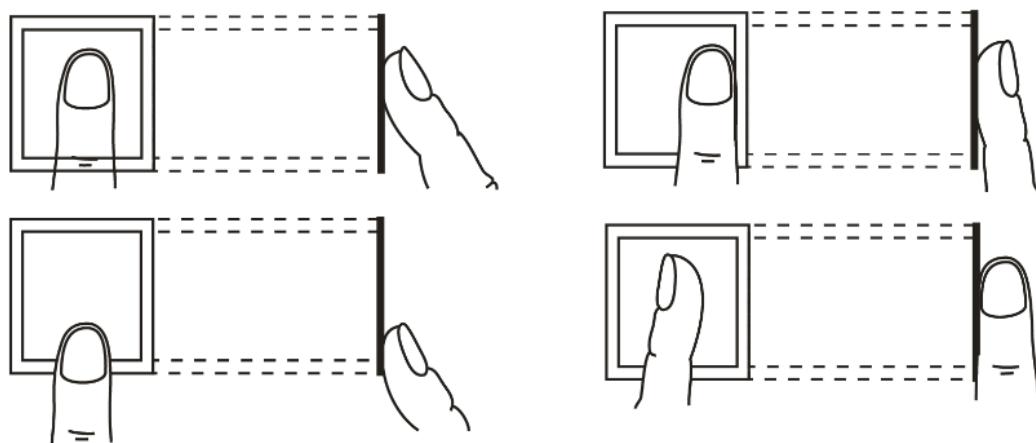


How to Press Your Fingerprint on the Scanner

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 lockout function

The account lockout 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 Allow list

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

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).





Contact Us

D-162, Okhla Industrial Area, Phase-I, Delhi 110020

Email: sales@timewatchindia.com

Phone: +91-11-41916615

Mobile No: +91-95999-53923



New Delhi - NCR



Mumbai



Ahmedabad



Bengaluru



Chennai



Kolkata



Dubai