

Access Standalone

User Manual



V1.0.0

Foreword

General

This manual introduces the functions and operations of the Access Standalone (hereinafter referred to as the "Device"). Read carefully before using the device, and keep the manual safe for future reference.

Model

Model J, Model H, Model F

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.
 ESD	Electrostatic Sensitive Devices. Indicates a device that is sensitive to electrostatic discharge.
 ELECTRIC SHOCK	Indicates dangerous high voltage. Take care to avoid coming into contact with electricity.
 LASER RADIATION	Indicates a laser radiation hazard. Take care to avoid exposure to a laser beam.
 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.	November 2025

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 manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.
- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Table of Contents

Foreword.....	I
1 Overview.....	1
2 Local Operations (Keypad Models).....	2
2.1 Preparation.....	2
2.1.1 Keypad Function.....	2
2.1.2 Input Method.....	3
2.2 Initialization.....	5
2.3 Main Screen.....	5
2.4 Logging in to the Main Menu.....	6
2.5 Unlocking Methods.....	7
2.5.1 Card.....	7
2.5.2 Fingerprint.....	7
2.5.3 User Password.....	8
2.5.4 Public Password.....	8
2.5.5 Temporary Password.....	9
2.6 Person Management.....	10
2.6.1 Adding New User.....	10
2.6.2 User/Admin List.....	12
2.6.3 Configuring Public Password.....	14
2.6.4 Deleting All Users.....	14
2.7 Access Control Management.....	14
2.7.1 Combination Unlock.....	14
2.7.2 Configuring Alarms.....	15
2.7.3 Configuring Lock Status.....	16
2.7.4 Configuring Verification Intervals.....	17
2.7.5 Managing Main Cards.....	17
2.7.6 Configuring PIN Code Authentication.....	18
2.8 Attendance Management.....	18
2.9 Communication Settings.....	18
2.9.1 Configuring IP.....	18
2.9.2 Configuring Wi-Fi.....	19
2.9.3 Configuring Wi-Fi AP.....	20
2.9.4 Mode Settings.....	21
2.10 System Settings.....	25
2.10.1 Configuring Time.....	25
2.10.2 Configuring Volume.....	26
2.10.3 Configuring Language.....	27

2.10.4	Configuring Screen Parameters.....	27
2.10.5	Configuring Card Settings.....	28
2.10.6	Managing Device Password.....	29
2.10.7	Restoring to Factory Defaults.....	30
2.10.8	Resetting Device.....	31
2.11	USB Management.....	31
2.11.1	Exporting Data.....	31
2.11.2	Importing Data.....	32
2.11.3	Updating Device.....	33
2.12	Records Management.....	33
2.13	Viewing Information.....	33
2.13.1	Viewing Data Capacity.....	33
2.13.2	Viewing Device Version.....	34
3	Local Operations (Touchscreen Models).....	35
3.1	Initialization.....	35
3.2	Appearance.....	35
3.3	Main Screen.....	35
3.4	Logging In to the Main Menu.....	37
3.5	Resetting the Password.....	38
3.6	Unlock Methods.....	39
3.6.1	Card.....	39
3.6.2	Fingerprint.....	39
3.6.3	Bluetooth.....	39
3.6.4	User Password.....	40
3.6.5	Public Password.....	41
3.6.6	Temporary Password.....	42
3.7	Person Management.....	43
3.7.1	Adding Users.....	43
3.7.2	Viewing User and Admin Information.....	45
3.7.3	Configuring Public Password.....	47
3.8	Access Control Management.....	47
3.8.1	Configuring Unlock Method.....	47
3.8.2	Configuring Alarms.....	49
3.8.3	Configuring Verification Interval.....	51
3.8.4	Configuring the Lock Status.....	51
3.8.5	Managing Main Cards.....	52
3.8.6	Configuring PIN Code Authentication.....	53
3.9	Attendance Management.....	53
3.10	Communication Settings.....	54
3.10.1	Configuring IP.....	54

3.10.2	Configuring Wi-Fi.....	55
3.10.3	Configuring Wi-Fi AP.....	55
3.10.4	Configuring Bluetooth.....	56
3.10.5	Mode Settings.....	57
3.11	System Settings.....	61
3.11.1	Configuring Time.....	61
3.11.2	Configuring Language.....	62
3.11.3	Configuring Volume.....	62
3.11.4	Configuring Screen Parameters.....	63
3.11.5	Configuring Card Settings.....	65
3.11.6	Configuring Device Password.....	67
3.11.7	Restoring Factory Defaults.....	67
3.11.8	Configuring Password Reset.....	68
3.11.9	Restarting the Device.....	68
3.12	USB Management.....	68
3.12.1	Exporting Data.....	69
3.12.2	Importing Data.....	69
3.12.3	Updating Device.....	70
3.13	Records Management.....	70
3.14	Viewing Information.....	71
3.14.1	Viewing Data Capacity.....	71
3.14.2	Viewing Device Version.....	71
4	Web Operations.....	72
4.1	Initialization.....	72
4.2	Logging In.....	72
4.3	Resetting the Password.....	73
4.4	Access Monitoring.....	73
4.5	Home Page.....	75
4.6	Person Management.....	75
4.7	Access Control Management.....	81
4.7.1	Access Control Parameters.....	81
4.7.2	Alarm.....	85
4.7.3	Card Settings.....	90
4.7.4	Configuring Periods.....	95
4.7.5	Configuring Expansion Modules.....	98
4.7.6	Configuring Back-end Comparison.....	98
4.7.7	Configuring First-Person Unlock.....	99
4.7.8	Configuring Anti-Passback.....	100
4.8	Attendance Configuration.....	102
4.8.1	Configuring Departments.....	102

4.8.2	Configuring Shifts.....	103
4.8.3	Configuring Holiday.....	105
4.8.4	Configuring Work Schedules.....	106
4.8.5	Exporting Attendance Record.....	109
4.8.6	Configuring Attendance Modes.....	110
4.9	Audio.....	111
4.9.1	Configuring Audio Parameters.....	111
4.9.2	Managing Audio Files.....	113
4.10	Communication Settings.....	113
4.10.1	Network Settings.....	113
4.10.2	Bluetooth Settings.....	125
4.10.3	Mode Settings.....	125
4.11	System Management.....	129
4.11.1	User Management.....	129
4.11.2	Viewing Online Users.....	132
4.11.3	Configuring Time.....	132
4.11.4	Configuring Always On.....	134
4.12	Maintenance Center.....	134
4.12.1	One-click Diagnosis.....	134
4.12.2	System Information.....	135
4.12.3	Data Capacity.....	135
4.12.4	Viewing Logs.....	136
4.12.5	Maintenance Management.....	137
4.12.6	Updating the System.....	139
4.12.7	Advanced Maintenance.....	140
4.13	Security Settings(Optional)	141
4.13.1	Security Status.....	141
4.13.2	Configuring HTTPS.....	142
4.13.3	Attack Defense.....	143
4.13.4	Installing Device Certificate.....	146
4.13.5	Installing the Trusted CA Certificate.....	149
4.13.6	Security Warning.....	150
4.13.7	Security Authentication.....	151
5	Phone Operations.....	152
5.1	Initialization.....	152
5.2	Logging in to the Webpage.....	152
5.3	Home Page.....	154
5.4	Person Management.....	156
5.5	Configuring the System.....	160
5.5.1	Viewing Version Information.....	160

5.5.2	Configuration Management.....	160
5.5.3	Maintenance.....	160
5.5.4	Configuring Time.....	161
5.5.5	Data Capacity.....	162
5.5.6	Language.....	162
5.6	Configuring Attendance.....	162
5.6.1	Configuring Departments.....	162
5.6.2	Configuring Shifts.....	164
5.6.3	Configuring Holiday.....	167
5.6.4	Configuring Work Schedules.....	168
5.6.5	Configuring Attendance Modes.....	170
5.7	Configuring Access Control.....	171
5.7.1	Configuring Unlock Methods.....	171
5.7.2	Configuring Access Control Parameters.....	172
5.7.3	Configuring Alarms.....	176
5.7.4	Configuring Alarm Linkages (Optional).....	179
5.7.5	Configuring Alarm Event Linkage.....	180
5.7.6	Configuring Card Settings.....	181
5.7.7	Configuring Screen Settings.....	183
5.8	Communication Settings.....	184
5.8.1	Configuring TCP/IP.....	184
5.8.2	Configuring Wi-Fi.....	186
5.8.3	Configuring Wi-Fi AP.....	186
5.8.4	Configuring Cloud Service.....	187
5.8.5	Configuring Auto Registration.....	187
5.8.6	Configuring Mode.....	188
5.8.7	Configuring Bluetooth.....	192
5.9	Configuring Audio Prompts.....	193
5.10	Viewing Logs.....	194
5.10.1	System Logs.....	194
5.10.2	Unlock Records.....	194
5.10.3	Call History.....	195
5.10.4	Alarm Logs.....	195
6	Smart PSS Lite Configuration.....	196
6.1	Installation.....	196
6.2	Initialization and Logging In.....	196
6.3	Adding Devices.....	197
6.3.1	Adding Device by Searching.....	197
6.3.2	Adding Device One by One.....	198
Appendix 1 Important Points of Fingerprint Registration Instructions.....		199

Appendix 2 Security Recommendation..... 201

1 Overview

The access standalone features a built-in high-performance processor and a newly upgraded exterior design. They support multiple entry methods, including fingerprint (available on select models), card, password, Bluetooth (available on select models), and combination verification. When paired with the management platform, these devices enable a variety of functions to meet diverse user needs.

2 Local Operations (Keypad Models)

2.1 Preparation

2.1.1 Keypad Function

The device is a non-touchscreen model that requires operation on physical keys. When the device is in standby mode, you can press any key to activate the screen.



Only for specific models, pressing the ring key can activate the screen.

Figure 2-1 Model H



Figure 2-2 Model J



Table 2-1 Description of keypad

Item	Description
Number or letter	Used to enter information or password.
^	Arrow keys to navigate the page.
v	
Esc	Cancel an operation or go back to the previous page.
OK	Go to the selected page or confirm your change.
<X	Backspace.
 	Ring the bell (only on the standby screen), navigate the screen, or change the input method.

2.1.2 Input Method

Changing Input Method

- Model H: Press  to change the input method.
- Model J: Press  to change the input method.

Input Method Overview

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

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

Entering Uppercase or Lowercase Letters

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

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

In the uppercase letter mode:

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

Table 2-2 Letter-key mapping

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

Entering Uppercase and Lowercase Letters

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

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

Entering Numbers

In numeric mode, press the desired number key.

Entering Characters

In character mode, press the corresponding number keys to select the desired character, and then press **^** / **√** to navigate to the previous/next page.

Figure 2-3 Enter characters

Create User(1/4)

ID 2

Name

Verification Mode Same as Device

+ =

1, 2, 3 ? 4 ! 5 : 6 ; 7 " 8 ' 9 `

2.2 Initialization

For first-time use or after restoring factory defaults, you need to set a password and associate your email address for the admin account. You also need to set the time zone of the Device. You can use the admin account to log in to the main menu of the Device, configure the Device, and log in to the web browser and SmartPSS Lite.

Figure 2-4 Initialization

Device Initialization ✓

Admin admin

PWD

PWD Confirm

E-mail

Time Zone < GMT+08:00 >



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

2.3 Main Screen

You can unlock the door on the main screen with your card, password, or fingerprint.



- The Device goes back to the standby page if there is no operation in 30 seconds.

- The screen in the user manual is for reference only.

Figure 2-5 Main screen

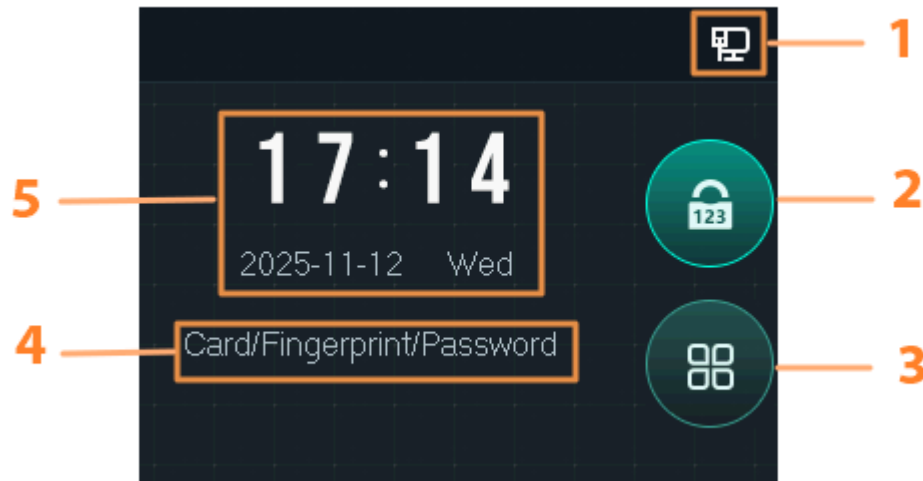


Table 2-3 Description of main screen

No.	Item	Description
1	Status	Displays the status of Wi-Fi, wired network (if any), and USB drive.
2	Unlock the door with password	Enter the user ID and password, or the administrator password to unlock the door.
3	Main menu	Tap to enter the main menu. Only Admin and users with administrator permission can log in to the main menu.
4	Unlocking methods	Displays the unlocking methods you configured.
5	Date & Time	Time and date.

2.4 Logging in to the Main Menu

Log in to the main menu to configure parameters of the Device. For example, you can add users of different permissions and change the unlocking mode.

Background Information

Only the administrator and admin users can log in to the main menu.

Procedure

- Step 1** On the standby screen, tap $\wedge$ / $\vee$ to navigate to , and then press **OK**.



Verification methods varies with the Device type.

- Step 2** Log in to the main menu.

- Log in as a user with the administrator permission by using a card, fingerprint, or password.

- Log in as **admin** : Press **admin**, and then enter the password you set during initialization.

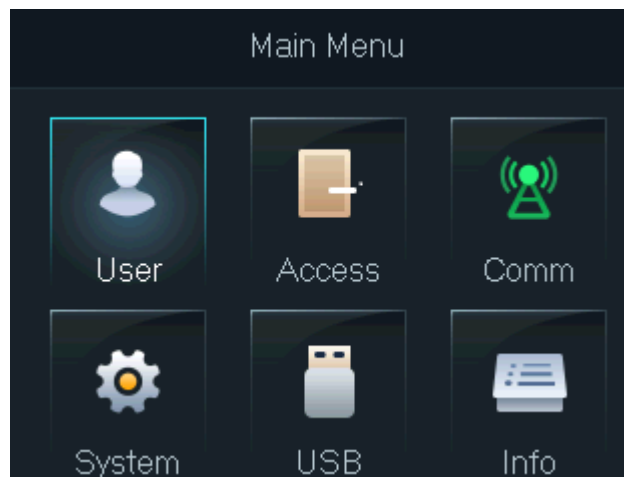
Step 3 On the main menu, tap $\wedge$ / $\vee$ to navigate the page, and then press **OK** to configure parameters of the Device.



Use the shortcuts to configure parameters by simply tapping 1–6.

- To configure user management, press 1.
- To configure access control, press 2.
- To configure communication, press 3.
- To configure system, press 4.
- To configure USB, press 5.
- To view system information, press 6.

Figure 2-6 Main menu



2.5 Unlocking Methods

2.5.1 Card

Swipe your card to unlock the door.



For the Access Standalone with ID function, if it is connected with an external ID card reader, the distance between the Access Standalone and the card reader must be larger than 10 cm. Otherwise, the card reader might malfunction because it is too close to the Access Standalone.

2.5.2 Fingerprint

Press your enrolled fingerprint on the fingerprint scanner to unlock the door.

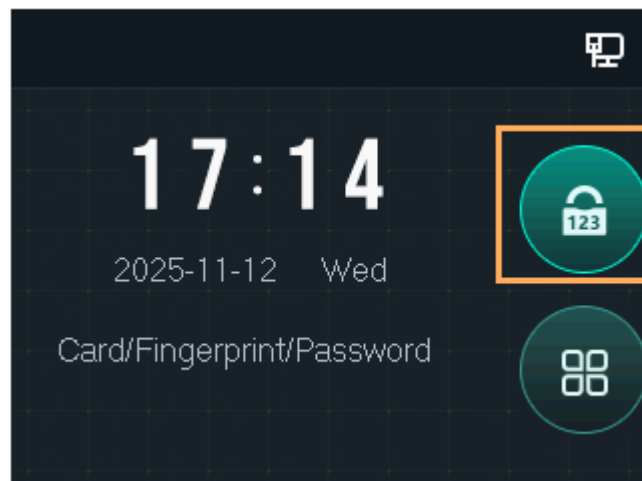
2.5.3 User Password

Enter the user ID and password to unlock the door.

Procedure

Step 1 Press $\wedge$ and $\vee$ on the main screen, select , and then press **OK**.

Figure 2-7 Main screen



Step 2 Select **Unlock by Password**, and then press **OK**.

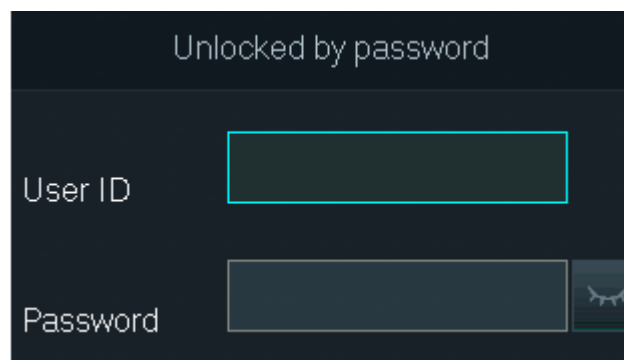
Step 3 Enter the user ID and password.



- To enter the user ID, you need to select the input box of user ID and then press **OK**.
- You can directly enter the password on the keypad.
- Press  to change the input method.

Step 4 Select **OK**, and then press **OK**.

Figure 2-8 Unlock by user password



2.5.4 Public Password

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

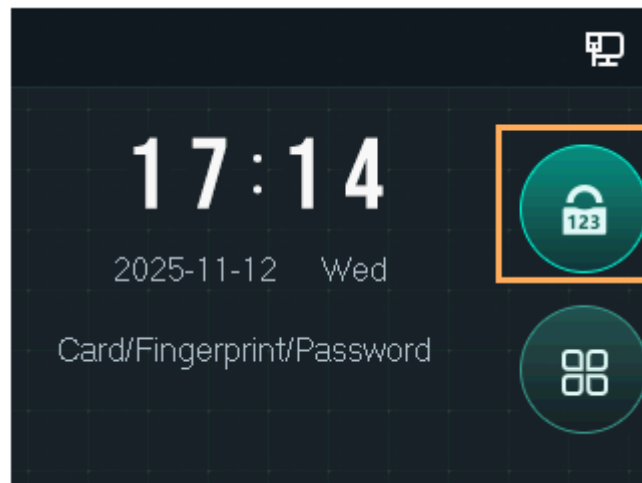
Background Information

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

Procedure

Step 1 Press $\wedge$ and $\vee$ on the main screen, select , and then press **OK**.

Figure 2-9 Main screen



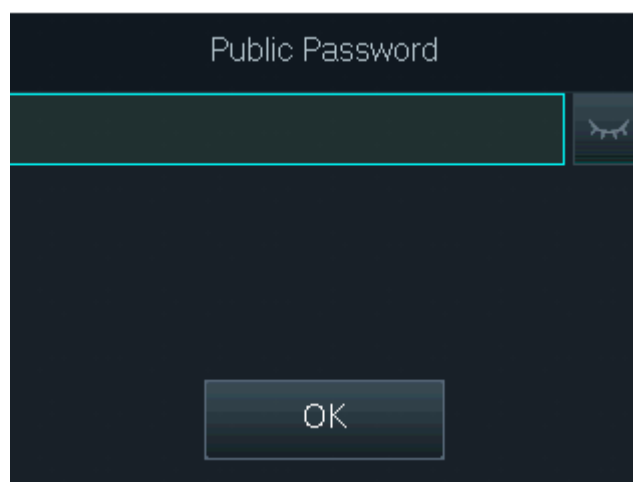
Step 2 Select **Unlock by Public Password**, and then press **OK**.

Step 3 Enter the public password, select **OK**, and then press **OK**.



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

Figure 2-10 Unlock by public password



2.5.5 Temporary Password

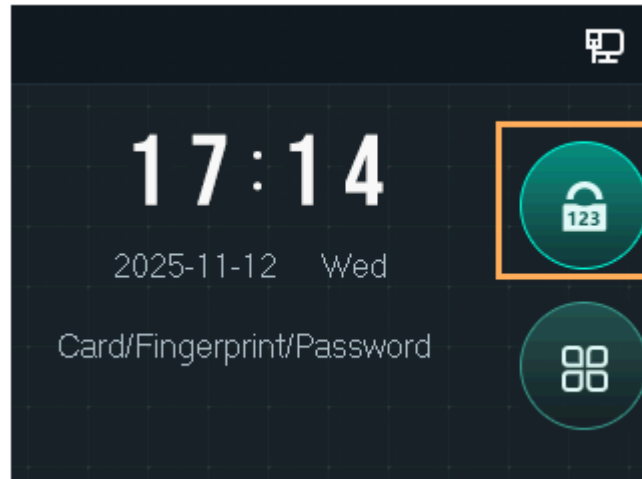
Prerequisites

You have obtained the temporary password issued from DMSS app.

Procedure

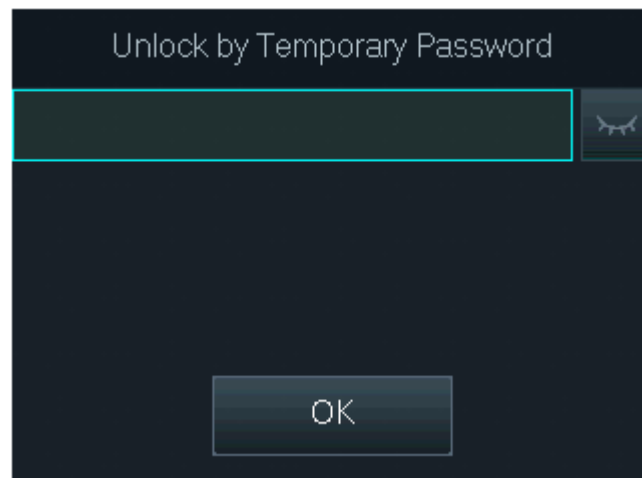
- Step 1 Press $\wedge$ and $\vee$ on the main screen, select , and then press **OK**.

Figure 2-11 Main screen



- Step 2 Select **Unlock by Temporary Password**, and then press **OK**.
Step 3 Enter the temporary password, select **OK**, and then press **OK**.

Figure 2-12 Unlock by temporary password



2.6 Person Management

You can add new users, view the user list or admin list on the **User** screen.

2.6.1 Adding New User

Procedure

- Step 1 On the standby screen, press $\wedge$ / $\vee$ to navigate to , and then press **OK**.
Step 2 Log in with the administrator account, and then select **Users** > **Create User**.



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

Figure 2-13 Create users

Create User(1/4)	Create User(2/4)
ID 2	Fingerprint 0
Name	Card 0
Verification Mode Same as Device	Password
Unlock Method Card/Fingerprint/Password	User Permission User >

Create User(3/4)	Create User(4/4)
General Plan 255-Default	Department 1-Default
Holiday Plan 255-Default	Schedule Mode Dept Schedule
Validity Period Forever	Permission Type Unlock and Attendance
User Type General User >	

Step 3 Configure the parameters.

Table 2-4 Description of user parameters

Parameter	Description
ID	Each user ID is unique. It can be 18 characters of numbers, letters, or their combination.
Name	Enter the name (a maximum of 32 characters, including numbers, symbols, and letters).
Fingerprint	Each user can add up to 3 fingerprints. Follow the on-screen prompts and voice prompts to add fingerprints. You can enable the duress fingerprint function under each fingerprint. After the duress alarm function is enabled, an alarm will be triggered if the door is unlocked by the duress fingerprint.  • We do not recommend setting the first fingerprint as the duress fingerprint. • Only certain models support the fingerprint function.

Parameter	Description
Card	You can register five cards for each user. On the card registration page, swipe your card on the card reader, and then the card information will be read by the Device. You can enable the duress card function on the card registration page. After the duress alarm function is enabled, an alarm will be triggered if the door is unlocked by the duress card.
Password	Enter the user password. The maximum length of the password is 8 digits. The duress password is adding 1 based on the last digit of the unlock password. For example, if the user password is 12345, the duress password will be 12346; if the user password is 789, and then the duress password is 780. A duress alarm will be triggered when a duress password is used to unlock the door.
Permission Type	You can select a user permission for the new user. • Normal users only have door unlock permission. • Administrators can configure the Device and unlock the door.
General Plan	A user can only have door access within the defined period. The default value is 255, which means no period is configured.
Holiday Plan	A user can only have door access within the scheduled holidays. The default value is 255, which means no holiday plan is configured.
Valid Period	Define a period during which the user has door access control.
User Type	• General: General users can unlock the door normally. • Blocklist: When users in the blocklist unlock the door, service personnel receive a notification. • Guest: Guests can unlock the door within a defined period or for a certain number of times. After the defined period expires or the unlocking times runs out, they cannot unlock the door. • Patrol: Paroling users can have their attendance tracked, but they have no unlocking permissions. • VIP: When VIP unlock the door, they are not restricted by unlock modes, such as Multi-card and Time Section. • Others: When they unlock the door, the door will stay unlocked for 5 more seconds. • Custom User 1/2: Same as General.

Step 4 Press **Esc**, and then press **OK** to save the settings.

2.6.2 User/Admin List

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

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

Figure 2-14 User list

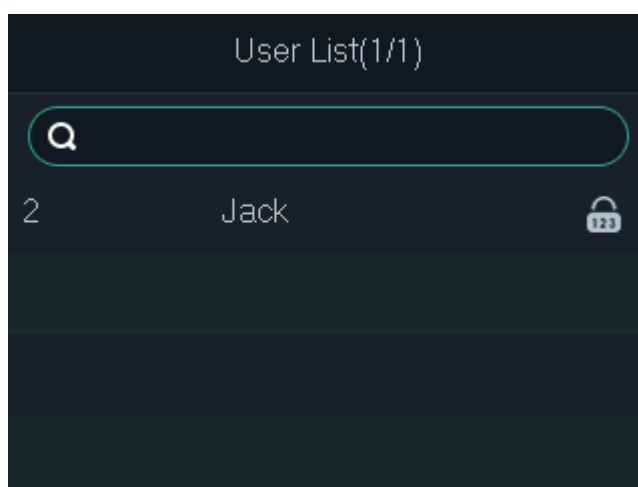
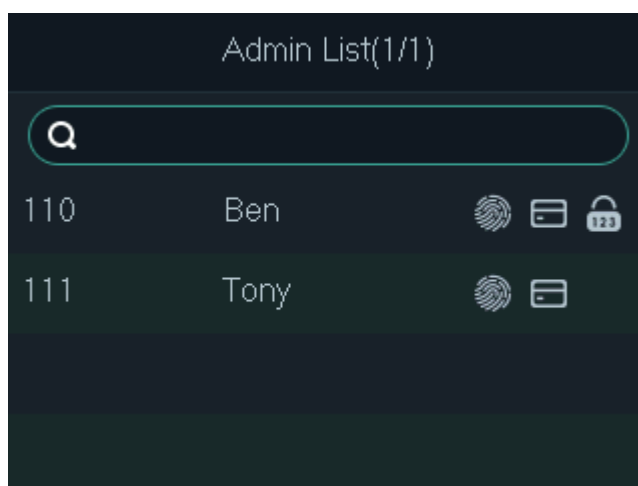


Figure 2-15 Admin list



Unlocking Method

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

Editing User Information

1. Select the user and press **OK**.
2. Edit the user information, and then press **Esc**.
3. Press **Esc** to save settings.

Searching for Users

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

Deleting Users

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

2.6.3 Configuring Public Password

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

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

Add Public Password

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

Enable Public Password

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

2.6.4 Deleting All Users

On the main menu, select **Users > Delete All Users**.

2.7 Access Control Management

2.7.1 Combination Unlock

Procedure

- Step 1 On the main menu, select **Access > Combination Unlock**, and then press **OK**.
- Step 2 Configure the unlocking combinations.
- Combination method: Select **Or** or **And**.
 - ◇ And: You have to verify all the selected unlocking methods to open the door.
 - ◇ Or: You can verify one of the selected unlocking methods to open the door.
 - Card: Unlock by card. Select **Yes** or **No**.



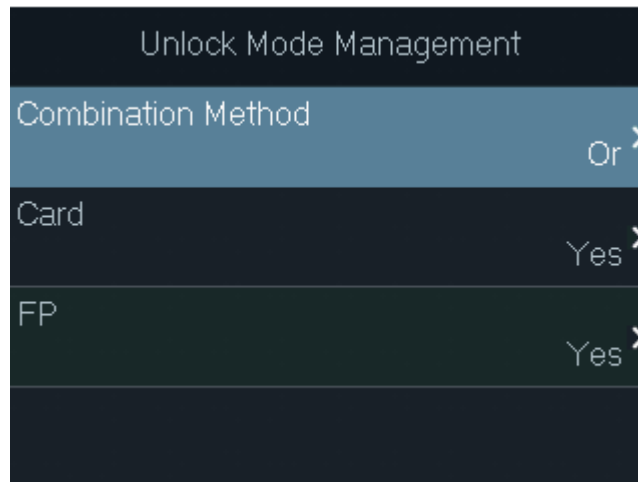
Only supported on select models.

- FP: Unlock by fingerprint. Select **Yes** or **No**.



Only supported on select models.

Figure 2-16 Unlock combination



2.7.2 Configuring Alarms

Configure access control alarms, and abnormal events can be sent to administrators timely.

Procedure

Step 1 On the main menu, select **Access** > **Alarm**, and then press **OK**.

Step 2 Enable the alarms according to your needs.

Figure 2-17 Alarm types

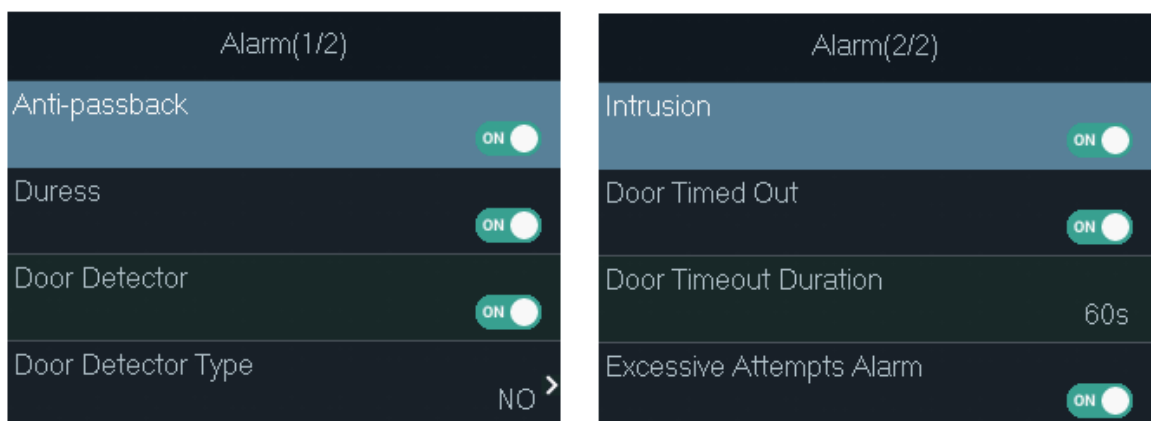


Table 2-5 Description of alarm types

Parameter	Description
Anti-passback	An alarm will be triggered when someone enter back again without being authorized.

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	When Door Detector is enabled, both Door Timed Out and Intrusion are be displayed.
Door Detector Type	Select the door detector type based on the connection: • NO : The door is considered open when the door detector signal line is broken (open circuit). • NC : The door is considered open when the door contact signal line is short-circuited (closed circuit).
Intrusion	When both the Door Detector and Intrusion are enabled, an intrusion alarm will be triggered upon abnormal door unlock.
Door Timed Out	When both the Door Detector and Door Timed Out are enabled, a timeout alarm will be triggered if the door remains open longer than the preset timeout duration.
Door Timed Out Duration	The door timeout duration can be configured within the range of 1 to 9999 seconds.
Excessive Attempts Alarm	If the password is entered incorrectly 5 times consecutively within 60 seconds or an unauthorized card is swiped 5 times consecutively, an excessive attempts alarm will be triggered.

2.7.3 Configuring Lock Status

Procedure

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

Step 2 Configure parameters.

Figure 2-18 Lock status

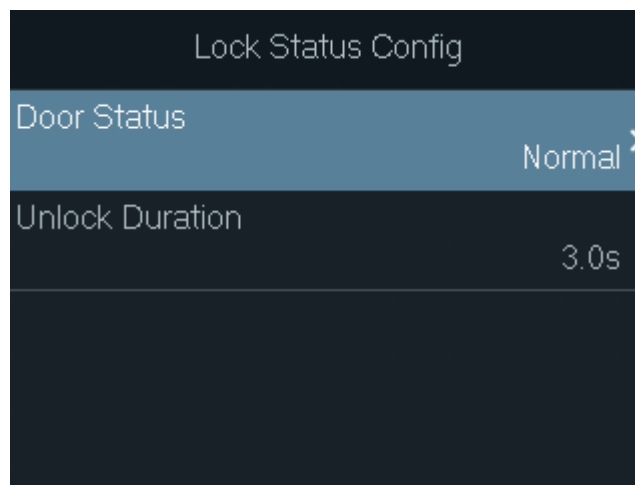


Table 2-6 Description of door status

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

2.7.4 Configuring Verification Intervals

Procedure

Step 1 On the main menu, select **Access > Verification Interval (Sec)**, and then press **OK**.

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

After the initial successful authentication for a person, their unlocking or attendance will be allowed, and corresponding records are generated. If the same person attempts to authenticate again within the set time, the door will not open or attendance be recorded, and no records will be generated. A secondary authentication must be performed after the interval time has elapsed.

2.7.5 Managing Main Cards

Adding Main Card

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

Deleting Main Card

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

Related Operations

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

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



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

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

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

2.7.6 Configuring PIN Code Authentication

Procedure

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

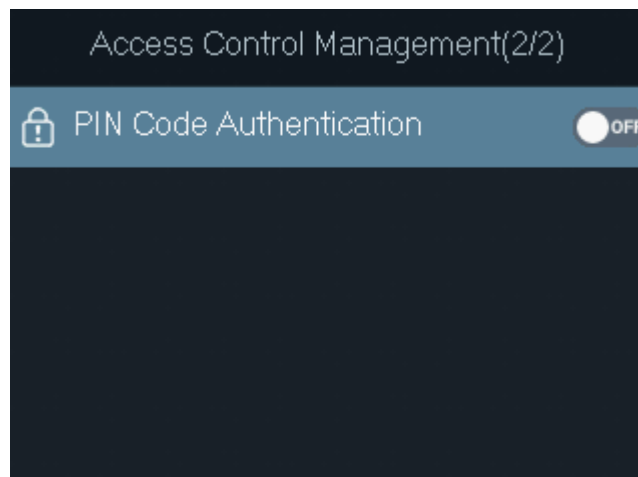
Step 2 Enable or turn off **PIN Code Authentication**.

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



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

Figure 2-19 PIN code



2.8 Attendance Management

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



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

2.9 Communication Settings

2.9.1 Configuring IP

Configure IP settings for the device.

Procedure

Step 1 On the main menu, select **Communication** > **IP Settings**, and then press **OK**.

Step 2 Configure parameters.

Figure 2-20 IP

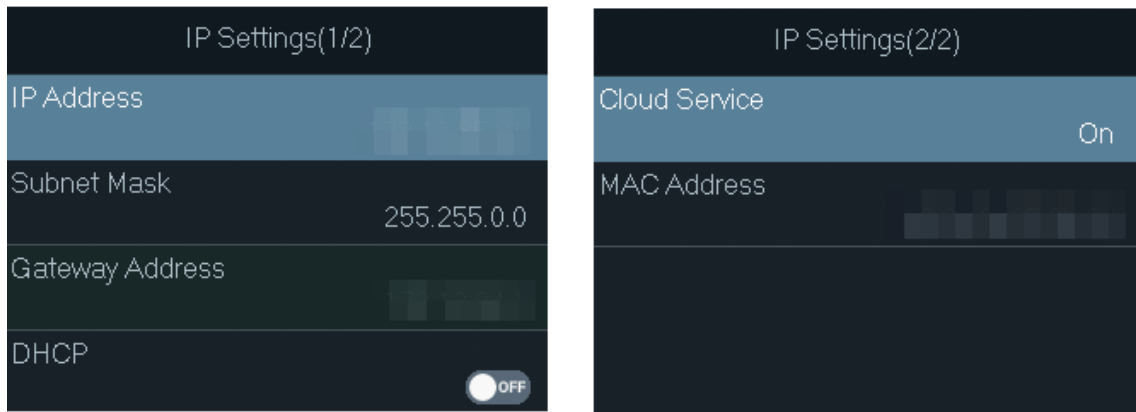


Table 2-7 Description of IP settings

Parameter	Description
IP Address	Enter the device IP address, subnet mask, gateway address and MAC address.
Subnet Mask	
Gateway Address	
MAC Address	
DHCP	Enable the DHCP (Dynamic Host Configuration Protocol) function to automatically obtain an IP address. In this case, the IP address, subnet mask, and gateway address cannot be set.
Cloud Service	Enable the function, and the device can connect to the cloud and be operated on the mobile app.

Step 3 Press **Esc** and then **OK** to save the settings.

2.9.2 Configuring Wi-Fi

Connect the device to the network through a wireless network



- Devices with a Wi-Fi module have this function.
- Wi-Fi AP and Wi-Fi functions are mutually exclusive.

Procedure

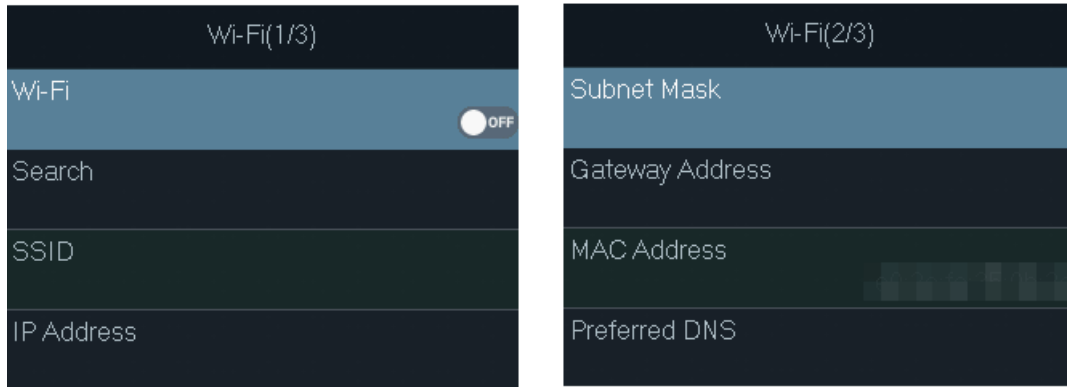
Step 1 On the main menu, select **Communication** > **Wi-Fi**, and then press **OK**.

Display the search results screen.



The function is ready for normal use in 1 minute.

Figure 2-21 Wi-Fi



Step 2 Select the searched Wi-Fi, and then press **OK**.

Step 3 Enter the Wi-Fi password, select **Connect**, and then press **OK**.

DHCP is enabled by default to automatically obtain an IP address. When DHCP is disabled, manual IP address entry is supported.

Step 4 (Optional) If no Wi-Fi is found, select **SSID**, and press **OK** to manually enter the Wi-Fi name.

Results

If both your mobile phone and the device are connected to the same Wi-Fi network. Enter the IP address displayed on the Wi-Fi screen into your phone browser to access the device.

2.9.3 Configuring Wi-Fi AP

Supports Wi-Fi AP. Once enabled, mobile devices can access the device through the AP.



- Devices with a Wi-Fi module have this function.
- Wi-Fi AP and Wi-Fi functions are mutually exclusive.

Uninitialized devices will automatically enable Wi-Fi AP upon first boot. The AP will automatically turn off if no client connects within 30 minutes.

Procedure

Step 1 On the main menu, select **Communication** > **Wi-Fi AP**, and then press **OK**.

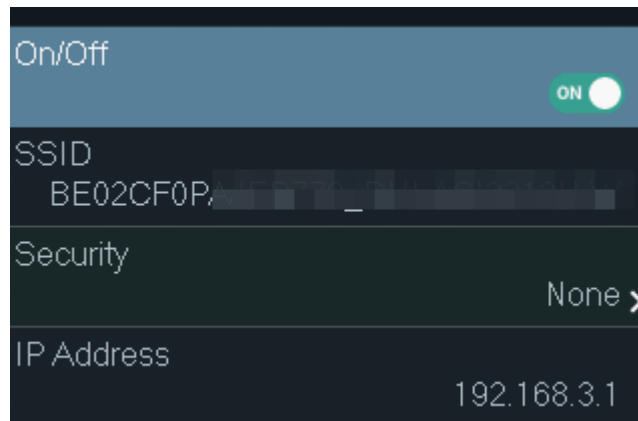
Step 2 Select **On/Off**, and then press **OK** to enable the function.

You can modify the SSID and Wi-Fi App password.



The function is ready for normal use in 1 minute.

Figure 2-22 Wi-Fi AP



Step 3 (Optional) Select **Security** to configure the Wi-Fi AP password.

The default value for **Security** is **None**. Enter the password to connect to the AP.

Results

When your phone connects to the device's AP, it will automatically redirect to the login page. Alternatively, you can manually enter the IP address displayed on the Wi-Fi AP screen (default IP: 192.168.3.1) in your browser to access the device.

2.9.4 Mode Settings

2.9.4.1 Controller Mode

The Device functions as an access controller, and connects to an external card reader, access controller or door control security module.

Procedure

Step 1 On the main menu, select **Communication** > **Mode Settings**, and then press **OK**.

Step 2 Set **Mode Settings** as **Access Controller**.

Step 3 Configure RS-485 and Wiegand settings.

- Select **RS-485 Settings**.

If you connect to other devices using the RS-485 port, configure the parameters.

Figure 2-23 Access controller

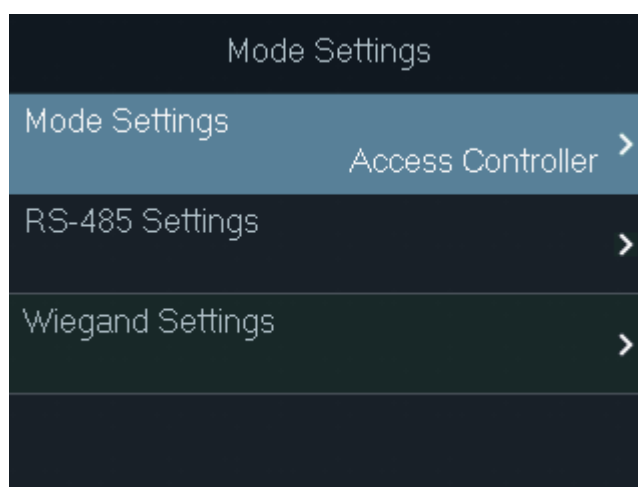


Table 2-8 Description of RS-485 parameters

Parameter	Description	Remark
Access Controller	Connects to other access controllers when the Device functions as a card reader, and sends data to other external access controllers to control access. ◇ ID: Outputs data based on the user ID. ◇ Card Number: Outputs data based on card number when users swipe card to unlock door; outputs data based on user's first card number when they use other unlock methods.	If the Device is connected to external access controller, when the people verify the identification on the Device, different permissions allow the people to control different doors. ◇ If the people have access permissions on the Device and the external access controller, the Device and the external access controller can be controlled. ◇ If the people only have access permissions on the Device, the external access controller cannot be controlled. ◇ If the people only have access permissions on the external access controller, the external access controller can be controlled.
Card Reader	The Device functions as an access controller, and connects to an external card reader.	—

Parameter	Description	Remark
Door Security Module	The door exit button, lock and fire linkage are not effective after the security module is enabled. ◇ Supports authentication through face, card, fingerprint, or password on this device to control the unlock of door security module. ◇ Supports authentication through external RS-485 card reader connected to the door control security module (by swiping a card) or through an external button to control the control the unlock of door security module.	
Lock Extension Module	The Device is connected to a door lock extension module. When Lock Extension Module is selected, the device's authentication only unlocks the local lock, while the external card reader's authentication unlocks the extension lock. After selection, in the Access Control Parameter and Alarm Config page, the door channel supports selecting Door 2, and relevant parameters for Door 2 can be configured.	
Reader (OSDP)	The Device connects to an OSDP protocol card reader, which sends access card information to the access controller or management platform.	

- Select **Wiegand Settings**.

- ◇ Wiegand Input: When connecting an external card reader device, select **Wiegand Input**.

Card No. Inversion: If the card number sequence obtained through Wiegand input does not match the actual card number sequence when interfacing with third-party devices, enable this function.

- ◇ Wiegand Output: When the Device functions as a card reader, and you need to connect it to another access controller, and select **Wiegand Output Config**.

Table 2-9 Description of Wiegand

Parameter	Description
Wiegand Output Type	The bit length of card numbers or ID that the device can recognize and output. ◇ Wiegand 26: Reads 3 bytes or 6 digits. ◇ Wiegand 34: Reads 4 bytes or 8 digits. ◇ Wiegand 66: Reads 8 bytes or 16 digits.
Pulse Width	Configure the pulse width and interval for wiegand output.

Parameter	Description
Pulse Interval	
Output Data Type	Select a Wiegand format to read card numbers or ID numbers. ◇ User ID: Outputs data based on user ID. ◇ Card: Outputs data based on user's first card number.
Wiegand Format	When Output Data Type is set as ID , you can select decimal or hexadecimal output formats.

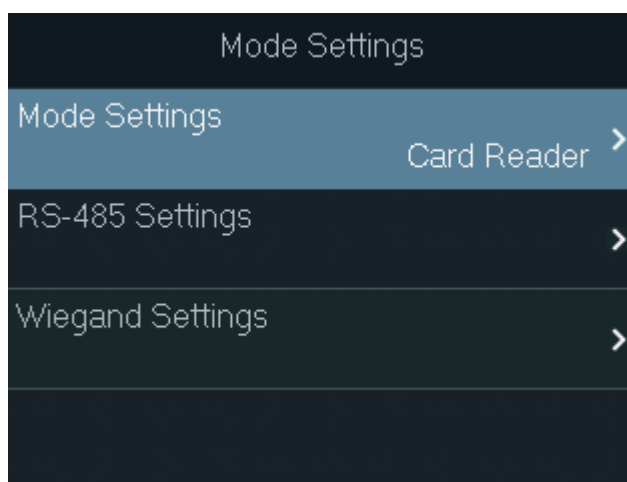
2.9.4.2 Card Reader Mode

When the device functions as a card reader connected to an external access controller, it does not perform authentication locally. Instead, it directly transmits access control data to the access controller, which then handles authentication and triggers the door unlock.

Procedure

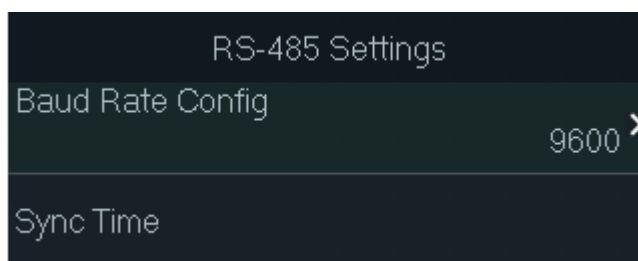
- Step 1 On the main menu, select **Communication** > **Mode Settings**, and then press **OK**.
- Step 2 Set **Mode Settings** as **Card Reader**.

Figure 2-24 Card reader mode



- Step 3 Configure RS-485 and Wiegand settings.
- Select **RS-485 Settings**.
 - ◇ Baud Rate Config: 9600 by default, which can be modified.
 - ◇ Sync Time: Adjust the time of the device based on the time of external controller. After connecting an external access controller (model H or J), synchronize this device's time based on the time of external controller.

Figure 2-25 RS-485

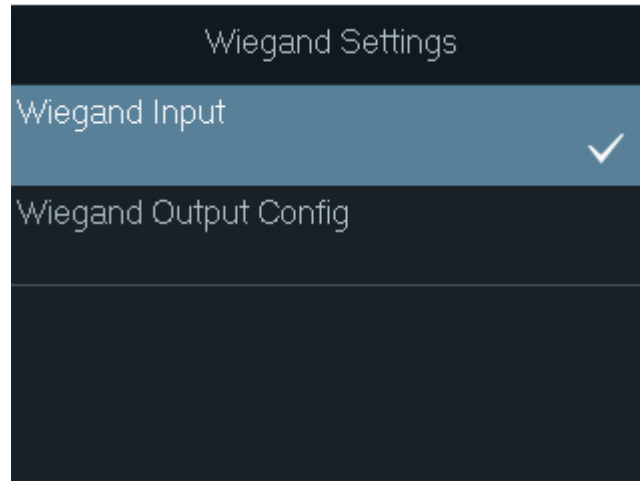


- Select **Wiegand Settings**.

The bit length of card numbers that the device can recognize and output.

- ◇ Wiegand 26: Reads 3 bytes or 6 digits.
- ◇ Wiegand 34: Reads 4 bytes or 8 digits.
- ◇ Wiegand 66: Reads 8 bytes or 16 digits.

Figure 2-26 Wiegand



2.10 System Settings

2.10.1 Configuring Time

Customize the system's time display and synchronization based on user preferences.

Procedure

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

Figure 2-27 time

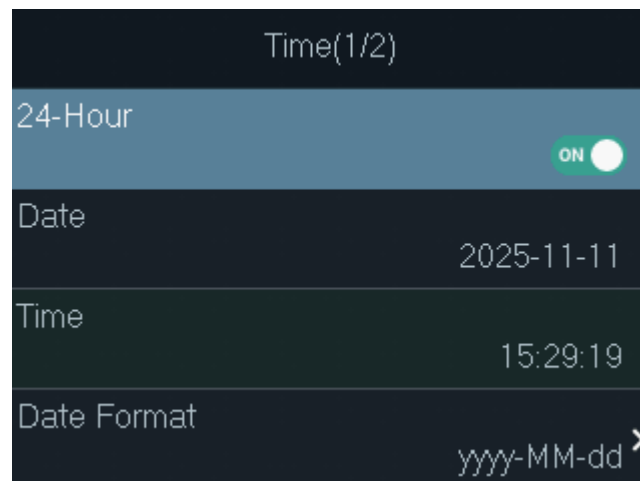


Table 2-10 Description of time parameter

Parameter	Description
24-Hour	Press < /> or OK to enable or turn off 24 hour format. When enabled, time will be displayed in 24-hour format; when turned off, time will be displayed in 12-hour format.
Date	1. Press ^ /V to select Date , and then press OK . 2. Enter the date, and then press OK .
Time	1. Press ^ /V to select Time , and then press OK . 2. Enter the time, and then press OK .
Date Format	1. Press ^ /V to select Date Format . 2. Press < /> or OK to select the format.
Time Zone	1. Press ^ /V to select Time Zone . 2. Press < /> or OK to select the time zone.

2.10.2 Configuring Volume

Procedure

Step 1 On the main menu, select **System** > **Volume**, and then press **OK**.

Step 2 Configure parameters.



The parameters might vary depending on device models.

Figure 2-28 Volume

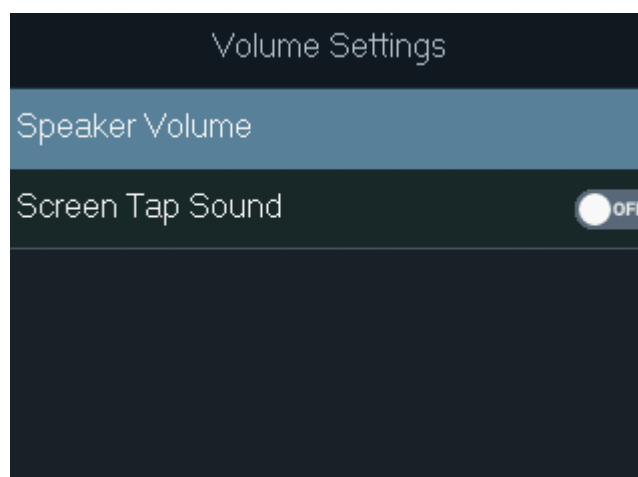


Table 2-11 Description of volume

Parameter	Description
Speaker Volume	Select Speaker Volume , press OK, and press $\wedge$, $\vee$, $>$, or $<$ to adjust volumes.  Only available on select models.
Screen Tap Sound	Enable it and there will be prompt time when pressing the keys.

2.10.3 Configuring Language

Procedure

- Step 1 On the main menu, select **System** > **Language**, and then press **OK**.
- Step 2 Select the language you need, and press **OK**.
- It is English by default.

2.10.4 Configuring Screen Parameters

Procedure

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

Figure 2-29 Screen settings

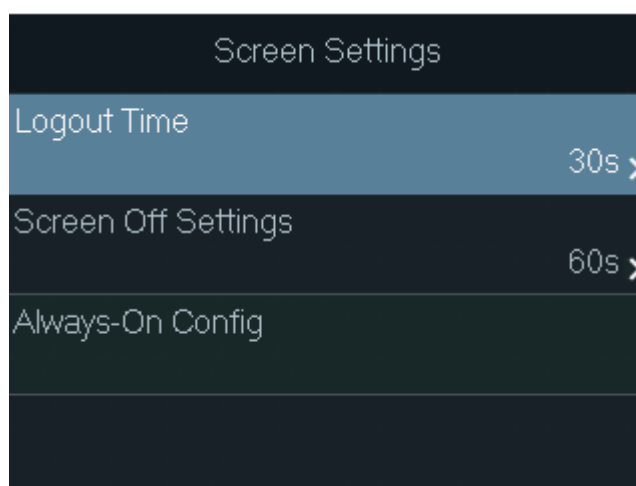


Figure 2-30 Always-on

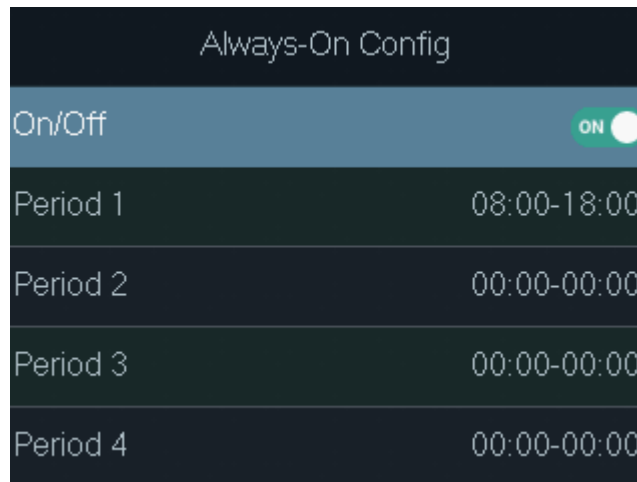


Table 2-12 Description of screen parameters

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

2.10.5 Configuring Card Settings

Background Information



Only devices with IC support this function.

Procedure

Step 1 On the main menu, select **System** > **Card Settings**, and then press **OK**.

Step 2 Configure parameters.

Figure 2-31 Card settings

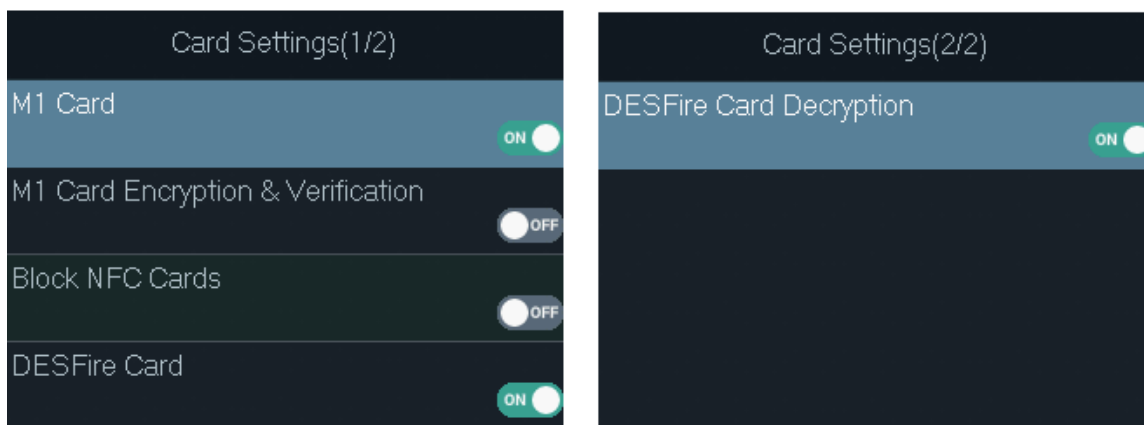


Table 2-13 Description of card parameters

Parameter	Description
M1 Card	
M1 Card Encryption & Verification	Only devices with IC support this function. Enable it and the device can read M1 card and ID serial number. It is enabled by default. Enable M1 Card Encryption & Verification after you have enabled M1 Card. Only supports reading M1 card.
Block NFC Cards	- Only devices with IC support this function. - Only certain phones support this function. After enabling the IC card, enable Block NFC Cards to prevent unauthorized access by blocking NFC-copied cards from opening doors.
DESFire Card	
DESFire Card Encryption	Only devices with IC support this function., and only hexadecimal card numbers are accepted. Enable the function, and the device can read the DESFire card's physical serial number (UID). After enabling the DESFire Card, enable DESFire Card Encryption, the device can read the contents of DESFire cards.

2.10.6 Managing Device Password

2.10.6.1 Changing Admin Password

Procedure

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

2.10.6.2 Modifying Reserved Email

Procedure

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

2.10.7 Restoring to Factory Defaults



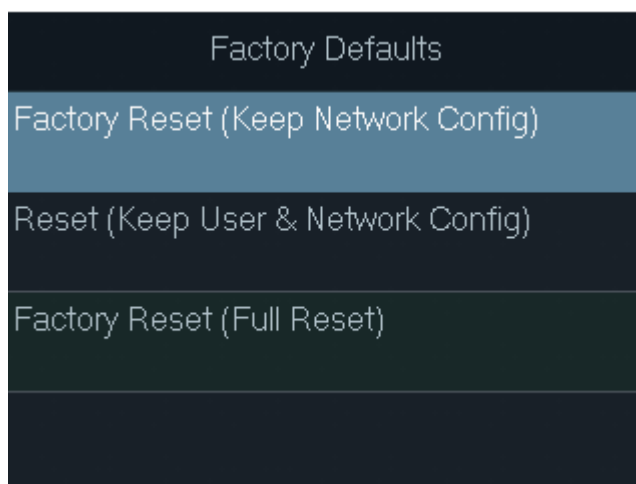
Restoring to factory defaults will result in data loss. Please proceed with caution.

Restoring Software Settings

On the main menu, select **System** > **Factory Defaults**, and then press **OK**.

- Factory Reset (Keep Network Config): Restores all settings to factory defaults except network configuration.
- Reset (Keep User & Network Config): Restores all settings to factory defaults except user data and network configuration.
- Factory Reset (Full Reset): All configurations and data will be reverted to factory defaults.

Figure 2-32 Factory defaults



Hardware Reset

The device supports factory reset through the tamper-proof button or reset pinhole (if available).

- Tamper-proof button: Within 5 minutes after the device starts up, press the tamper-proof button 5 times consecutively within 8 seconds. The standby interface will display a factory reset prompt; press **OK** or press and hold the tamper-proof button for seconds. After the device restarts, the reset will be successful. All configurations and information will be restored to factory settings.
- Reset pinhole: Within 5 minutes after the device starts up, short-circuit the reset hole.
 - ◇ Short-circuit for 500 milliseconds, the device emits a beep, then disconnect the short-circuit. After the device restarts, the reset will be successful. Except for user information, logs, and IP settings, all other configurations will be restored to factory settings.
 - ◇ Short-circuit for 5 seconds, the device emits a beep, then disconnect the short-circuit. After the device restarts, the reset will be successful. All configurations and information will be restored to factory settings.



Only some devices have a reset pinhole.

2.10.8 Resetting Device

On the main menu, select **System** > **Reset**, and then press **OK**.

2.11 USB Management

2.11.1 Exporting Data

After inserting the USB drive, export the data from the device to the USB drive. Some exported data is encrypted and cannot be edited.

Prerequisites

The USB drive has been inserted into the device and is properly recognized.



The supported formats for the USB drive are FAT32, with a capacity ranging from 4 GB to 128 GB.

Procedure

Step 1 On the main menu, select **USB** > **USB Export**, and then press **OK**.

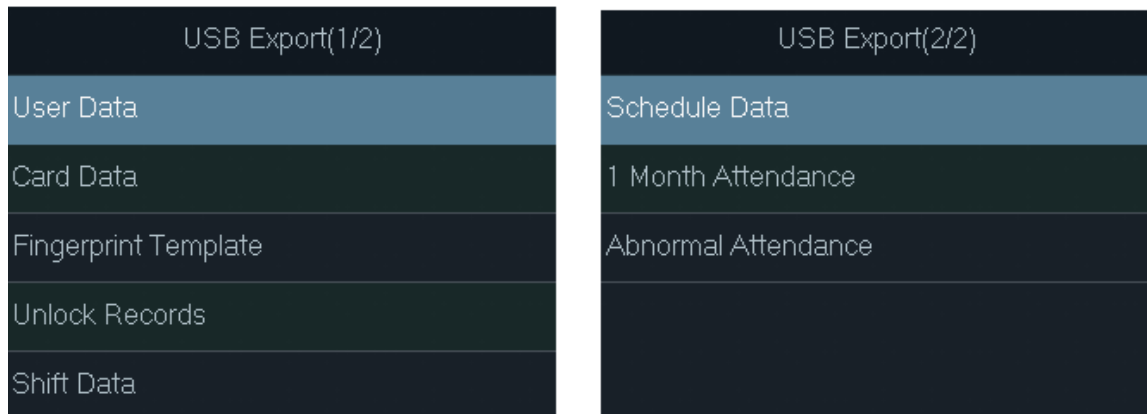
Step 2 Select the data type that needs to be exported, and then press **OK**.

The exported information will be saved to the USB drive.



- When the exported data is in Excel format, it can be edited
- User data, card data, and fingerprint data are exported as encrypted.

Figure 2-33 USB export



2.11.2 Importing Data

Only data exported from one device can be imported into another device.

Prerequisites

The USB drive has been inserted and is properly recognized by the device.

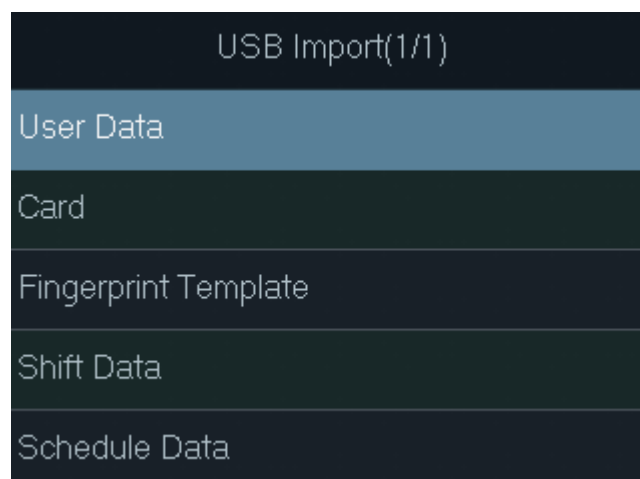
Procedure

- Step 1 On the main menu, select **USB** > **USB Import**, and then press **OK**.
Step 2 Select the data type that needs to be imported, and then press **OK**



It is recommended that you import data between devices of the same model and version. Importing data between different models or versions may result in data loss.

Figure 2-34 USB import



2.11.3 Updating Device

Perform system upgrades through a USB drive.



For new devices or after a factory reset, the system files are backed up within the first 10 minutes of startup. Upgrading during this time is not recommended.

Procedure

- Step 1 Rename the update file as **update.bin**, and save it to the root directory of the USB drive. Insert the USB drive to the device.
- Step 2 Log in to the main menu of the device.
- Step 3 Select **USB > USB Update**, and then press **OK**.
Screen displays confirmation prompt.
- Step 4 Press **OK** to update.
The system upgrade has started. The device will automatically restart once the upgrade is complete.

2.12 Records Management

On the main menu, select **Records** , and then press **OK** to view the unlock records.

Figure 2-35 Unlock records

Unlock Records		
ID	Time	Results
	11-07 11:09	Failed

2.13 Viewing Information

2.13.1 Viewing Data Capacity

On the main menu, select **Info > Data Capacity**, and then press **OK** to view data capacity, such as user, card, fingerprint capacity of the device.

2.13.2 Viewing Device Version

登 On the main menu, select **Info** > **Data Capacity**, and then press **OK** to view device SN, MAC address, software version and other information.

- Select **SN** , press **OK**. The QR code is displayed and scan it with the mobile app to add the device.
- Select **Documentation QR** , press **OK**. The QR code is displayed and scan it to view the user manual.



Only supported on select models.

3 Local Operations (Touchscreen Models)

- Configurations might differ depending on the actual product.
- External expansion modules are only available on select models.
- You might see some UI texts are not displayed because of the limited space. Press and hold the text for 3 seconds and it will show.

3.1 Initialization

For first-time use or after restoring factory defaults, you need to set a password and associate your email address for the admin account. You also need to set the time zone of the Device. You can use the admin account to log in to the main menu of the Device, configure the Device, and log in to the web browser and SmartPSS Lite.



- If you forget the administrator password, send a reset request to your reserved Email address.
- 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.

3.2 Appearance

The device is a touchscreen model that requires operation on the screen.

Figure 3-1 Appearance



3.3 Main Screen

You can unlock the door through cards, passwords, fingerprint, Bluetooth (some unlocking methods are available only on select models). Unlock methods might differ depending on the models of the product.

You can only modify the theme of the main screen through the webpage of the Device. This section uses the general mode as the example.



This manual is for reference only. Slight differences might be found between the main screen in this manual and the actual device.

Figure 3-2 Main screen

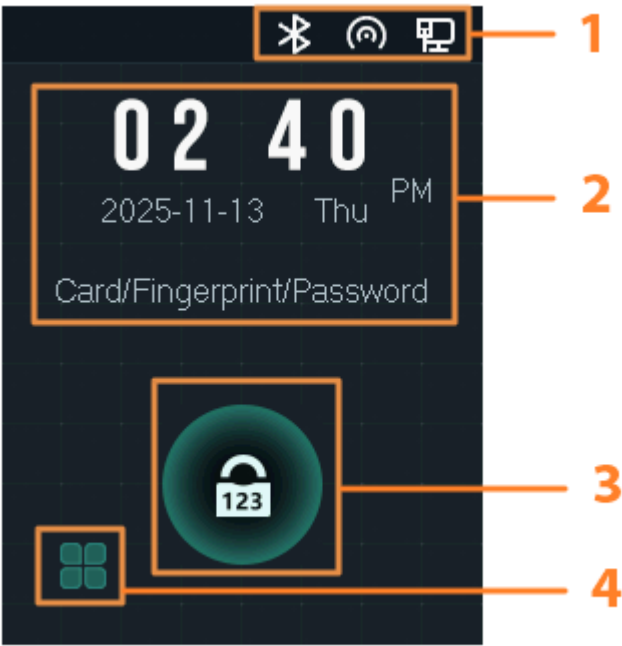


Table 3-1 Description of main screen

No.	Description
1	Displays the connection status of Wi-Fi, Wi-Fi AP, wired network, USB drive, and Bluetooth.  Only certain models support Wi-Fi and Wi-Fi AP.
1	Display the current date, time, day of the week, and unlocking method.
3	Unlock by password. Supports user password, temporary password, or public password.
4	Main menu. Select the verification method to go to the main menu.

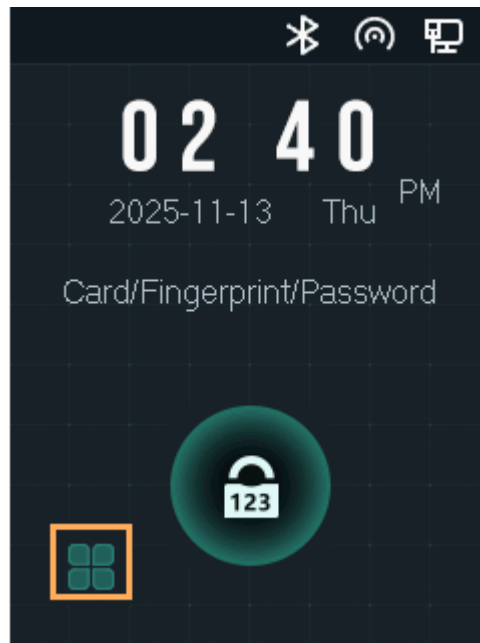
3.4 Logging In to the Main Menu

Log in to the main menu to configure the Device. Only admin account and administrator account can enter the main menu of the Device. For the first-time use, use the admin account to enter the main menu screen and then you can create the other administrator accounts.

Procedure

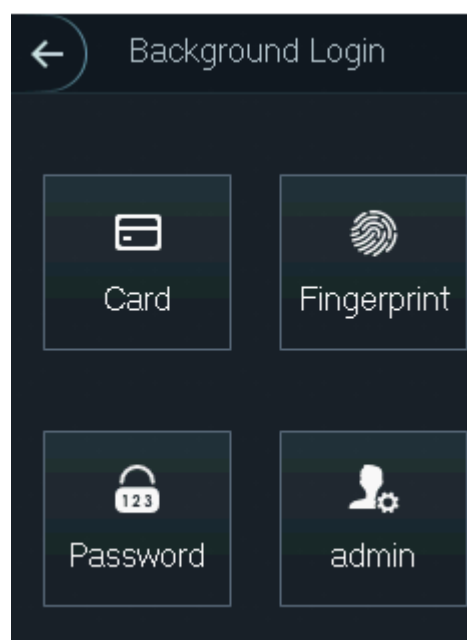
Step 1 On the standby screen, tap .

Figure 3-3 Standby screen



Step 2 Select verification methods.

Figure 3-4 Verification methods



- Fingerprint: After successfully recognizing the administrator's fingerprint, you can go to the main menu.



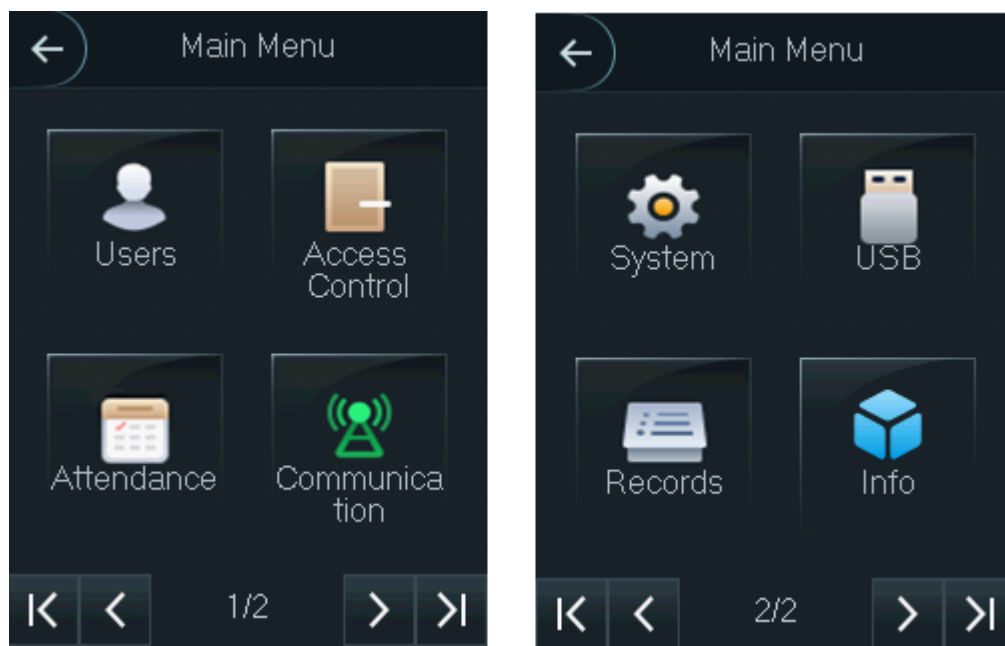
Only supported on select models.

- Card swipe: After successfully recognizing the administrator's card, you can go to the main menu.
- Password: Enter the administrator's ID and password to go to the main menu.
- Admin: Enter the admin password to go to the main menu.

Results

After successful authentication, you can go to the device's main menu.

Figure 3-5 Main menu



3.5 Resetting the Password

If the login password for the admin user is forgotten, the password can be reset through the following two methods.

You Have Configured Reserved Email Address

1. Press and hold the standby screen for 1.5 seconds.
2. Tap **admin**, and then tap once on the blank area of the screen.
3. Click **Forgot password**.
4. Read the on-screen prompt, and then click **Enter**.
5. Tap **QR Code**, and then scan the QR code.
6. Send the scanning results to the designated email address.
7. Enter the security code.



If the wrong security code is entered 5 times in a row, the administrator account will be frozen for 5 minutes.

8. Click **Next**.
9. Reset and confirm the password.



The password must 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 ' " ; : &).

10. Click **OK**.

You Have Not Configured Reserved Email Address

1. Press and hold the standby screen for 1.5 seconds.
2. Tap **admin**, and then tap once on the blank area of the screen.
3. Click **Forgot password**.
4. Follow the on-screen prompt to contact the local leader or technical support or help.

3.6 Unlock Methods

3.6.1 Card

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



This function is only available on select models.

3.6.2 Fingerprint

Place your finger on the fingerprint scanner.



This function is only available on select models.

3.6.3 Bluetooth

You can unlock the door by the Bluetooth through the DMSS app.



This function is only available on select models.

Prepare the following things.

- The Bluetooth has been enabled. For details, see "3.10.4 Configuring Bluetooth".
- The Device has been added to the DMSS app. For details, see the corresponding user manual.

Unlock the door through the DMSS app.

The voice prompt **Successfully unlocked** means that the door opens and you can enter.

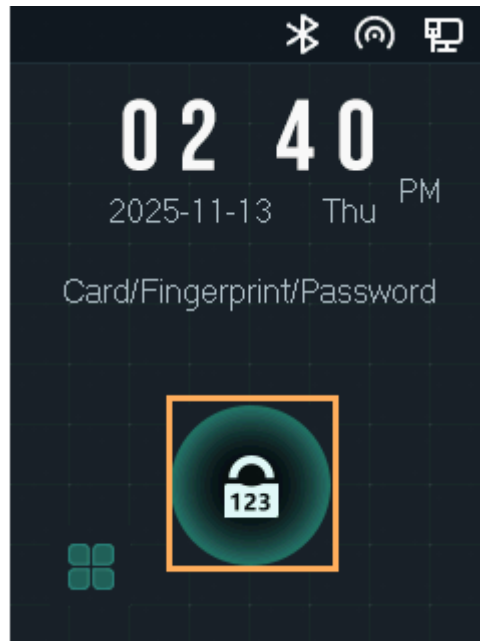
3.6.4 User Password

Enter the user ID and password to unlock the door.

Procedure

Step 1 Tap  on the main screen.

Figure 3-6 Main screen



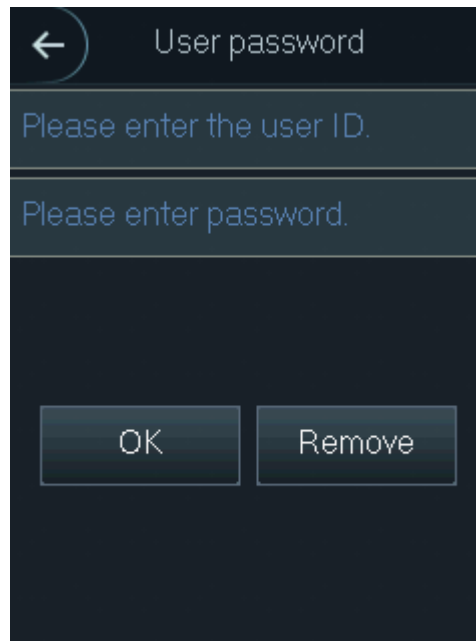
Step 2 Tap **User Password**.

Step 3 Enter the registered or issued user ID and password, and then tap **OK**.

After successful verification, the door can be opened.

If the **PIN Code Authentication** is enabled, you can enter the user password to unlock the door.

Figure 3-7 User password

A dark-themed mobile application screen titled "User password". At the top left is a back arrow icon. Below the title are two text input fields: the first is labeled "Please enter the user ID." and the second is labeled "Please enter password.". At the bottom of the screen are two buttons: "OK" and "Remove".

3.6.5 Public Password

Enter only the public password to unlock the door. The door can be unlocked through public password except for always closed door. One device allows for only one public password.

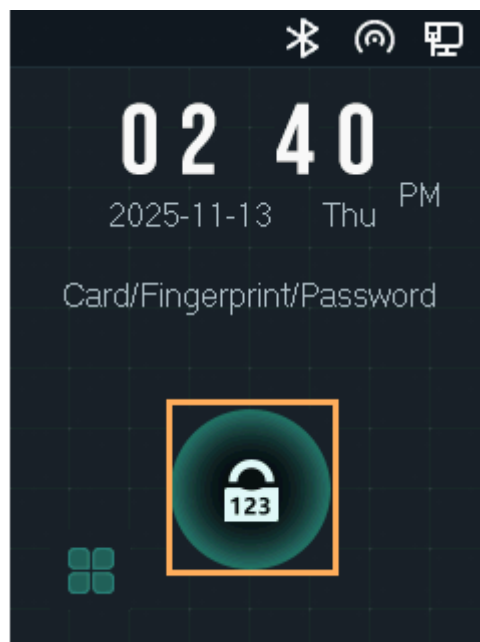
Prerequisites

The public password was configured. For details, see "3.7.3 Configuring Public Password".

Procedure

Step 1 Tap  on the main screen.

Figure 3-8 Main screen

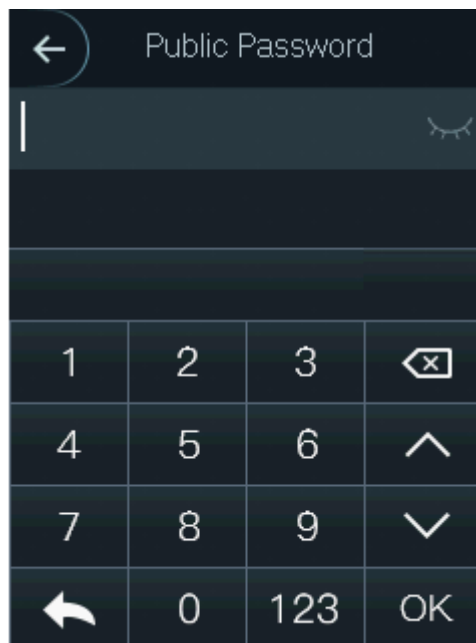


Step 2 Tap **Public Password**.

Step 3 Enter the public password, and then tap **OK**.

After successful verification , the door can be opened.

Figure 3-9 Public password



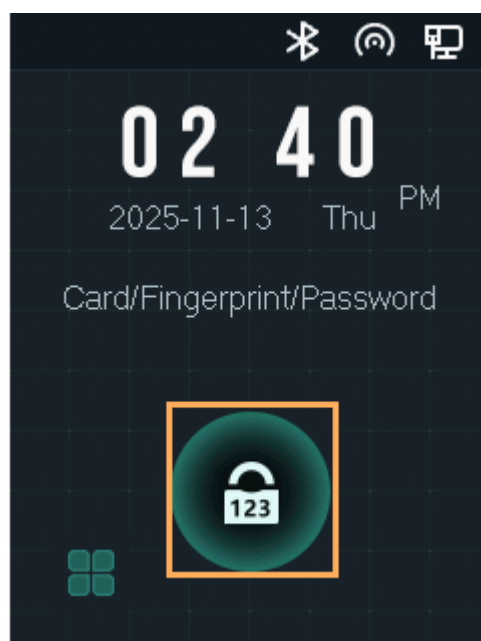
3.6.6 Temporary Password

Unlock the door by the temporary password.

Procedure

Step 1 Tap  on the main screen.

Figure 3-10 Main screen

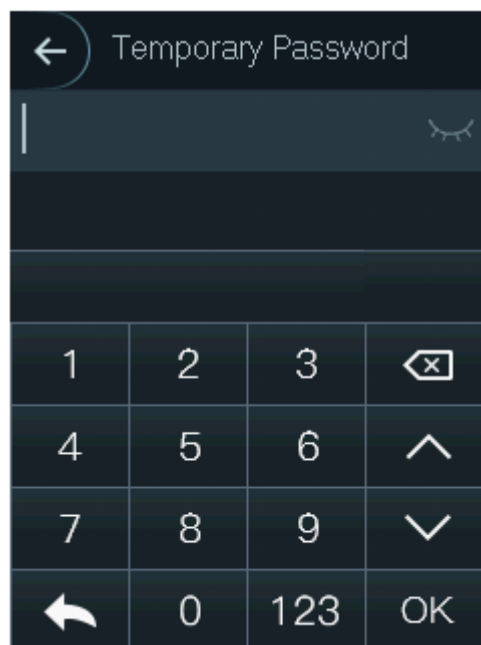


Step 2 Tap **Temporary Password**.

Step 3 Enter the temporary password, and then tap **OK**.

After successful verification, the door can be opened.

Figure 3-11 Temporary password



3.7 Person Management

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



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

3.7.1 Adding Users

Procedure

Step 1 Log in with the administrator account, and then select **Users** > **User List**.



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

Step 2 Tap  at the top-right corner, and then configure user parameters.

Figure 3-12 Add users

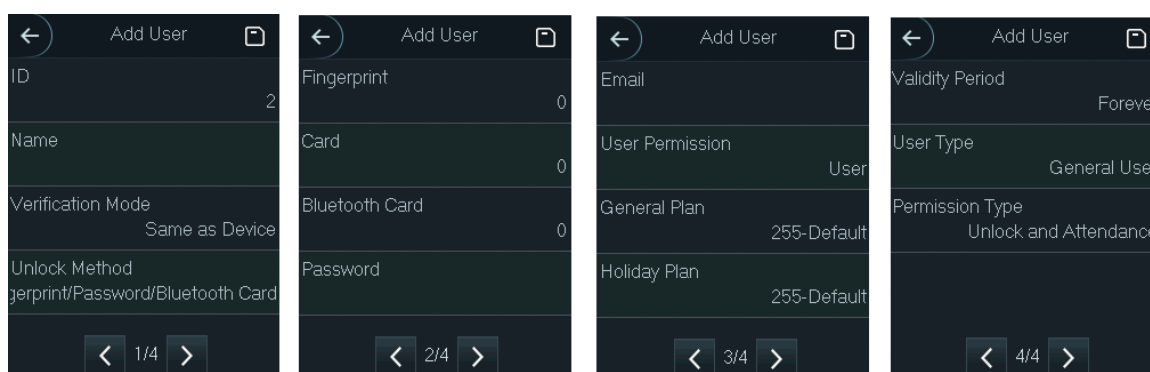


Table 3-2 Description of user parameters

Parameter	Description
ID	Each user ID is unique. It can be 18 characters of numbers, letters, or their combination.
Name	Enter the name (a maximum of 32 characters, including numbers, symbols, and letters).
Verification Mode	Supports configuring verification methods for each personnel.
Unlock Method	- Same as Device: The personnel will use the device's configured verification method for authentication. - Custom: The personnel will be authenticated using the custom methods. Select Custom , and select Unlock Method, tap OK. Select Combinational Element and Combination Method.  - The custom unlock method only supports local device authentication and does not work with external card readers. - If the custom verification method conflicts with the device's default method, the custom configuration takes priority.
Fingerprint	Each user can add up to 3 fingerprints. Follow the on-screen prompts and voice prompts to add fingerprints. You can enable the duress fingerprint function under each fingerprint. After the duress alarm function is enabled, an alarm will be triggered if the door is unlocked by the duress fingerprint.  - We do not recommend setting the first fingerprint as the duress fingerprint. - Only certain models support the fingerprint function.
Card	You can register 5 cards for each user. On the card registration page, swipe your card on the card reader, and then the card information will be read by the Device. You can enable the duress card function on the card registration page. After the duress alarm function is enabled, an alarm will be triggered if the door is unlocked by the duress card.

Parameter	Description
Bluetooth Card	You can register 5 Bluetooth cards for each user. On the card registration page, select request through Email or registration code to register your Bluetooth card.
Password	Enter the user password. The maximum length of the password is 8 digits. The duress password is adding 1 based on the last digit of the unlock password. For example, if the user password is 12345, the duress password will be 12346; if the user password is 789, and then the duress password is 780. A duress alarm will be triggered when a duress password is used to unlock the door.
Email	Enter the email that is used for password reset.
Permission Type	You can select a user permission for the new user. • Normal users only have door unlock permission. • Administrators can configure the Device and unlock the door.
General Plan	A user can only have door access within the defined period. The default value is 255, which means no period is configured.
Holiday Plan	A user can only have door access within the scheduled holidays. The default value is 255, which means no holiday plan is configured.
Valid Period	Define a period during which the user has door access control.
User Type	• General: General users can unlock the door normally. • Blocklist: When users in the blocklist unlock the door, service personnel receive a notification. • Guest: Guests can unlock the door within a defined period or for a certain number of times. After the defined period expires or the unlocking times runs out, they cannot unlock the door. • Patrol: Patrolling users can have their attendance tracked, but they have no unlocking permissions. • VIP: When VIP unlock the door, they are not restricted by unlock modes, such as Multi-card and Time Section. • Others: When they unlock the door, the door will stay unlocked for 5 more seconds. • Custom User 1/2: Same as General.

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

3.7.2 Viewing User and Admin Information

Query users or administrators within the device, and modify or delete user information or administrator information.

- The user list is used to display all user information in the current device.
- The administrator list is used to display all administrator information in the current device.

Log in to the main menu of the device, select **Users > User List** or **Users > Admin List** to view the user or admin information.

- : Fingerprint.

- : Card.
- : Password.

Figure 3-13 User list

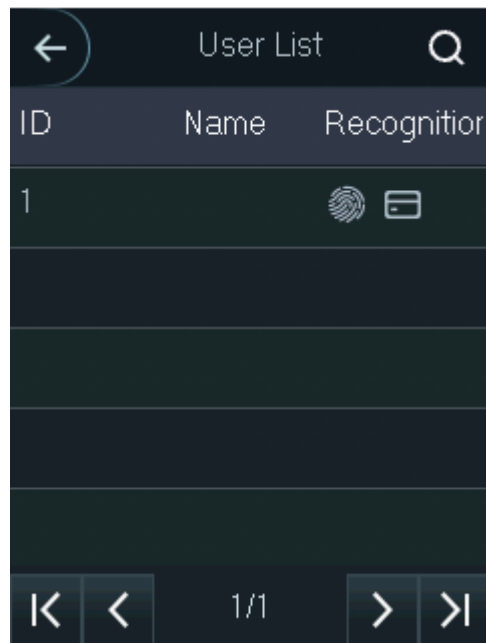
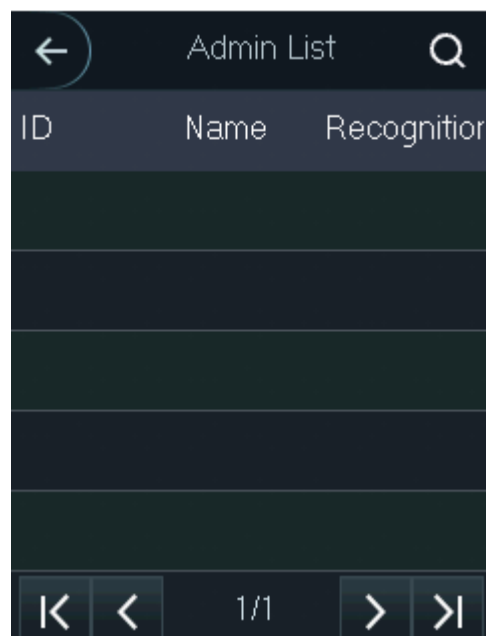


Figure 3-14 Admin list



- Modify user information. Click the user or administrator you want to modify, modify the information, and then tap .
- Search for users. Tap , enter the user ID to search for users.
- Delete users.

- ◇ Delete one by one: In the user list or admin list, tap  at the top-right corner, and then tap **OK**.
- ◇ Delete all users: On the **Users** screen, tap **Delete All Users**, and then tap **OK**.

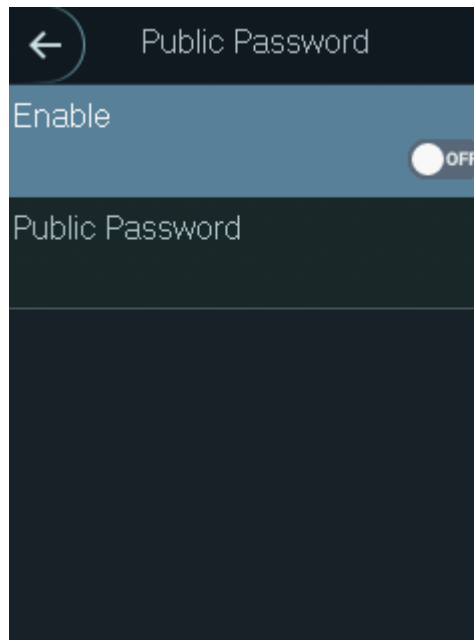
3.7.3 Configuring Public Password

When using the public password, there is no need to enter a user ID, and it is not restricted by user type. Only one public password can be configured per device.

Procedure

- Step 1 Log in to the main menu.
- Step 2 Select **Users** > **Public Password**.
- Step 3 Enable the function, tap **Public Password** to enter the password, and then tap **OK**.

Figure 3-15 Public password



3.8 Access Control Management

You can configure settings for doors such as the unlock method, alarm, door status unlock duration and other parameters. The available unlock modes might differ depending on the product model.

On the main menu, tap **Access Control** to go to the **Access Control Management** screen.

3.8.1 Configuring Unlock Method

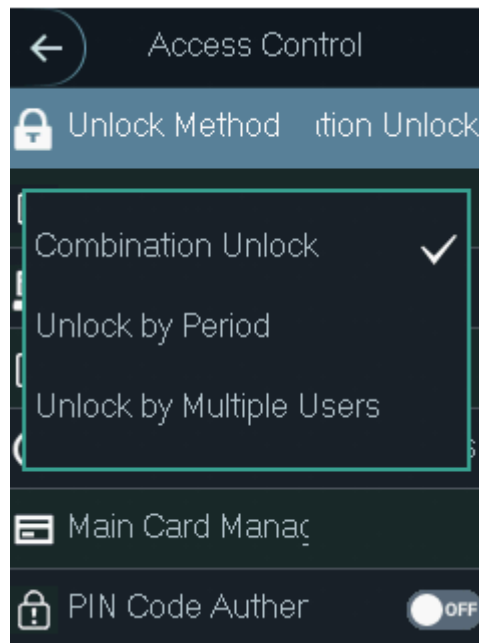
3.8.1.1 Configuring Unlock Combinations

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

Procedure

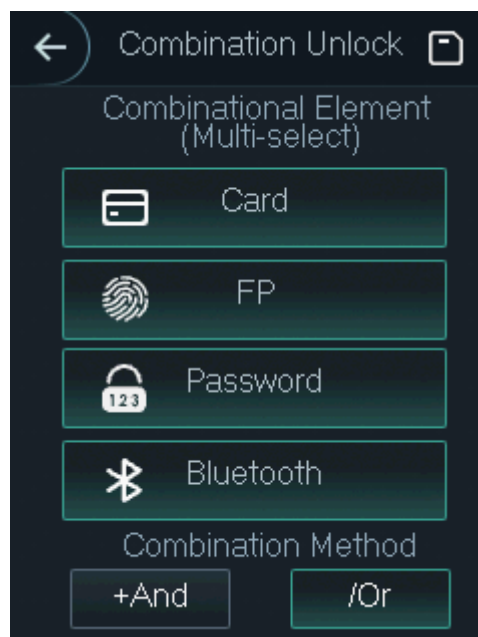
- Step 1 Log in to the main menu.
- Step 2 Select **Access Control** > **Unlock Method**.

Figure 3-16 Combination unlock



- Step 3 Tap **Combination Unlock**, and select unlock methods.

Figure 3-17 Combination unlock



- Step 4 Tap **+And** or **/Or** to configure combinations.
- To cancel your selection, tap the selected method again.

- **+And :**

Verify all the selected unlock methods to open the door.



People have to complete verification in the order of card, fingerprint, face and password.

- **/Or :** Verify one of the selected unlock methods to open the door.

Step 5 Tap  to save changes.

3.8.1.2 Configuring Unlock by Period

Procedure

Step 1 Select **Access Control**.

Step 2 Select **Access Control** > **Unlock Method**, and then select **Unlock by Period** from the list.

For details on how to configure unlock by period, see "4.7.1.2 Configuring Unlock Methods".

Step 3 Tap  to save changes.

3.8.1.3 Configuring Unlock by Multiple Users

Procedure

Step 1 Select **Access Control**.

Step 2 Select **Access Control** > **Unlock Method**, and then select **Unlock by Multiple Users** from the list.

For details on how to configure unlock by multiple users, see "4.7.1.2 Configuring Unlock Methods".

Step 3 Tap  to save changes.

3.8.2 Configuring Alarms

Configure access control alarms, and abnormal events can be sent to administrators timely.

Procedure

Step 1 On the main menu, select **Access Control** > **Alarm**.

Step 2 Enable the alarms according to your needs.

Figure 3-18 Alarm types

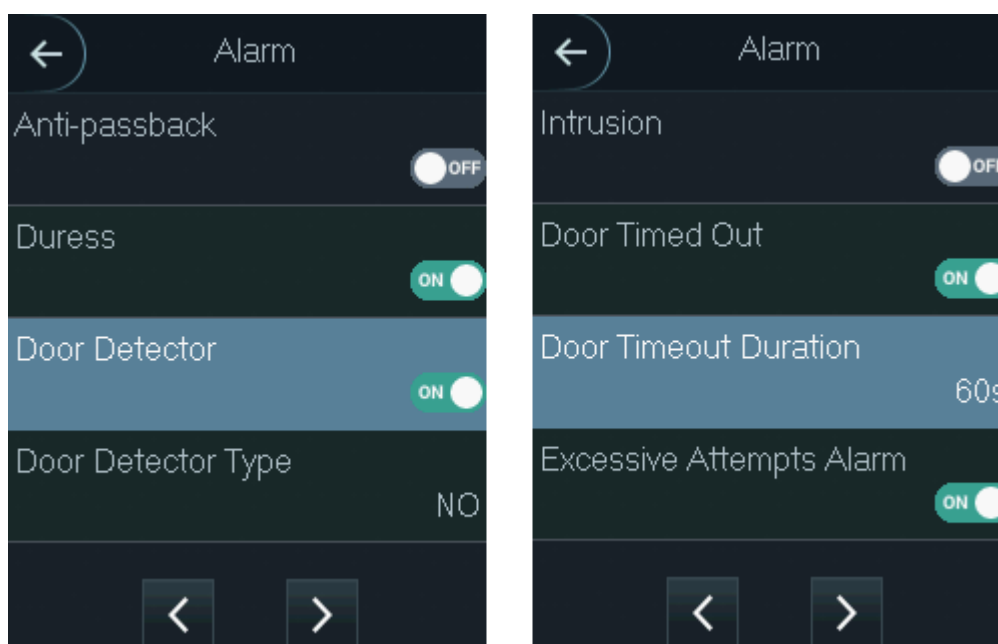


Table 3-3 Description of alarm types

Parameter	Description
Anti-passback	An alarm will be triggered when someone enter back again without being authorized.
Duress	An alarm will be triggered when a duress card, duress password or duress fingerprint is used to unlock the door.
Door Detector	When Door Detector is enabled, both Door Timed Out and Intrusion are be displayed.
Door Detector Type	Select the door detector type based on the connection: • NO : The door is considered open when the door detector signal line is broken (open circuit). • NC : The door is considered open when the door contact signal line is short-circuited (closed circuit).
Intrusion	When both the Door Detector and Intrusion are enabled, an intrusion alarm will be triggered upon abnormal door unlock.
Door Timed Out	When both the Door Detector and Door Timed Out are enabled, a timeout alarm will be triggered if the door remains open longer than the preset timeout duration.
Door Timed Out Duration	The door timeout duration can be configured within the range of 1 to 9999 seconds.
Excessive Attempts Alarm	If the password is entered incorrectly 5 times consecutively within 60 seconds or an unauthorized card is swiped 5 times consecutively, an excessive attempts alarm will be triggered.

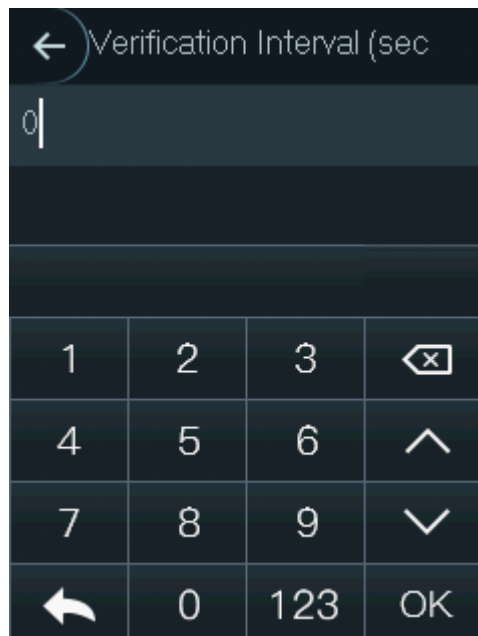
3.8.3 Configuring Verification Interval

If you verify your identity multiple times within a defined period, only the earliest verification will be considered valid, and the door will not open after the second or later verifications. Only after the configured period, you can verify the identity again.

Procedure

- Step 1 On the main menu, select **Access Control** > **Alarm**.
- Step 2 Tap **Verification Interval (sec)**, enter the time interval, and then tap **OK**.

Figure 3-19 Verification interval



3.8.4 Configuring the Lock Status

Procedure

- Step 1 On the main menu, select **Access Control** > **Door Status**.
- Step 2 Set door status.

Figure 3-20 Lock status

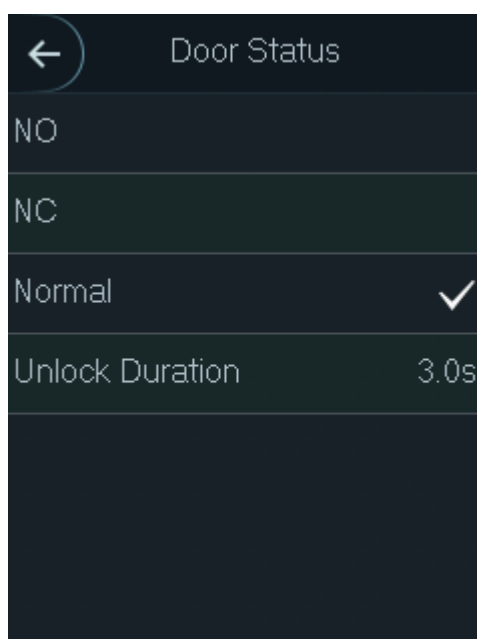


Table 3-4 Parameters description

Parameter	Description
Door Status	• 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.

3.8.5 Managing Main Cards

Adding Main Cards

Log in to the main menu, select **Access Control** > **Main Card Management** > **Add Main Card**, tap **General Card** and then swipe the card.

Deleting Main Cards

Log in to the main menu, select **Access Control** > **Main Card Management** > **Delete Main Card**, and then tap **OK**.

Related Operations

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

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



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

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

3.8.6 Configuring PIN Code Authentication

Procedure

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

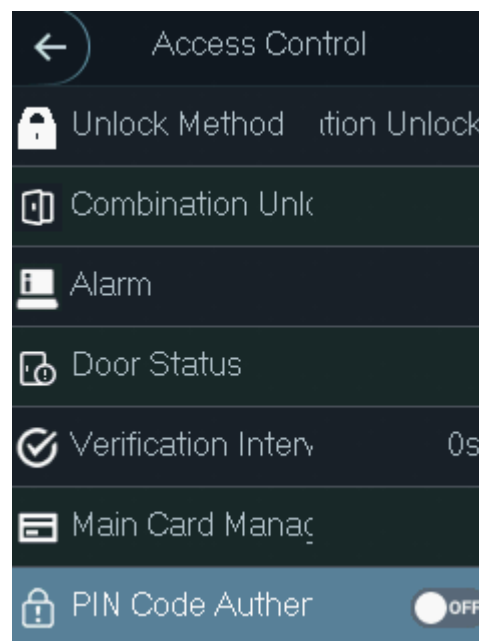
Step 2 Enable or turn off **PIN Code Authentication**.

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



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

Figure 3-21 PIN code authentication



3.9 Attendance Management

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



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

3.10 Communication Settings

Configure the network, RS-485 port and Wiegand port.



The RS-485 port and the Wiegand port might differ depending on the models of Device.

3.10.1 Configuring IP

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 > IP Settings**.
- Step 2 Set the IP address.

Figure 3-22 IP address

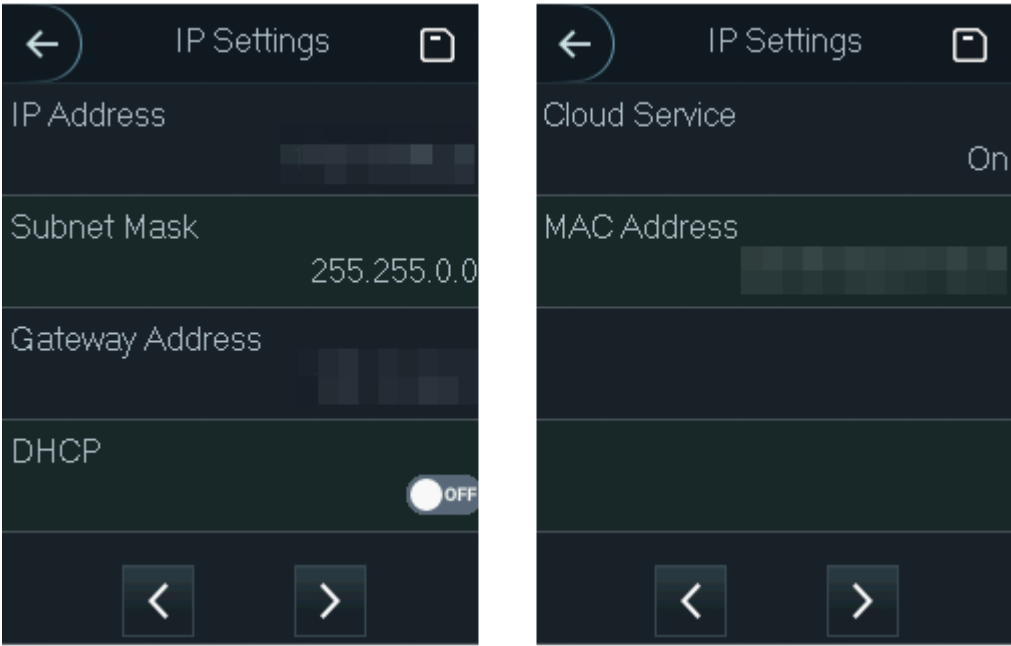


Table 3-5 Description of IP settings

Parameter	Description
IP Address	Enter the device IP address, subnet mask, gateway address and MAC address.
Subnet Mask	
Gateway Address	
MAC Address	
DHCP	Enable the DHCP (Dynamic Host Configuration Protocol) function to automatically obtain an IP address. In this case, the IP address, subnet mask, and gateway address cannot be set.
Cloud Service	Enable the function, and the device can connect to the cloud and be operated on the mobile app.

3.10.2 Configuring Wi-Fi

Connect the device to the network through a wireless network.



- Devices with a Wi-Fi module have this function.
- Wi-Fi AP and Wi-Fi functions are mutually exclusive.

Procedure

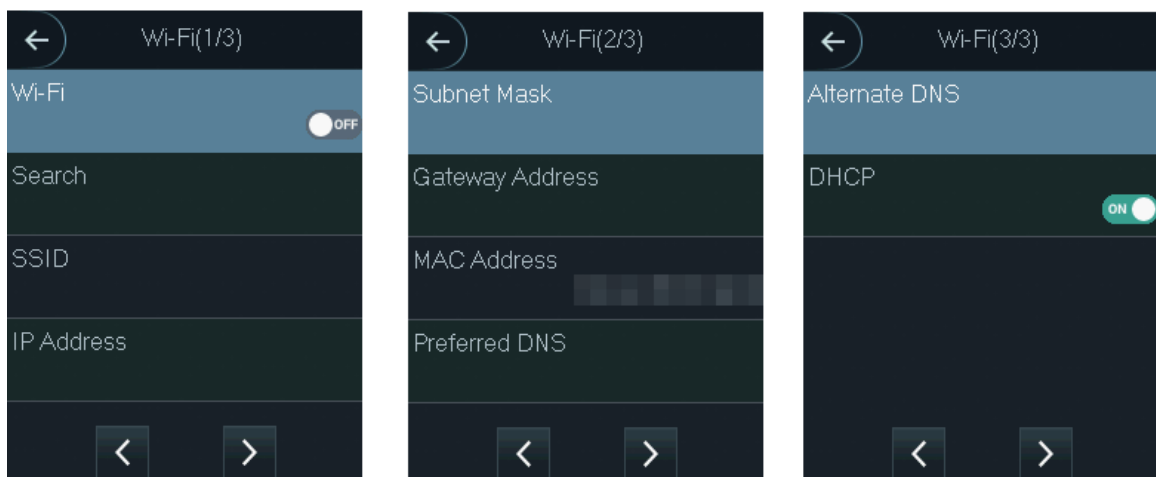
Step 1 On the main menu, select **Communication** > **Wi-Fi**.

Display the search results screen.



The function is ready for normal use in 1 minute.

Figure 3-23 Wi-Fi



Step 2 Select the searched Wi-Fi, and then press **OK**.

Step 3 Enter the Wi-Fi password, select **Connect**, and then tap **OK**.

DHCP is enabled by default to automatically obtain an IP address. When DHCP is disabled, manual IP address entry is supported.

Step 4 (Optional) If no Wi-Fi is found, select **SSID**, and tap **OK** to manually enter the Wi-Fi name.

Results

If both your mobile phone and the device are connected to the same Wi-Fi network. Enter the IP address displayed on the Wi-Fi screen into your phone browser to access the device.

3.10.3 Configuring Wi-Fi AP

Use your computer or your phone to connect to Wi-Fi AP of the Device to access its webpage. This function is only available on select models.

Procedure

Step 1 On the main menu, select **Communication** > **Wi-Fi AP**.

Step 2 Turn on Wi-Fi AP.

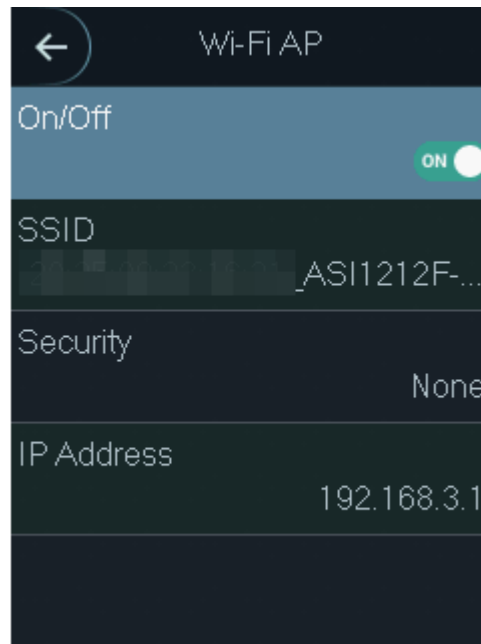
You can configure **Security** of the Wi-Fi AP.

Select **None** to directly connect to the Wi-Fi AP. Select **WPA2-Personal** to configure the password and connect to the Wi-Fi AP through the password.



- Wi-Fi AP and Wi-Fi function cannot be enabled at the same time.
- Every time you power on the Device, the Wi-Fi AP function will be automatically enabled for 30 minutes.

Figure 3-24 Connect to Wi-Fi AP



Results

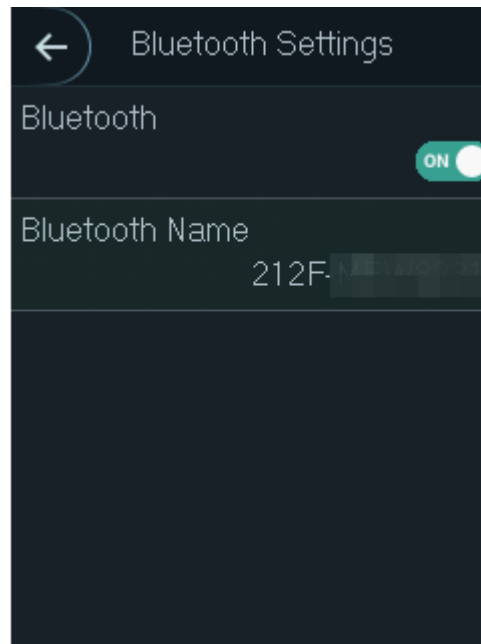
When your phone connects to the device's AP, it will automatically redirect to the login page. Alternatively, you can manually enter the IP address displayed on the Wi-Fi AP screen (default IP: 192.168.3.1) in your browser to access the device.

3.10.4 Configuring Bluetooth

Procedure

- Step 1 On the main menu, select **Communication** > **Bluetooth Settings**.
- Step 2 Turn on **Bluetooth**.

Figure 3-25 Bluetooth



3.10.5 Mode Settings

3.10.5.1 Controller Mode

The Device functions as an access controller, and connects to an external card reader, access controller or door control security module.

Procedure

- Step 1 On the main menu, select **Communication** > **Mode Settings**.
- Step 2 Set **Mode Settings** as **Access Controller**.
- Step 3 Configure RS-485 and Wiegand settings.
 - Select **RS-485 Settings** .
If you connect to other devices using the RS-485 port, configure the parameters.

Figure 3-26 Access controller



Table 3-6 Description of RS-485 parameters

Parameter	Description	Remark
Access Controller	Connects to other access controllers when the Device functions as a card reader, and sends data to other external access controllers to control access. ◇ ID: Outputs data based on the user ID. ◇ Card Number: Outputs data based on card number when users swipe card to unlock door; outputs data based on user's first card number when they use other unlock methods.	If the Device is connected to external access controller, when the people verify the identification on the Device, different permissions allow the people to control different doors. ◇ If the people have access permissions on the Device and the external access controller, the Device and the external access controller can be controlled. ◇ If the people only have access permissions on the Device, the external access controller cannot be controlled. ◇ If the people only have access permissions on the external access controller, the external access controller can be controlled.
Card Reader	The Device functions as an access controller, and connects to an external card reader.	—

Parameter	Description	Remark
Door Security Module	The door exit button, lock and fire linkage are not effective after the security module is enabled. ◇ Supports authentication through face, card, fingerprint, or password on this device to control the unlock of door security module. ◇ Supports authentication through external RS-485 card reader connected to the door control security module (by swiping a card) or through an external button to control the control the unlock of door security module.	
Lock Extension Module	The Device is connected to a door lock extension module. When Lock Extension Module is selected, the device's authentication only unlocks the local lock, while the external card reader's authentication unlocks the extension lock. After selection, in the Access Control Parameter and Alarm Config page, the door channel supports selecting Door 2, and relevant parameters for Door 2 can be configured.	
Reader (OSDP)	The Device connects to an OSDP protocol card reader, which sends access card information to the access controller or management platform.	

- Select **Wiegand Settings**.

- ◇ Wiegand Input: When connecting an external card reader device, select **Wiegand Input**.

Card No. Inversion: If the card number sequence obtained through Wiegand input does not match the actual card number sequence when interfacing with third-party devices, enable this function.

- ◇ Wiegand Output: When the Device functions as a card reader, and you need to connect it to another access controller, and select **Wiegand Output Config**.

Table 3-7 Description of Wiegand

Parameter	Description
Wiegand Output Type	The bit length of card numbers or ID that the device can recognize and output. ◇ Wiegand 26: Reads 3 bytes or 6 digits. ◇ Wiegand 34: Reads 4 bytes or 8 digits. ◇ Wiegand 66: Reads 8 bytes or 16 digits.
Pulse Width	Configure the pulse width and interval for wiegand output.

Parameter	Description
Pulse Interval	
Output Data Type	Select a Wiegand format to read card numbers or ID numbers. ◇ User ID: Outputs data based on user ID. ◇ Card: Outputs data based on user's first card number.
Wiegand Format	When Output Data Type is set as ID , you can select decimal or hexadecimal output formats.

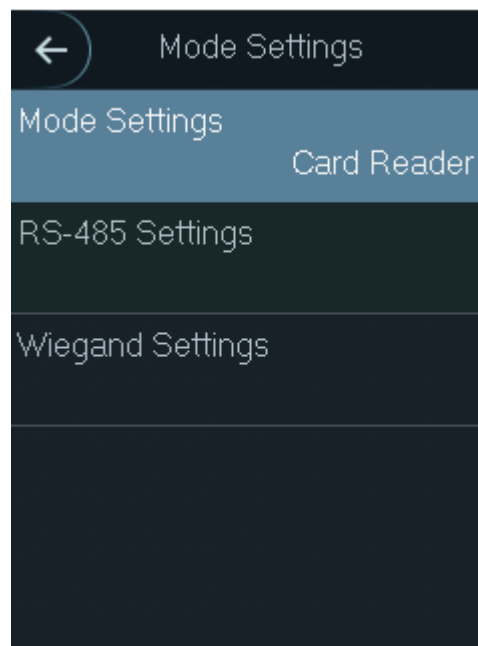
3.10.5.2 Card Reader Mode

When the device functions as a card reader connected to an external access controller, it does not perform authentication locally. Instead, it directly transmits access control data to the access controller, which then handles authentication and triggers the door unlock.

Procedure

- Step 1 On the main menu, select **Communication** > **Mode Settings**, and then press **OK**.
- Step 2 Set **Mode Settings** as **Card Reader**.

Figure 3-27 Card reader mode



- Step 3 Configure RS-485 and Wiegand settings.
- Select **RS-485 Settings** .
 - ◇ Baud Rate Config: 9600 by default, which can be modified.
 - ◇ Sync Time: Adjust the time of the device based on the tome of external controller.
 - Select **Wiegand Settings** .

The bit length of card numbers that the device can recognize and output.

 - ◇ Wiegand 26: Reads 3 bytes or 6 digits.
 - ◇ Wiegand 34: Reads 4 bytes or 8 digits.
 - ◇ Wiegand 66: Reads 8 bytes or 16 digits.

Figure 3-28 Wiegand



3.11 System Settings

The parameters might differ according to different device models.

Tap  or  to switch pages.

3.11.1 Configuring Time

Customize the system's time display and synchronization based on user preferences.

Procedure

- Step 1 On the main menu, select **System** > **Time**.
- Step 2 Configure parameters.

Figure 3-29 time

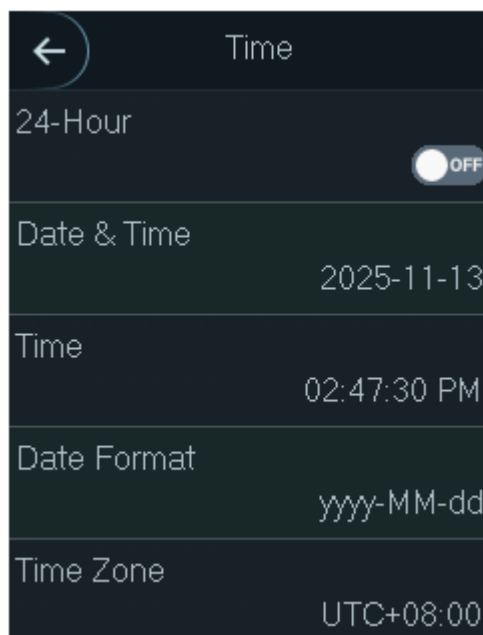


Table 3-8 Description of time parameter

Parameter	Description
24-Hour	Enable or turn off 24 hour format. When enabled, time will be displayed in 24-hour format; when turned off, time will be displayed in 12-hour format.
Date & Time	1. Tap to select Date & Time . 2. Enter the date, and then press OK .
Time	1. Tap to select Time . 2. Enter the time, and then press OK .
Date Format	1. Tap to select Date Format . 2. Select the format.
Time Zone	1. Tap to select Time Zone . 2. Select the time zone.

3.11.2 Configuring Language

On the main menu, select **System** > **Language**, select the language for the Device.

3.11.3 Configuring Volume

Procedure

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

Figure 3-30 Volume settings

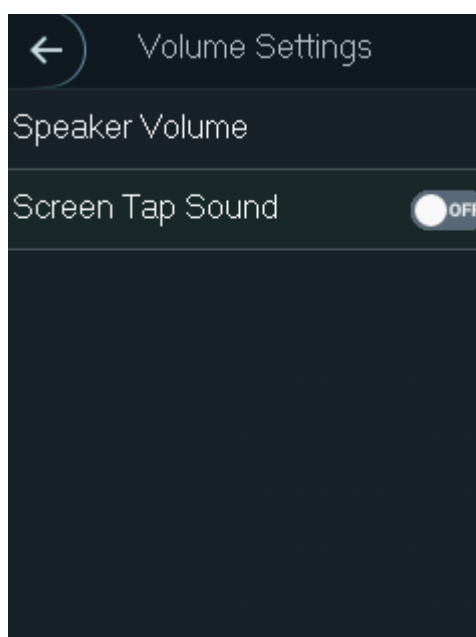


Table 3-9 Parameters description

Parameters	Description
Speaker Volume	Tap the volume, and then tap + or - to adjust the volume.
Screen Tap Sound	When this function is enabled, touch screen devices will produce tap sound.

3.11.4 Configuring Screen Parameters

Procedure

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

Figure 3-31 Screen settings

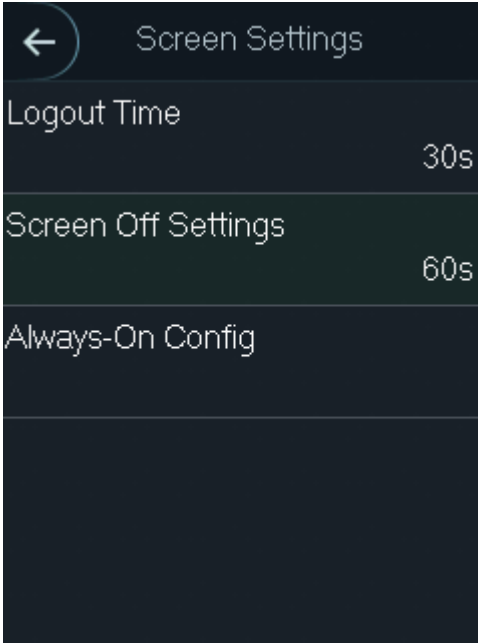


Figure 3-32 Always-on

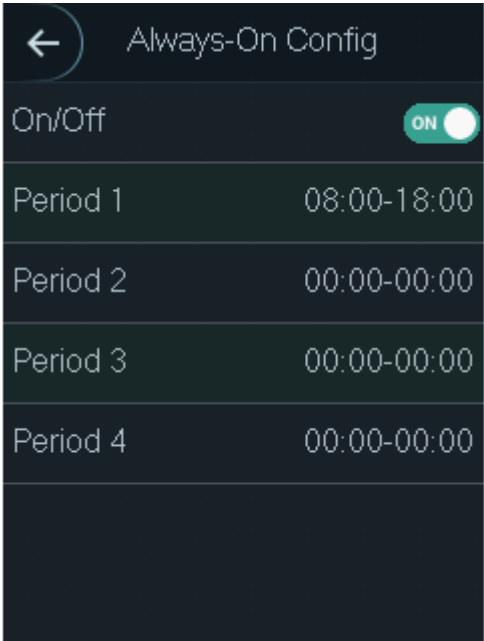


Table 3-10 Description of screen parameters

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

3.11.5 Configuring Card Settings

Background Information



Only devices with IC support this function.

Procedure

Step 1 On the main menu, select **System** > **Card Settings**.

Step 2 Configure parameters.

Figure 3-33 Card settings

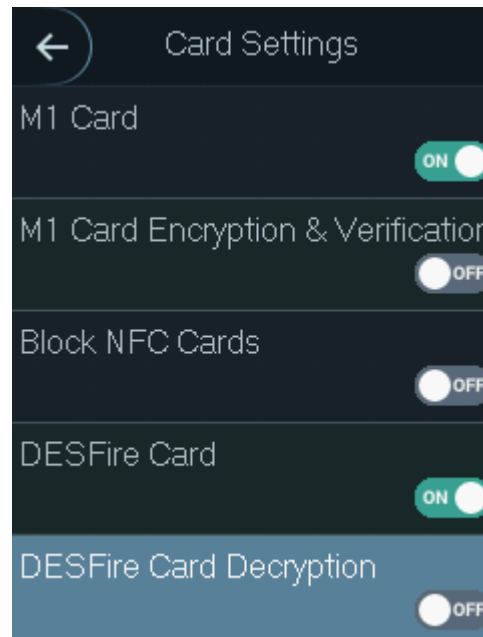


Table 3-11 Description of card parameters

Parameter	Description
M1 Card	
M1 Card Encryption & Verification	Only devices with IC support this function. Enable it and the device can read M1 card and ID serial number. It is enabled by default. Enable M1 Card Encryption & Verification after you have enabled M1 Card. Only supports reading M1 card.
Block NFC Cards	- Only devices with IC support this function. - Only certain phones support this function. After enabling the IC card, enable Block NFC Cards to prevent unauthorized access by blocking NFC-copied cards from opening doors.
DESFire Card	
DESFire Card Encryption	Only devices with IC support this function., and only hexadecimal card numbers are accepted. Enable the function, and the device can read the DESFire card's physical serial number (UID). After enabling the DESFire Card , enable DESFire Card Encryption, the device can read the contents of DESFire cards.

3.11.6 Configuring Device Password

3.11.6.1 Changing Password

Procedure

- Step 1 Select **System** > **Device Password** > **Change Password**.
- Step 2 Enter the old password, new password, confirm the password, and then tap **OK**.

3.11.6.2 Modifying Reserved Information

The reserved email address is used for receiving the security code to reset the password.

Procedure

- Step 1 Select **System** > **Device Password** > **Modify Reserved Info**.
- Step 2 Enter the email address, and then tap **OK**.

3.11.7 Restoring Factory Defaults



Restoring the device to the factory settings might cause data loss. Please be advised.

Restore through the Software

1. On the main menu, select **System** > **Factory Defaults**.
2. Restore factory defaults if necessary. Restore the factory default settings if necessary.
 - Restore to factory settings (keep network config): Resets all the configurations except for network configurations.
 - Restore to defaults (keep logs, user info, and network config): Resets all the configurations and data except for user information, logs, network configurations.
 - Restore to factory settings (complete reset): Resets all the configurations.

Figure 3-34 Factory defaults



Restore through the Hardware

The device supports the tamper button and the reset button.

- Tamper button: Within 5 minutes after the device is powered on, if you press the tamper button for 5 times in 8 seconds, the device displays the prompt. Click **OK** or press and hold the tamper button for seconds, and the device restarts. All the configurations and information are restored to the factory settings.
- Reset hole: To reset the device, you have to short it by inserting a pin into the pinhole.
 - ◇ If you wish to perform a partial reset and preserve the user information, logs and IP configurations, the pin must be inserted for 500 ms.
 - ◇ If you wish to perform a complete reset, the pin must remain inserted for 5 seconds.



The reset pinhole is available on select models.

3.11.8 Configuring Password Reset

On the main menu, tap **System**, and then turn on **Password Reset**. After the function is turned on, when you forget the password, you can use the configured email to receive the security code and reset the password. It is turned on by default.

3.11.9 Restarting the Device

On the main menu, select **System** > **Restart**, and the Device will be restarted.

3.12 USB Management

3.12.1 Exporting Data

After inserting the USB drive, export the data from the device to the USB drive. Some exported data is encrypted and cannot be edited.

Prerequisites

The USB drive has been inserted into the device and is properly recognized.



The supported formats for the USB drive are FAT32, with a capacity ranging from 4 GB to 128 GB.

Procedure

Step 1 On the main menu, select **USB** > **USB Export**.

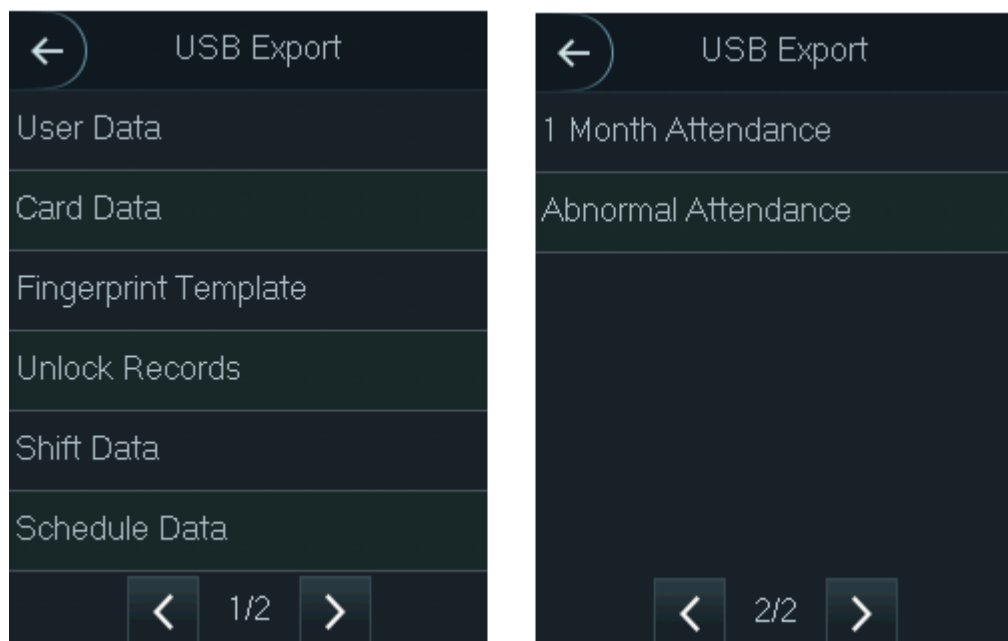
Step 2 Select the data type that needs to be exported, and then tap **OK**.

The exported information will be saved to the USB drive.



- When the exported data is in Excel format, it can be edited
- User data, card data, and fingerprint data are exported as encrypted.

Figure 3-35 USB export



3.12.2 Importing Data

Only data exported from one device can be imported into another device.

Prerequisites

The USB drive has been inserted and is properly recognized by the device.

Procedure

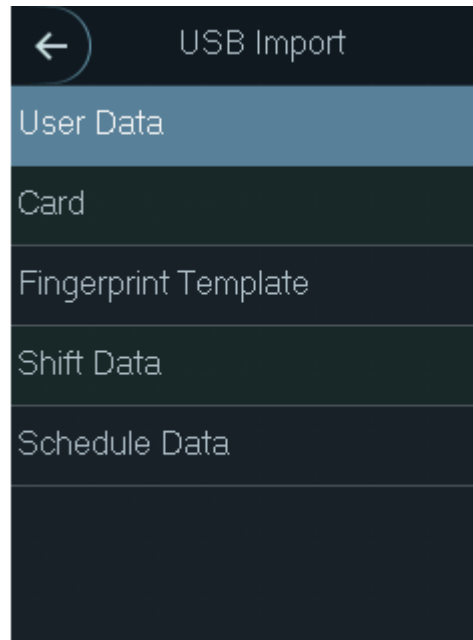
Step 1 On the main menu, select **USB** > **USB Import**.

Step 2 Select the data type that needs to be imported, and then tap **OK**



It is recommended that you import data between devices of the same model and version. Importing data between different models or versions may result in data loss.

Figure 3-36 USB import



3.12.3 Updating Device

Perform system upgrades through a USB drive.



For new devices or after a factory reset, the system files are backed up within the first 10 minutes of startup. Upgrading during this time is not recommended.

Procedure

- Step 1 Rename the update file as **update.bin**, and save it to the root directory of the USB drive. Insert the USB drive to the device.
- Step 2 Log in to the main menu of the device.
- Step 3 Select **USB > USB Update**.
Screen displays confirmation prompt.
- Step 4 Tap **OK** to update.
The system upgrade has started. The device will automatically restart once the upgrade is complete.

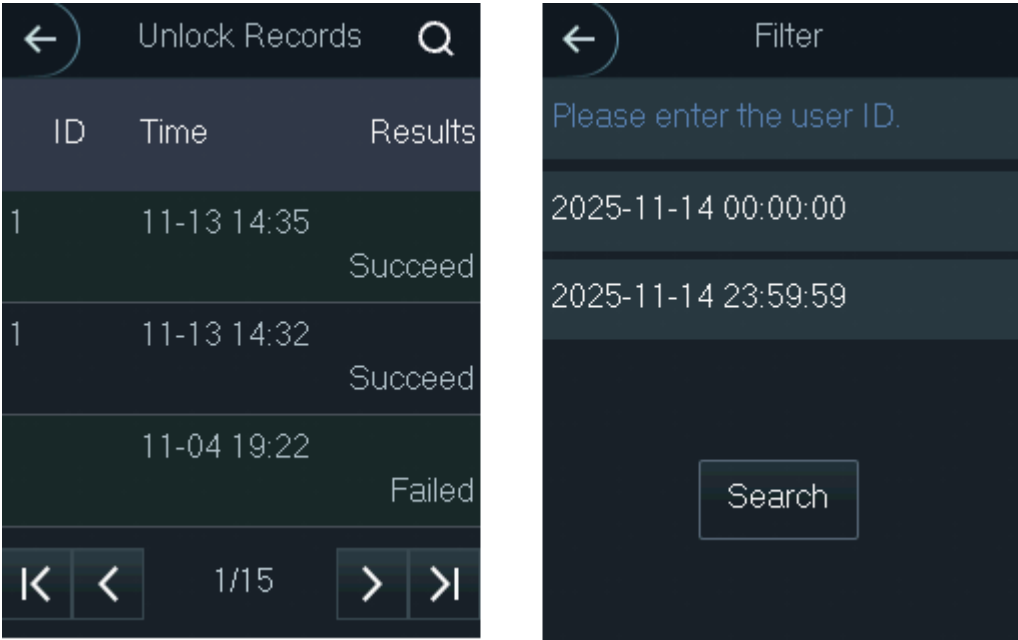
3.13 Records Management

Procedure

- Step 1 On the main menu, select **Records**.
It displays unlock records.

Step 2 (Optional) Tap  at the top right corner, enter the user ID, select the time period, and then tap **Search**.

Figure 3-37 Unlock records



3.14 Viewing Information

You can view data capacity and device version.

3.14.1 Viewing Data Capacity

On the main menu, select **Device Info** > **Data Capacity**. You can view storage capacity of each data type.

3.14.2 Viewing Device Version

On the main menu, select **Device Info** > **Device Version**. You can view the device version, such as product model, serial number, software version and more.

Tap **Product Documentation QR Code**, scan the QR code with your phone to view the product documents.



This function is only available on select models.

4 Web Operations

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



Web configurations differ depending on models of the Device.

4.1 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 on 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.

4.2 Logging In

Procedure

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

Step 2 Enter the user name and password.



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

Step 3 Click **Login**.

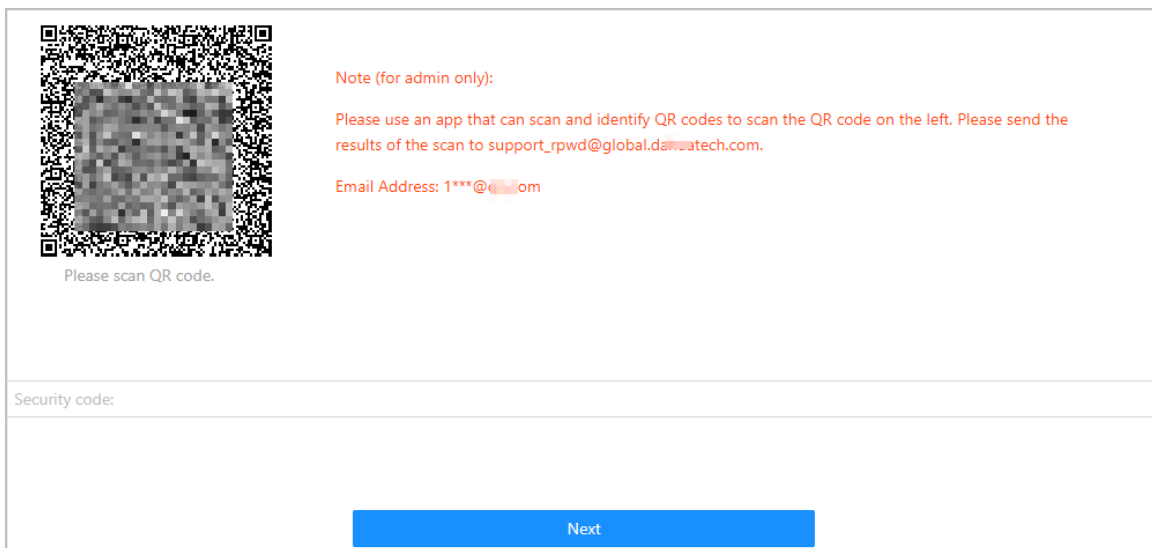
4.3 Resetting the Password

Reset the password through the linked email when you forget the admin password. If no email address was entered to reset the password, you need to contact local dealer or technical support.

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 4-1 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 email 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**.

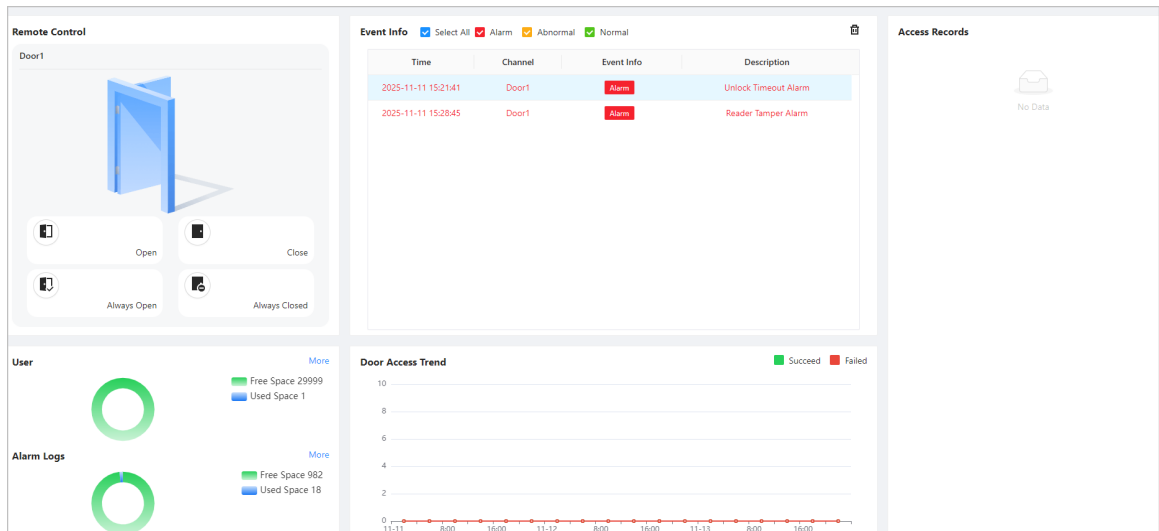
4.4 Access Monitoring

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



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

Figure 4-2 Access monitoring



Remote Control

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

Door Access Trend

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

Access Records

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

Event Information

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

User and Alarm Logs

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

4.5 Home Page

Click  at the upper-left corner or the webpage to go to the homepage.

Figure 4-3 Home page

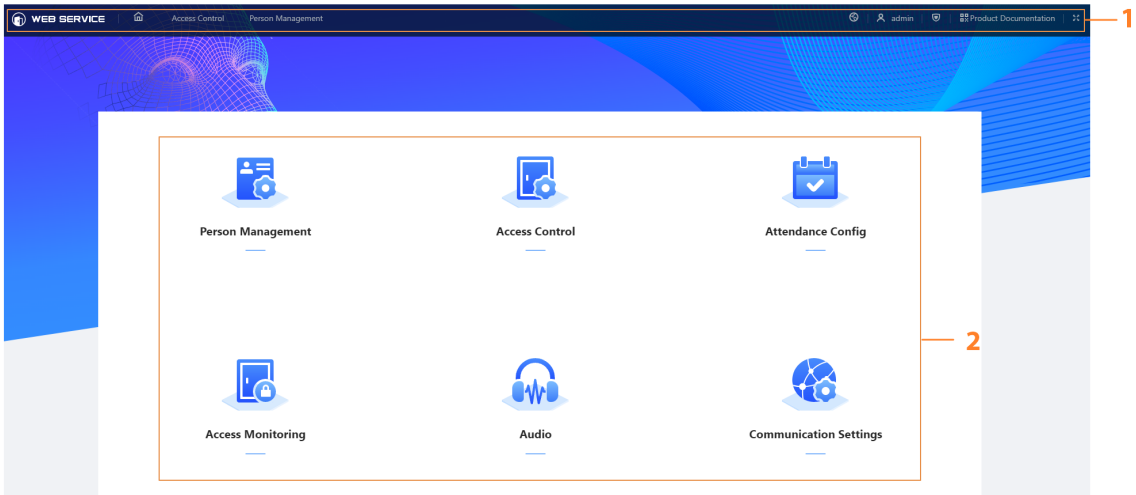


Table 4-1 Home page description

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

4.6 Person Management

Procedure

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

Figure 4-4 Basic information

Basic Info

* ID

Name

* Department

1-

* Schedule Mode

Department Schedule

Validity Period

Forever

* Permission

User

* User Type

General User

* Times Used

Unlimited

* General Plan

255-Default x

* Holiday Plan

255-Default x

Permission Type

Unlock and Attendance

Email

Verification Mode

☐ Same as Device
 ☒ Custom

Combination Meth...

☐ And
 ☒ Or

* Unlock Method

Card x

Fingerprint x

Password x

Bluetooth Card x

Table 4-2 Description of basic information

Parameter	Description
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 contain 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. For how to create department, see "4.8.1 Configuring Departments".
Schedule Mode	- Department Schedule: Assign department schedule to the user. For details, see "4.8.4 Configuring Work Schedules". - Personal Schedule: Assign personal schedule to the user. For details, see "4.8.4 Configuring Work Schedules". ◇ This function is only available on select models. If you set the schedule mode to department schedule here, the personal schedule you have configured for the user in Attendance > Schedule Config > Personal Schedule is invalid.
Validity Period	Set a date on which the door access and attendance permissions of the person will be expired.
Permission	User : Users only have door access or time attendance permissions. Admin : Administrators can configure the Device besides door access and attendance permissions.

Parameter	Description
User Type	● General User : General users can unlock the door. ● Blocklist User : When users in the blocklist unlock the door, service personnel will receive a notification. ● Guest User : Guests can unlock the door within a defined period or for certain amount of times. After the defined period expires or the unlocking times runs out, they cannot unlock the door. ● Patrol User : Patrol users can take attendance on the Device, but they do not have door permissions. ● VIP User : When VIP unlock the door, they are not restricted by unlock modes, such as Multi-card and Time Section. ● Other User : When they unlock the door, the door will stay unlocked for 5 more seconds. ● Custom User 1 /Custom User 2: Same as general users.
Times Used	Set an unlock limit for guest users. After the unlock times run out, they cannot unlock the door.
General Plan	People can unlock the door or take attendance during the defined period.  You can select more than one plan.
Holiday Plan	People can unlock the door or take attendance during the defined holiday.  You can select more than one holiday.
Permission Type	● Unlock and attendance: Person has the permission of attendance and can unlock the door using the configured verification methods. ● Attendance: Person only has the permission of attendance and cannot unlock the door. After the person successfully verifies the identification, one failed unlock record is generated.
Verification Mode	Configure the verification mode for the person. You can use the mode that is the same as the device or customize the mode. ● Same as Device : The mode is the same as the device. ● Custom : After you select Custom, Combination Method and Unlock Method are displayed. Select the combination method and unlock methods as needed. ◇ Or: Use one of the selected unlock methods to open the door. ◇ And: Use all the selected unlock methods to open the door.  ◇ The customized verification mode is only valid for the local device. It cannot be used in external card readers. ◇ When the customized verification mode is different from the mode of the device, the customized mode takes the priority.

Figure 4-5 Access credentials

Access Credentials

Table 4-3 Description of access credentials

Parameter	Description
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	 The card function is only available on select models. A user can register up to 5 cards at most. Enter your card number or swipe your card on the Device or an external card reader, and then the card information will be read by the Device.
	 Only certain models support collection through an external card reader. • Enter the card number manually. 1. Click Add. 2. Enter the card number, and then click Add. • Read the number automatically through the enrollment reader or the Device. 1. Click Add, and then click Modify to select an enrollment reader or the Device. 2. Read the card. ◇ For the enrollment reader of IC and ID card, click Read Card, and then swipe cards on the card reader. A 60-second countdown is displayed to remind you to swipe cards, and the system will read the card number automatically. If the 60-second countdown expires, click Read Card again to start a new countdown. ◇ For the enrollment reader of the Desfire card, place the card on the enrollment reader, and then click Read Card. If the Desfire card has been written with the card number, it will be read and displayed here. If the card is empty, then the card number needs to be written first. The card number will be automatically generated on the computer, and be written to the card. 3. Click Add. You can enable the Duress Card function. An alarm will be triggered if a duress card is used to unlock the door. • : Set duress card. • : Change card number.  One user can only set one duress card.

Parameter	Description
Fingerprint	Register fingerprints. A user can register up to 3 fingerprints, and you can set a fingerprint to the duress fingerprint. An alarm will be triggered when the duress fingerprint is used to unlock the door. Enroll fingerprints through an external enrollment reader or the Device.  Only certain models support fingerprint collection through an external enrollment reader. 1. Click Add , and then click Modify to select an enrollment reader or the Device. 2. Press finger on the scanner according to the on-screen instructions. 3. Click Add.  • 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. • Fingerprint function is available if the Device supports connecting a fingerprint module.
Bluetooth Card	 Bluetooth is only available on select models. You can select Request through Email or Request through Registration Code. • Request through Email : Suitable for the first time a Bluetooth card is requested. You can request up to 5 Bluetooth cards, and have to use the email that is registered to DMSS.  You must have entered your reserved Email before you use the function. 1. Configure the Email that is registered to DMSS. 2. Click Request through Email, and then the Bluetooth cards can be requested. • Request through Registration Code : Suitable when you already have a Bluetooth card and want to reuse it on another access controller supporting Bluetooth function. 1. Copy the Bluetooth registration code from the DMSS. 2. Click Request through Registration Code, and then enter the code. 3. Click OK.

Step 3 Click **Add**.

You can click **Add More** to add other users.

Related Operations

- Clear: Clear all users.
- Refresh: Refresh the user list.
- Search: Search by user name or user ID.

- Click **Bluetooth Cards Records**, and then you can view the Bluetooth card records. For users who issued cards unsuccessfully, you can reissue cards here.



You can issue cards in batches on devices that support Bluetooth function.

4.7 Access Control Management

4.7.1 Access Control Parameters

4.7.1.1 Configuring Basic Parameters

Procedure

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

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

Figure 4-6 Basic parameters

Basic Settings

Name: Door1

Door Status: ☒ Normal ☐ Always Closed ☐ Always Open

Normally Open Period: General Plan Disabled Holiday Plan Disabled

Normally Closed Period: General Plan Disabled Holiday Plan Disabled

Verification Interval: 0 s (0-180)

Card Swiping Interval: 0 s (0-86400)

Public Password: ☐

Table 4-4 Basic parameters description

Parameter	Description
Name	The name of the door.
Door Status	Set the door status. - Normal: The door will be locked and unlocked according to your settings. - Always open: The door remains unlocked all the time. - Always closed: The door remains locked all the time.

Parameter	Description
Normally Open Period	When you select Normal , you can select a time template from the drop-down list. The door remains open or closed during the defined time. For details on how to configure general plans and holiday plans, see "4.7.4 Configuring Periods".
Normally Closed Period	 - When normally open period conflicts with normally closed period, normally open period takes priority over normally closed period. - When the general plan conflicts with the holiday plan, the holiday plan takes priority over the general plan.
Verification Interval	If you verify your identity multiple times within a defined period, only the earliest verification will be considered valid, and the door will not open after the second or later verifications. From the moment the door fails to open, you must wait for the configured verification time interval before attempting to verify your identity again.
Card Swiping Interval	For first-time verification through card, you can normally unlock the door or perform attendance, and the records are generated. Within the configured period, if you swipe the card for verification again, you cannot unlock the door or perform attendance, and the records are not generated. Please verify the identification after the configured period.  The Card Swiping Interval takes priority over Verification Interval.
Public Password	After the public password is enabled, configure the password. You can use the public password without entering the user ID to unlock the door. Only one public password is supported for one device.

Step 3 Click **Apply**.

4.7.1.2 Configuring Unlock Methods

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

Procedure

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

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

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

Figure 4-7 Combination unlock

The screenshot shows the 'Unlock Settings' window. At the top, the title is 'Unlock Settings'. Below it, the 'Unlock Method' is set to 'Combination Unlock' in a dropdown menu. The 'Combination Method' has two radio buttons: 'Or' (selected) and 'And'. The 'Unlock Method (Multi-select)' section has four checkboxes: 'Card', 'Fingerprint', 'Password', and 'Bluetooth Card', all of which are checked. The 'Bluetooth Mode' has two radio buttons: 'Short-range' and 'Long-range' (selected). The 'PIN Code Authentication' is a toggle switch that is currently turned off. The 'Door Unlocked Duration' is a text input field containing '3.0', with a unit 's (0.2-600)' to its right. The 'Remote Verification' is another toggle switch, also turned off. At the bottom of the settings area, there are three buttons: 'Apply' (highlighted in blue), 'Refresh', and 'Default'.

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

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

Figure 4-8 Add group

Add

No.

Unlock Method ...

Select Person

Valid No.

Selected People

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

>

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

OK

Cancel

Figure 4-9 Unlock by multiple users

Unlock Settings

Unlock Method

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

Add

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

Verification of Multi-person Unlock Timeout Duration s (10-60)

Bluetooth Mode

☐ Short-range
 ☒ Mid-range
 ☐ Long-range

PIN Code Authentication

☐

Door Unlocked Duration s (0.2-600)

Remote Verification ☐

Apply

Refresh

Default

Table 4-5 Unlock settings description

Parameter	Description
Unlock Method (Multi-select)	Unlock methods might differ depending on the models of product.
Verification of Multi-person Unlock Timeout Duration	During verification, the interval between every two verifiers must be within this time period.

Parameter	Description
PIN Code Authentication	When PIN code authentication is enabled and you select user password to unlock, you only need to enter the user password without the user ID. When PIN code authentication is enabled, the remote verification is not supported when using user password to unlock.
Bluetooth Mode	Select the range for Bluetooth. You can select from Long-range and Short-range. It is only available for devices with Bluetooth function.
Door Unlock Duration	After a person is granted access, the door will remain unlocked for a defined time for the person to pass through. It ranges from 0.2 to 600 seconds.
Remote Verification	If this function is enabled, you can control the door on the corresponding platform.

- 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 4-10 Unlock by period

Unlock Method: Unlock by Period

Time: 00:00:00 - 23:59:59

Combination: ☒ Or ☐ And

Unlock Method: ☒ Card ☒ Fingerprint ☒ Password

Buttons: OK Delete

Door Unlocked Duration: s (0.2-600)

Remote Verification: ☐

Step 3 Click **Apply**.

4.7.2 Alarm

4.7.2.1 Configuring Alarm

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

Procedure

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

Step 2 (Optional) Select the door channel.

If you have selected **Lock Extension Module** as the **External Device** through **Communication Settings** > **RS-485 Settings** on the Access Controller, you can select the channel here.

Figure 4-11 Select the channel



Step 3 Configure alarm parameters.

Figure 4-12 Alarm

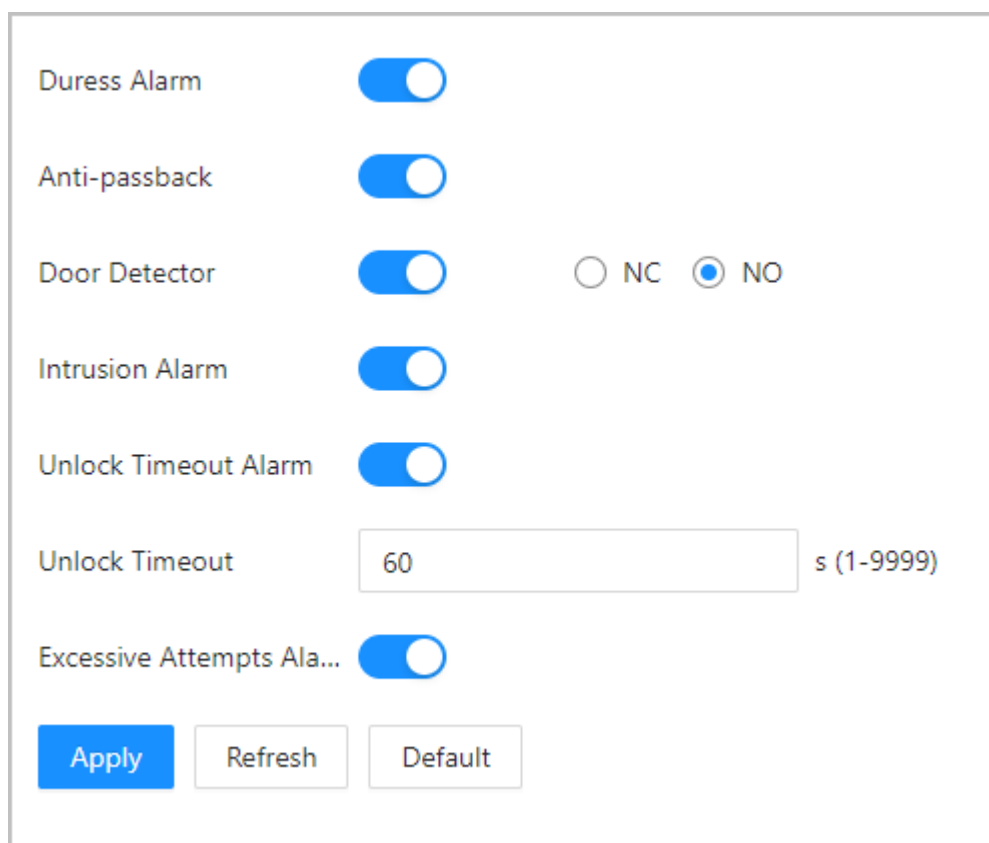


Table 4-6 Description of alarm parameters

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
Anti-passback	Users need to verify their identities both for entry and exit; otherwise an alarm will be triggered. It helps prevents a card holder from passing an access card back to another person to gain entry. When anti-passback is enabled, the card holder must leave the secured area through an exit reader before system will grant another entry. ● If a person enters after authorization and exits without authorization, an alarm will be triggered when they attempt to enter again, and access is denied at the same time. ● If a person enters without authorization and exits after authorization, an alarm will be triggered when they attempt to enter again, and access is denied at the same time.  If the Device can only connect one lock, verifying on the Device means entry direction, and verifying on the external card reader means exit direction by default. You can modify the setting on the management platform.
Door Detector	With the door detector wired to your device, alarm can be triggered when doors are opened or closed abnormally. The door detector includes 2 types, including NC detector and NO detector. ● NC: The sensor is in a shorted position when the door or window is closed. ● NO: An open circuit is created when the window or door is actually closed.
Intrusion Alarm	If the door is opened abnormally, an intrusion alarm will be triggered and last for a defined time.  The door detector and intrusion need to be enabled at the same time.
Unlock Timeout Alarm	When the door remains unlocked for longer than the defined timeout duration, the door timeout alarm will be triggered and last for the defined time.
Unlock Timeout	 The door detector and door timed out function need to be enabled at the same time.
Excessive Attempts Alarm	If the wrong password or card is used 5 times in a row within 60 seconds, the alarm for excessive use of illegal card will be triggered and lasts for a defined time.

Step 4 Click **Apply**.

4.7.2.2 Configuring Alarm Linkages (Optional)

You can configure alarm linkages.

Procedure

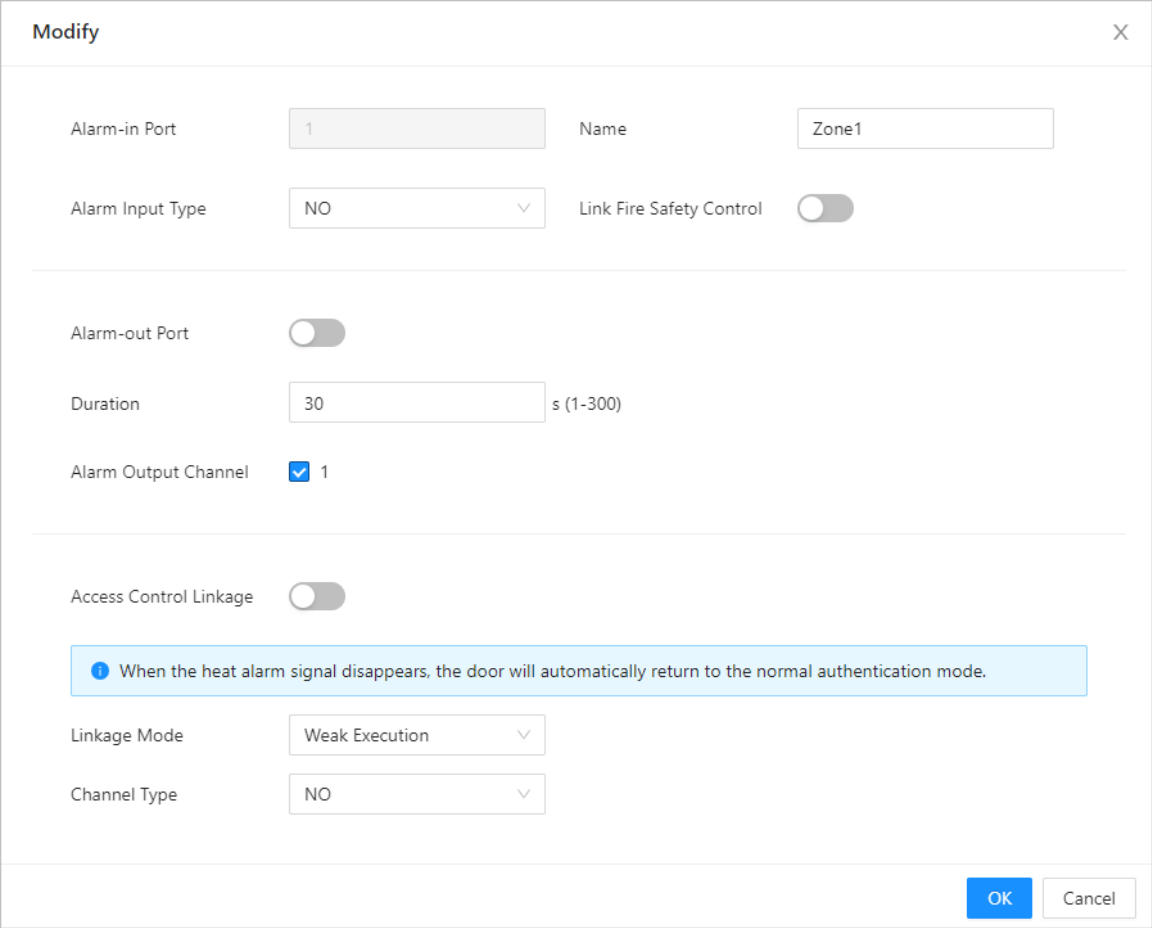
Step 1 Select **Access Control** > **Alarm** > **Alarm Linkage Setting**.



- If the Device is added to a management platform, the alarm settings will be synchronized to the platform.
- This function is only available on models that have alarm input and alarm output ports.
- The number of alarm input and output ports differs depending on models of the product.

Step 2 Click  to configure alarm.

Figure 4-13 Alarm linkage



The 'Modify' dialog box contains the following configuration options:

- Alarm-in Port:** 1
- Name:** Zone1
- Alarm Input Type:** NO (dropdown menu)
- Link Fire Safety Control:** Toggle switch (disabled)
- Alarm-out Port:** Toggle switch (disabled)
- Duration:** 30 s (1-300)
- Alarm Output Channel:** ☒ 1
- Access Control Linkage:** Toggle switch (disabled)
- Information:** When the heat alarm signal disappears, the door will automatically return to the normal authentication mode.
- Linkage Mode:** Weak Execution (dropdown menu)
- Channel Type:** NO (dropdown menu)

Buttons: OK, Cancel

Step 3 Create a name for the alarm zone.

Step 4 Enable **Link Fire Safety Control**, and select a type for the alarm input device.

- NC: The alarm input is in a normally closed (NC) circuit state when the alarm has not been tripped. Opening a normally closed circuit sets off the alarm.
- NO: The alarm input device is in a normally open (NO) circuit state when the alarm has not been tripped. Closing the circuit sets off the alarm.

Step 5 If you want to link access control when the fire alarm is triggered, enable **Access Control Linkage**.



This function takes effect only after **Link Fire Safety Control** is enabled.

Step 6 Select a linkage mode.

- Strong Execution: When the fire alarm signal disappears, the door remains the current status. Please manually changes to its previous door status settings if you want to.
- Weak Execution: When the fire alarm signal disappears, the door automatically returns to its previous door status.

Step 7 Select a channel type.

- NO: The door automatically opens when fire alarm is triggered.
- NC: The door automatically closes when fire alarm is triggered.

Step 8 Click **OK**.

4.7.2.3 Configuring Alarm Event Linkage

Procedure

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

Step 2 Configure alarm event linkages, and then click **Apply**.

Figure 4-14 Alarm event linkage

The screenshot displays the 'Alarm Event Linkage' configuration window. It is organized into four main sections, each with a toggle switch and a 'Please enable' message box:

- Intrusion Alarm Linkage:** Toggle is ON. Message: 'Please enable Intrusion Alarm.' Below are 'Buzzer' (checked, 15s) and 'Link Alarm Output' (checked, 15s).
- Unlock Timeout Alarm Linkage:** Toggle is ON. Message: 'Please enable Unlock Timeout Alarm.' Below are 'Buzzer' (checked, Custom Time 15s) and 'Link Alarm Output' (checked, Custom Time 15s).
- Max Use Alarm Link:** Toggle is ON. Below are 'Buzzer' (checked, 15s) and 'Link Alarm Output' (checked, 15s).
- Tamper Alarm Linkage:** Toggle is ON. Below are 'Buzzer' (checked, 3s) and 'Link Alarm Output' (unchecked, 15s).

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

Table 4-7 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. ● Link Alarm Output: The external alarm device generates alarms when the 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. The duration supports Custom Time and Until the Door Locks. ◇ Until the Door Locks: The alarm sound stops after the door is closed. ◇ Custom Time: You can configure the duration. ● Local Alarm Output: The external alarm device generates alarms when the unlock timeout alarm is triggered. The duration supports Custom Time and Until the Door Locks. ◇ Until the Door Locks: The alarm output stops after the door is closed. ◇ Custom Time: You can configure the duration.
Max Use Alarm Link	If the wrong password or card is used 5 times in a row within 60 seconds, the alarm for excessive use of illegal card will be triggered and lasts for a defined time. ● Buzzer: The buzzer sounds when the excessive use alarm is triggered. You can configure the alarm duration. ● Link Alarm Output: The external alarm device generates alarms when the unlock timeout alarm is triggered. You can configure the alarm duration.
Tamper Alarm Linkage	The tamper alarm is triggered when someone has tried to physically damage the Device. ● Buzzer: The buzzer sounds when the tamper alarm is triggered. You can configure the alarm duration. ● Link Alarm Output: The external alarm device generates alarms when the tamper alarm is triggered. You can configure the alarm duration.

4.7.3 Card Settings

4.7.3.1 Configuring Card Settings



This function is only available on select models.

Procedure

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

Figure 4-15 Card parameters

Card Settings

M1 Card

M1 Card Encryption & Verification

Block NFC Cards

DESFire Card

DESFire Card Decryption

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

DESFire Card Write

Acquisition De...

Device

Please place the card on the swiping area and enable DESFire card and DESFire Card Decryption.

Card Number

Write

Table 4-8 Card parameters description

Item	Parameter	Description
Card Settings	M1 Card	The M1 card can be read when this function is enabled. This function is only available on select models.
	M1 Card Encryption & Verification	Only the encrypted IC card can be read when this function is enabled. Make sure M1 Card is enabled.

91

Item	Parameter	Description
	Block NFC Cards	Prevent unlocking through duplicated NFC card after this function is enabled.  • This function is only available on models that support IC cards. • Make sure M1 Card is enabled. • NFC function is only available on select models of phones.
	Desfire Card	The Device can read the card number of Desfire card when this function is enabled.  • This function is only available on models that support IC cards. • Only supports hexadecimal format.
	Desfire Card Decryption	Information in the Desfire card can be read when Enable Desfire Card and Desfire Card Decryption are enabled at the same time.  • This function is only available on models that support IC cards. • Make sure that Desfire card is enabled.
Card No. System	Card No. System	Select decimal format or hexadecimal format for the card number when Wiegand card reader is connected. The card No. system is the same for both card number input and output.
DESFire Card Write	Acquisition Device	Select the device, place the card on the reader, enter the card number, and then click Write to write card number to the card.  • Desfire card function and Desfire card decryption function must be enabled. • Only supports hexadecimal format. • Supports up to 8 characters.
	Card Number	

Step 4 Click **Apply**.

4.7.3.2 Configuring Access Card Rule Parameters

The platform supports 5 types of Wiegand formats by default. You can also add custom Wiegand formats.

Procedure

Step 1 Log in to the webpage.

Step 2 Select **Access Control** > **Card Settings** > **Access Card Rule Setting**.

Step 3 Click **Add**, and then configure new Wiegand formats.

Figure 4-16 Add new Wiegand formats

The 'Add' dialog box is used to configure Wiegand formats. It includes fields for Wiegand Format, Total Bits, Facility Code, Card Number, and Parity Code, each with an 'Add' button to open a configuration table. The Facility Code, Card Number, and Parity Code tables have columns for No., Start Bit, End Bit, Total Bits, and Operation (trash icon).

Table 4-9 Wiegand format description

Parameter	Description
Wiegand format	The name of the Wiegand format.
Total bits	Enter the total number of bits.
Facility Code	Click Add , and then enter the start bit and the end bit for the facility code.
Card number	Click Add , and then enter the start bit and the end bit for the card number.
Parity Code	1. Click Add . 2. Enter the even parity start bit and even parity end bit. 3. Enter the odd parity start bit and odd parity end bit.

Step 4 Click **OK**.

Related Operations

- You can also click **Add Protocol** to import a Wiegand file to the platform.
- Facility Code: If the function is enabled, and you have set **Card No. System** to decimal format on the **Person Management** page, the facility code and the card number are transformed into decimal format separately, and then combine together.
- HID26: If the function is turned on:
 - ◇ Only Wiegand 26 is supported.
 - ◇ The platform only supports displaying card in decimal format.

- ### 4.7.3.3 Configuring Custom Conversion

Procedure

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

- Figure 4-17 Auto match (successfully matched)

- Import conversion rule: Import other rules to convert the card number.

Click **Upload File** , select the rule file, and then click **Open**.

Figure 4-18 Import conversion rule

The screenshot shows a configuration window for an 'Import Conversion Rule'. At the top, there is an 'Enable' toggle switch which is turned on (blue). Below this, the 'Matching Mode' is set to 'Import Conversion Rule' (indicated by a blue dot next to the text), with 'Auto Match' as an alternative option. Under the 'Version' label, the date '2025-03-31' is displayed. To the right of the date are two buttons: 'Upload File' and 'Default'. At the bottom of the window, a light blue box contains the text: 'You can only upload files in zip format and the size must not exceed 1 MB.'

4.7.4 Configuring Periods

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

4.7.4.1 Configuring General Plan

You can configure up to 128 periods (from No.0 through No.127) of time periods. 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 4-19 Configure general plan

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

- No.:** A dropdown menu with the value "0" selected.
- General Plan Name:** A text input field containing "Plan 1".
- Time Plan:** A section with a horizontal timeline at the top labeled 0 through 11. Below it is a table with rows for days of the week (Sun, Mon, Tue, Wed, Thu, Fri, Sat) and columns for hours. A blue shaded area covers the time range from 12:30:00 to 23:59:59 across all days. To the right of each row is a "Copy" button.
- Time Selection Pop-up:** A small dialog box is open over the timeline, showing a time range from 12:30:00 to 23:59:59. It has "OK" and "Delete" buttons.
- Bottom Buttons:** "OK" and "Cancel" buttons are located at the bottom right of the main window.

Step 4 Click **OK**.

4.7.4.2 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 4-20 Add a holiday group

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

- No.:** A dropdown menu with the value '2' selected.
- Holiday Group Name:** A text input field containing 'Holiday Group for 2023'.
- Holiday Group Config:** A section containing an 'Add' button and a table.

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

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

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

Figure 4-21 Add a holiday to a holiday group

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

- Holiday Name:** A text input field containing 'National Day'.
- * Period:** A date range selector showing '2023-10-01' to '2023-10-07' with a calendar icon on the right.

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

Step 4 Click **OK**.

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

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

Figure 4-22 Add holiday plan

Step 6 Click **OK**.

4.7.5 Configuring Expansion Modules

For Device that supports connecting expansion modules, configure the type of the module that the Device supports.

Background Information



- The type the expansion module might differ depending on models of the Device.
- The settings of expansion module remain after restoring the Device to factory defaults.

Procedure

Step 1 On the webpage, select **Access Control** > **Expansion Module**.

Step 2 Select the type of the module that the Device supports.

Step 3 Click **Apply**.

The configurations become effective after Device is restarted.

-  is displayed at the right corner on the standby screen, which means it was successfully set.
-  is displayed at the right corner on the standby screen, which means the type of the expansion module you configured does not match the actual expansion module that is connected to Device.
- If **None** is selected and no expansion module is connected to the Device, the expansion module icon will not be displayed.

4.7.6 Configuring Back-end Comparison

Before configurations, make sure that the Device is connected to the third-party platform through SDK. You can directly pass data such as QR code or card number to the third-party platform for data validation rather than validating data on the Device.

Select **Access Control** > **Back-end Comparison**.

Figure 4-23 Back-end comparison

Table 4-10 Back-end comparison

Parameters	Description
QR Code Pass-through	After it is enabled, the scanned QR code is passed to the third-party platform for data validation.
Card No. Pass-through	After it is enabled, the card number is passed to the third-party platform for data validation.

4.7.7 Configuring First-Person Unlock

Any person can only access doors after the persons you specify pass through. When you specify multiple persons, other persons can access doors after any one of specified persons pass through.

Prerequisites

Persons can only be set as first persons when they have permissions to access doors.

- Only the general users can be configured as the first person.
- After the first person verifies the identity, if the Device restarts, the first person needs to verify the identity again.
- After the function is enabled, patrol users can normally clock in and out.

Procedure

- Step 1 Select **Access Control** > **First-Person Unlock**.
- Step 2 Select the door channel, and then enable the function.

Figure 4-24 First-person unlock

Step 3 Configure the parameters.

Table 4-11 Parameter description

Parameter	Description
Time Templates	Select when this rule is effective.
Door Status after First-Card Unlock	● Normal : Other persons must verify their identifications to pass. ● Always Open : All people can pass without verifying their identifications.
Person List	Click + to select one or more persons, and they will have permissions to access the doors.

Step 4 Click **Apply**.

4.7.8 Configuring Anti-Passback

Users need to verify their identities both for entry and exit; otherwise an anti-passback alarm will be triggered. It prevents a card holder from passing an access card back to another person so they gain entry. When anti-passback is enabled, the card holder must leave the secure area before system will grant another entry.

- If a person enters after being authorized and exits without being authorized, an alarm will be triggered when they attempt to enter again, and access is denied at the same time.
- If a person without being authorized and exits after being authorized, an alarm will be triggered when they attempt to enter again, and access is denied at the same time.

Procedure

Step 1 Select **Access Control** > **Anti-passback**.

Step 2 Turn on this function, and then configure the reset time.

Specify a time when the anti-passback status of all personnel will be reset.

Step 3 Select the general plan and the holiday plan.

Anti-passback is effective during the defined time.

Step 4 In entry group, click **Add**, and then select the card reader.

Step 5 In exit group, click **Add**, and then select the card reader.

Figure 4-25 Anti-passback

Enable ☒

Reset Time min (5-300)

Time Templates

General Plan

Holiday Plan

Anti-passback Group Config

Entry Group

+ Add

Clear

/Reader 1

Remove

Exit Group

+ Add

Clear

/Reader 2

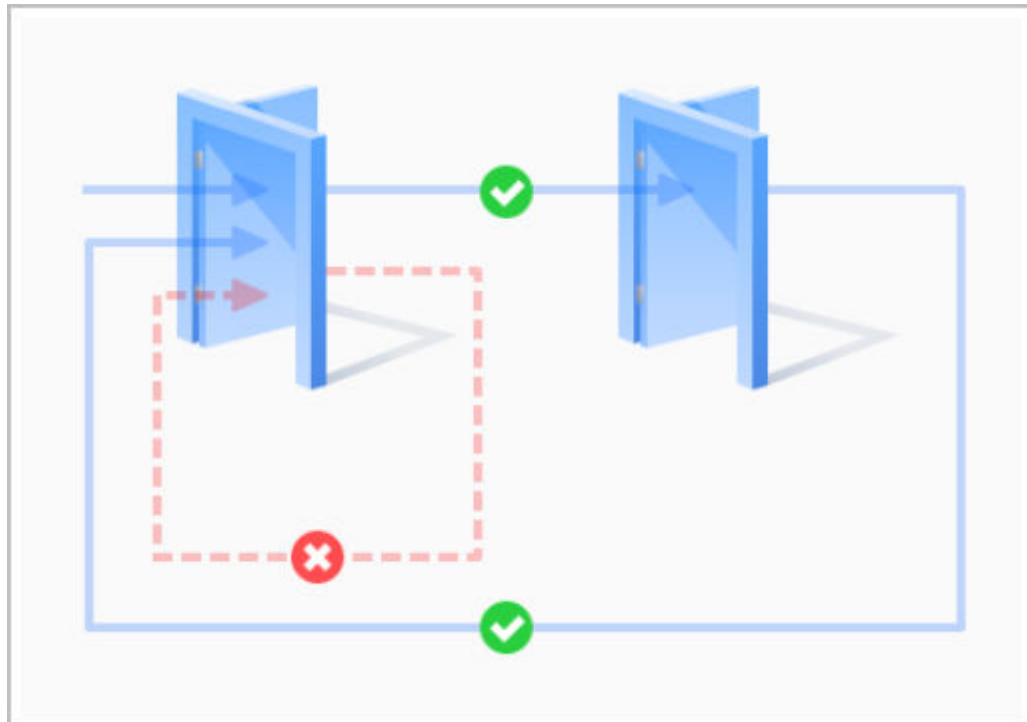
Remove

Step 6 Click **Apply**.

Results

The group number indicates the sequence of swiping cards. Card must be used following the specific sequence of groups. For example, you must swipe card at a reader in entry group, and then at a reader for exit group. As long as you swipe card following the established sequence, the system works fine.

Figure 4-26 Anti-passback function



4.8 Attendance Configuration

This function is only available on select models.

4.8.1 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 4-27 Create departments

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

Related Operations

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

4.8.2 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 4-28 Configure the shift

Edit Shift

* Shift No.

1

* Shift Name

Default

* Period 1

08:00 → 17:00

* Period 2

00:00 → 00:00

* Period 3

00:00 → 00:00

* Overtime Period

00:00 → 00:00

* Limit for Arriving Late

5

min (0-99)

* Limit for Leaving Early

5

min (0-99)

OK

Cancel

Table 4-12 Shift parameters description

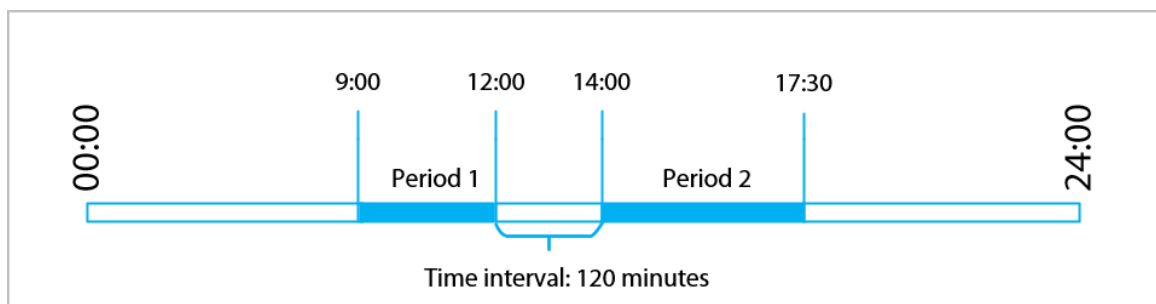
Parameter	Description
Shift Name	Enter the name of the shift.

Parameter	Description
Period 1	Specify a time range when people can clock in and clock out for the workday. You must configure at least 1 period.
Period 2	
Period 3	
	• 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 records. 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. • If you set 3 periods, the 3 periods cannot overlap. Employees need to clock in and clock out for adjacent 2 periods.  The last period can cross days. If the overtime period is the last one, you can configure it to cross days.
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 you configure more than one periods, refer to the following instructions to perform attendance function.

- 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 4-29 Time interval (even number)



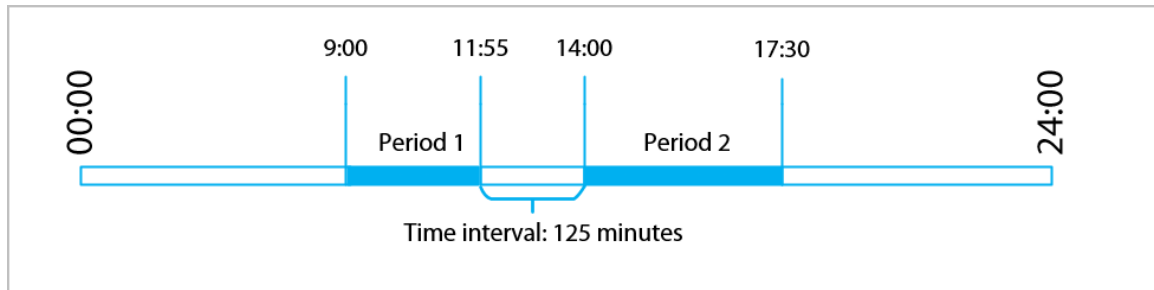
For example: If the interval is 120 minutes, then the clock-out time for period 1 is from 12:00 to 12:59, and the clock-in time for period 2 is from 13:00 to 14:00.



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 4-30 Time interval (odd 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.

- If there is only one period, and you do not clock in or out by the designated time, it is considered as absent for 1 day.
- If there are more than one period, and you do not clock in or out by the designated time of one period, it is considered as absent for 0.5 days. If you do not clock in or out by the designated time of 2 or more than 2 periods, it is considered as absent for 1 day. Attendance during overtime periods does not change the absent status of the person.

When you configure the last period to cross days, refer to the following instructions to perform attendance function.

- If the second day is the normal shift, the attendance is as normal.
- If the second day is the holiday, you can clock out in any time of 24 hours in the holiday day.



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.

4.8.3 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 4-31 Create holiday plans

Add Attendance Holiday X

* Attendance Holiday ... 1 ▾

* Attendance Holiday Attendance Holiday for October

* Time 2023-10-01 → 2023-10-07 📅

OK Cancel

Table 4-13 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**.

4.8.4 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.

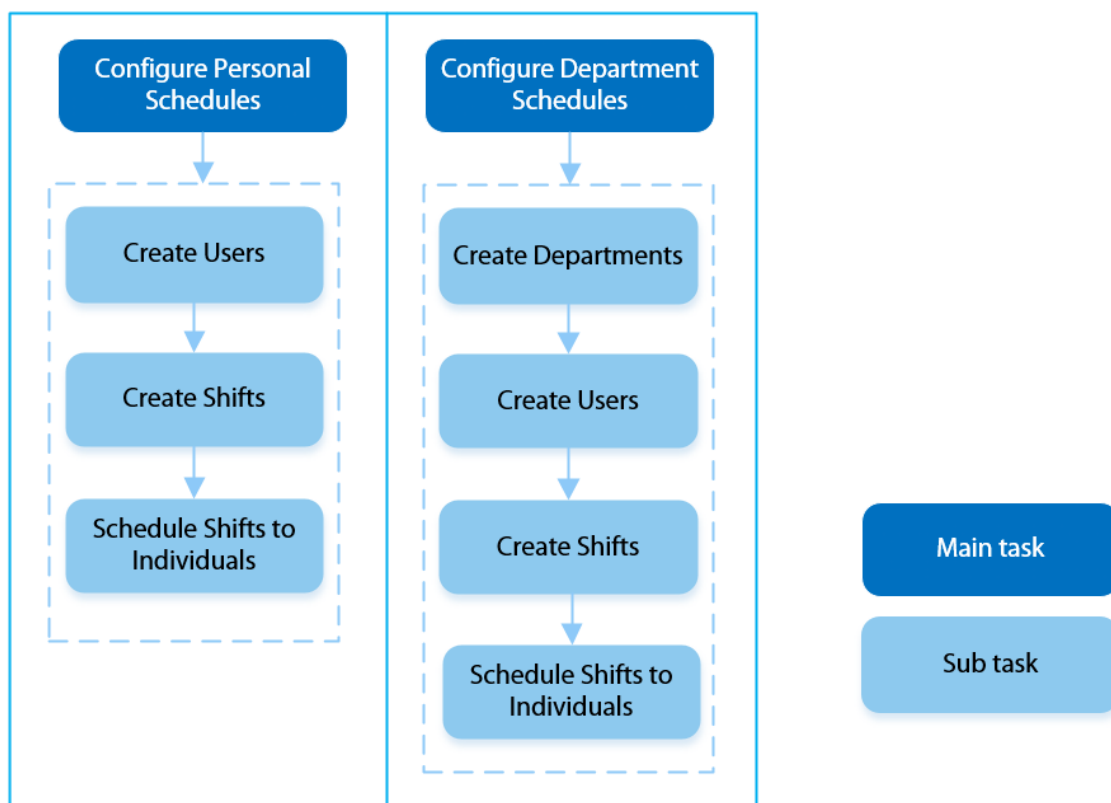
Background Information

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



When configuring the schedule, there should be no overlapping time periods on the same day and the previous or following day.

Figure 4-32 Configure 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 4-33 Personal schedule

The screenshot displays the 'Personal Schedule' interface. On the left, there is a 'Person List' with two entries: '1-' and '2-'. Below them are two IDs: '2678490-' and '9958875-'. The '2678490-' entry is selected. A 'Batch Configure' button is located next to the selected entry. The main area is a calendar grid for the month of May. The grid shows days of the week (Su, Mo, Tu, Th, Fr, Sa) and dates (01 to 11). A 'Select Shift' dropdown menu is open, showing options: '0-Rest', '1-Default', '2-Default', '3-Default', '4-Default', '5-Default', '6-Default', '7-Default', and '8-Default'. The '1-Default' option is selected. The calendar grid shows the following values for the selected person (2678490-):

Day	Shift
Su 01	0
Mo 02	1
Tu 03	1
Th 05	1
Fr 06	1
Sa 07	0
Su 08	0
Mo 09	1
Tu 10	13
Th 12	1
Fr 13	1
Sa 14	0
Su 15	0
Mo 16	1
Tu 17	1
Th 18	1
Fr 19	1
Sa 20	1
Su 21	0
Mo 22	0
Tu 23	1
Th 24	1
Fr 25	1
Sa 26	1
Su 27	1
Mo 28	0
Tu 29	0
Th 30	1
Fr 31	1
Sa 01	0
Su 02	0
Mo 03	0
Tu 04	0
Th 05	0
Fr 06	0
Sa 07	0
Su 08	0
Mo 09	0
Tu 10	0
Th 11	0



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

- 0 indicates break.
- 1 to 24 indicates the number of the pre-defined shifts. For how to configure shifts, see "4.8.2 Configuring Shifts".
- 25 indicates business trip.
- 26 indicates leave of absence.

Step 3 Set work 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 pre-defined shifts. For how to configure shifts, see "4.8.2 Configuring Shifts".
 - 25 indicates business trip.
 - 26 indicates leave of absence.

Figure 4-34 Schedule shifts to a department

The screenshot displays the 'Department Schedule' interface. On the left, a 'Department List' shows 18 departments, all labeled 'X-Default'. The main area shows a weekly shift cycle for '3-Default'. The days of the week are Sun, Mon, Tue, Thu, Fri, and Sat. The shift values are: Sun (0), Mon (2), Tue (1), Thu (1), Fri (1), and Sat (0). A 'Select Shift' dialog box is open, showing a list of shifts from 0-Default to 8-Default, with '2-Default' selected.



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

4.8.5 Exporting Attendance Record

You can export the unlock record and attendance records.

Procedure

- Step 1 Select **Attendance Config > Attendance Report**.
- Step 2 Select the type, select the date, and then click **Export**.
- For the access control device, you can select the type from **Unlock Records , 1 Month Attendance**, and **Abnormal Attendance**.
 - For the attendance device, you can select the type from **Attendance Records , 1 Month Attendance**, and **Abnormal Attendance**.
 - If you select **1 Month Attendance**, personal attendance report, attendance detailed report, and attendance summary are exported at the same time.



The exported files are in XML format.

Figure 4-35 Export the record

The screenshot shows a dialog box for exporting records. It has two main sections: 'Type' and 'Date'. The 'Type' section has a dropdown menu currently set to 'Unlock Records'. The 'Date' section has a date range selector showing '2025-06-10' to '2025-06-11' with a calendar icon. Below these sections is a blue 'Export' button.

4.8.6 Configuring Attendance Modes

Procedure

- Step 1

Select **Attendance Config** > **Attendance Config**.
- Step 2

Enable **Local Attendance**, and then set the attendance mode.
- Step 3

Configure attendance modes.

Figure 4-36 Attendance modes

Local Attendance

☒

Mode Settings

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

Check In

06:00 AM → 09:59 AM

Break Out

10:00 AM → 12:59 PM

Break In

01:00 PM → 03:59 PM

Check Out

04:00 PM → 08:59 PM

Overtime Check In

12:00 AM → 12:00 AM

Overtime Check Out

12:00 AM → 12:00 AM

Apply

Refresh

Default

Table 4-14 Attendance mode

Parameter	Description
Auto/Manual Mode	The screen displays the attendance status automatically after you clock in or out, but you can also manually change your attendance status. • 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 ends. • Overtime check in: Clock in when your overtime period starts. • Overtime check out: Clock out when your overtime period ends.

Parameter	Description
Auto Mode	The screen displays your attendance status automatically after you clock in or out. • 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 ends. • Overtime check in: Clock in when your overtime period starts. • Overtime check out: Clock out when your overtime period ends.
Manual Mode	Manually select your attendance status when you clock in or out.
Fixed Mode	When you clock in or out, the screen will display the pre-defined attendance status all the time.

Step 4 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.

4.9 Audio

4.9.1 Configuring Audio Parameters

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

Procedure

Step 1 Select **Audio > Audio Config**.

Step 2 Configure audio parameters, and then click **Apply**.

Figure 4-37 Audio

Speaker Volume
 (0-100) ⓘ

Key Sound
☐

Voice Broadcast Settings

Successfully verified. ▾

Period1
 ⓘ
 ⓘ
☐ Enable

Audio File
 ▾

Period2
 ⓘ
 ⓘ
☐ Enable

Audio File
 ▾

Period3
 ⓘ
 ⓘ
☐ Enable

Audio File
 ▾

Period4
 ⓘ
 ⓘ
☐ Enable

Audio File
 ▾

Figure 4-38 DND

DND Mode
☒

Time

Period 1
 → ⓘ

Period 2
 → ⓘ

Period 3
 → ⓘ

Period 4
 → ⓘ

Table 4-15 Description of audio parameters

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

Parameters	Description
Key Sound	When enabled, touchscreen devices will produce a prompt sound for local touch operations, while non-touchscreen devices will produce a prompt sound for key/button operations.
Voice Broadcast Settings	Set voice prompts for successful and failed verification. Supports up to 6 time periods.  Only available on select models. Click corresponding time period to enable it. Configure the time period, and select an audio file. Supports selecting audio files uploaded in Audio > Audio File. For details, see "4.9.2 Managing Audio Files".
DND Mode	When enabled, there will be no prompt sounds for local verification (such as door access or attendance) during the configured time periods. Supports up to 4 time periods.

4.9.2 Managing Audio Files

Background Information

Upload and manage audio files.



It is only supported on select models.

Procedure

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

Figure 4-39 Manage audio file

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

 Upload

No.	Name	Operation
 No Data		

4.10 Communication Settings

4.10.1 Network Settings

4.10.1.1 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 4-40 TCP/IP

The screenshot displays the TCP/IP configuration window. It includes a dropdown for 'NIC' set to 'NIC 1', radio buttons for 'Mode' with 'Static' selected, and a disabled 'MAC Address' field. Below these are dropdowns for 'IP Version' (IPv4) and input fields for 'IP Address' (192.168.1.1), 'Subnet Mask' (255.255.0.0), 'Default Gateway' (192.168.1.1), 'Preferred DNS' (8.8.8.8), and 'Alternate DNS' (8.8.4.4). An 'MTU' field is set to 1500. At the bottom are 'Apply', 'Refresh', and 'Default' buttons.

Table 4-16 Description of TCP/IP

Parameter	Description
Mode	• Static: Manually enter IP address, subnet mask, and gateway. • DHCP: It stands for Dynamic Host Configuration Protocol. When DHCP is turned on, the Device will automatically be assigned with IP address, subnet mask, and gateway.

Parameter	Description
MAC Address	MAC address of the Device.
IP Version	IPv4 or IPv6.
IP Address	If you set the mode to Static , configure the IP address, subnet mask and gateway.
Subnet Mask	
Default Gateway	
	 • IPv6 address is represented in hexadecimal. • IPv6 version do not require setting subnet masks. • The IP address and default gateway must be in the same network segment.
Preferred DNS	Set IP address of the preferred DNS server.
Alternate DNS	Set IP address of the alternate DNS server.
MTU	MTU (Maximum Transmission Unit) refers to the maximum size of data that can be transmitted in a single network packet in computer networks. It is 1500 by default.

Step 3 Click **OK**.

4.10.1.2 Configuring Wi-Fi



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

Procedure

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

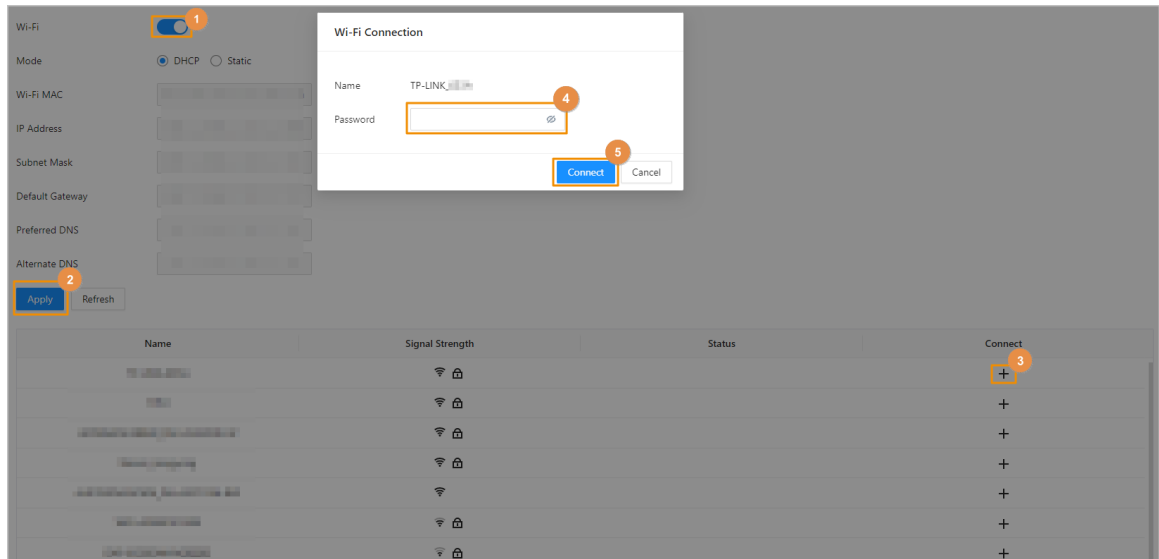
Step 2 Turn on Wi-Fi, and then click **Apply**.

All available Wi-Fi are displayed.

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

The Wi-Fi is connected.

Figure 4-41 Wi-Fi



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.

4.10.1.3 Configuring Wi-Fi AP

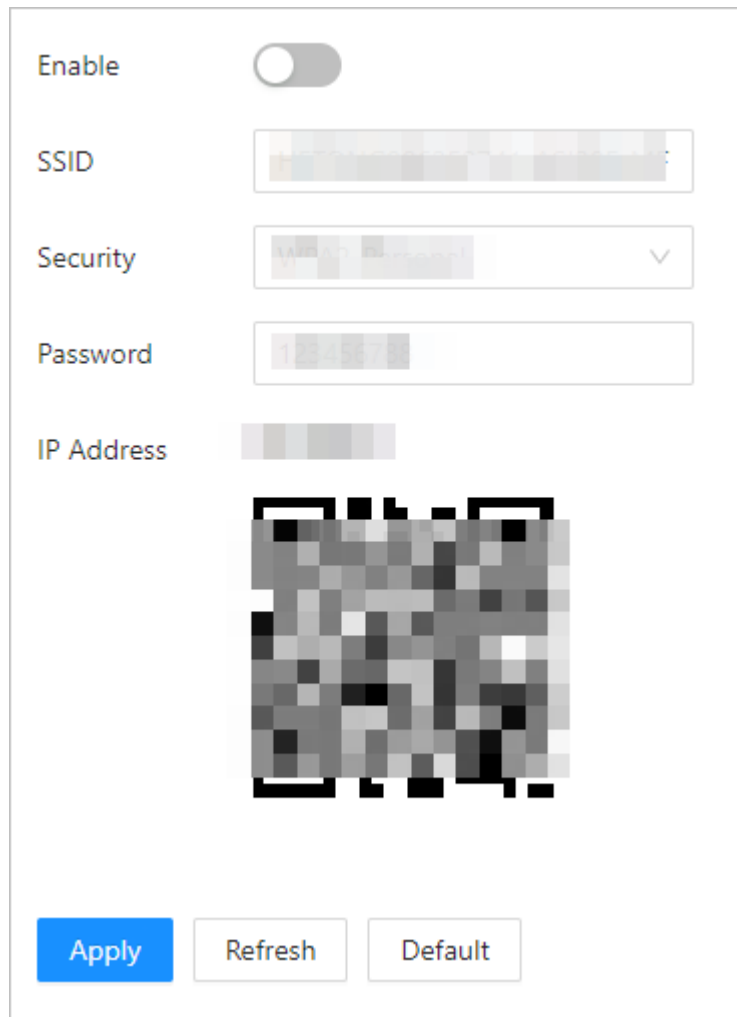


- The Wi-Fi function is available on select models.
- The Wi-Fi and Wi-Fi AP cannot be enabled at the same time.

Procedure

- Step 1 Select **Communication Settings** > **Network Setting** > **Wi-Fi AP**.
- Step 2 Enable the function, and then click **Apply**.

Figure 4-42 Wi-Fi AP

The image shows a web-based configuration interface for a Wi-Fi Access Point (AP). It features several input fields and a QR code. At the top, there is an 'Enable' toggle switch which is currently turned off. Below it are fields for 'SSID', 'Security' (a dropdown menu), 'Password', and 'IP Address'. A large QR code is positioned below the IP address field. At the bottom of the interface, there are three buttons: 'Apply' (highlighted in blue), 'Refresh', and 'Default'.

Results

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

4.10.1.4 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.



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

Figure 4-43 Configure ports

Max Connection	50	(1-50)
TCP Port	37777	(1025-65535)
HTTP Port	80	
HTTPS Port	443	
RTSP Port	554	
Apply Refresh Default		

Table 4-17 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.
RTSP Port	Default value is 554.

Step 3 Click **Apply**.

4.10.1.5 Configuring Basic Service

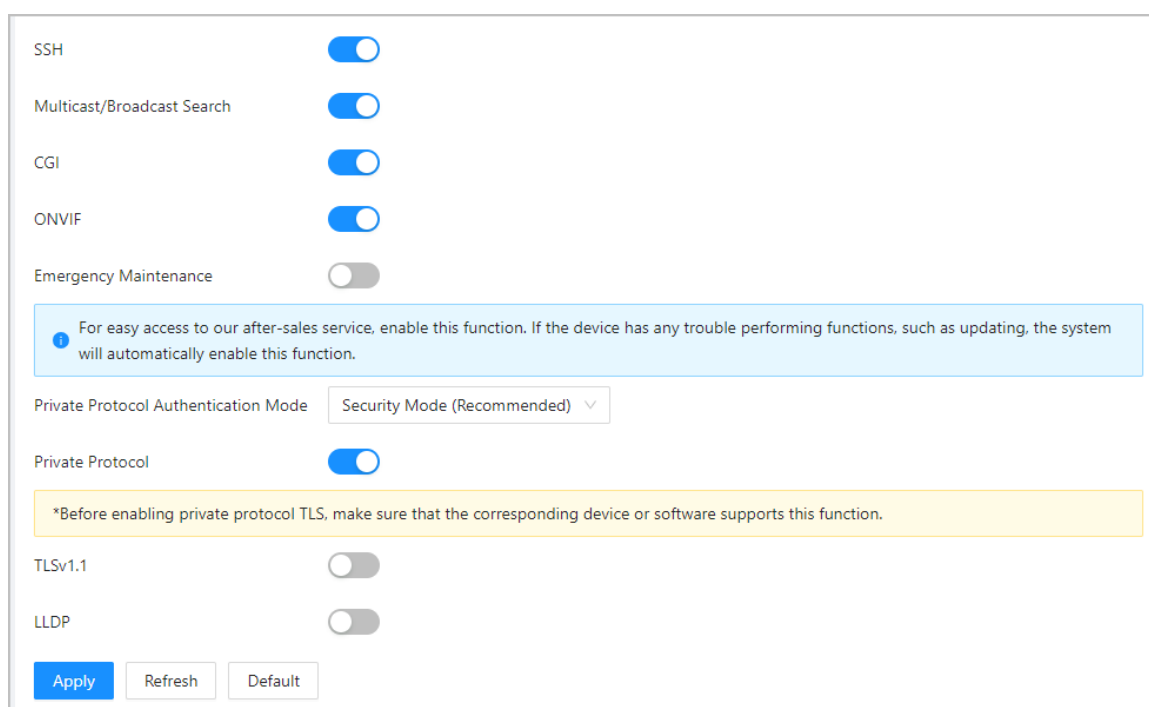
When you want to connect the Device to a third-party platform, turn on the CGI and ONVIF functions.

Procedure

Step 1 Select **Communication Settings > Network Settings > Basic Services**.

Step 2 Configure the basic service.

Figure 4-44 Basic service



SSH ☒

Multicast/Broadcast Search ☒

CGI ☒

ONVIF ☒

Emergency Maintenance ☐

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

Private Protocol Authentication Mode Security Mode (Recommended) ▾

Private Protocol ☒

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

TLSv1.1 ☐

LLDP ☐

Apply Refresh Default

Table 4-18 Basic service parameter description

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

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

Step 3 Click **Apply**.

4.10.1.6 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 4-45 Cloud service

Enable ☒

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

P2P Status ● Offline

PaaS Status ● Offline

SN 8[REDACTED]759



Apply

Refresh

Step 3 Click **Apply**.

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

4.10.1.7 Configuring SDK Auto Registration

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

Background Information

The auto registration only supports SDK.

Procedure

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

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

121

Figure 4-46 Auto Registration

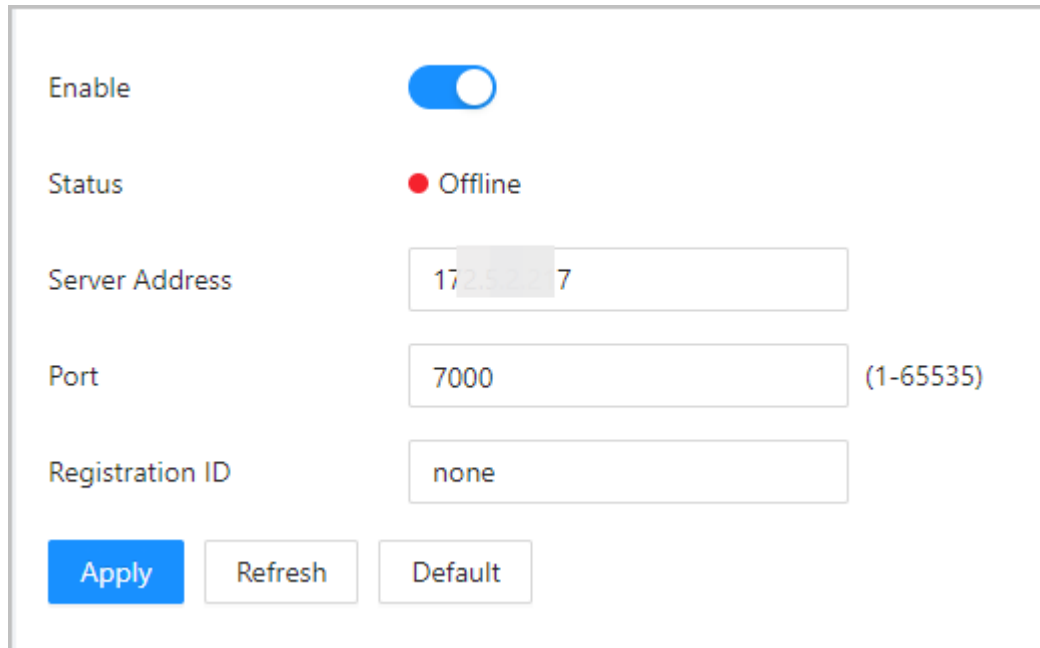


Table 4-19 Automatic registration description

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**.

4.10.1.8 Configuring CGI Auto Registers

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 configure the parameters.

Step 3 Click , and then configure parameters.

Figure 4-47 CGI auto registration

Edit [X]

Enable ☐

Device ID

Address Type

Host IP

Port

HTTPS ☐

Username

Password

[OK] [Cancel]

Table 4-20 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	- Host IP: Enter the IP address of the third-party platform. - Domain Name: Enter the domain name of the third-party platform.
Domain Name	
HTTPS	Access the third-party platform through HTTPS. HTTPS secures communication over a computer network.
Username/Password	Enter the username and password of the device.

Step 4 Click **OK**.

4.10.1.9 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 4-48 Automatic upload

No.	IP/Domain Name	Port	HTTPS	Path	Heartbeat	Authentication	Event Type	Test	Delete
1	192.168.1.108	80	☐	/	30		Person Info, Unlock Reco...	Test	

Table 4-21 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.
Event Type	Select the type of event that will be pushed to the management platform. - Before you use this function, enable Push Person Info. - Person information can only be pushed to one management platform and unlock records can be pushed to multiple management platforms.

Step 5 Click **Apply**.

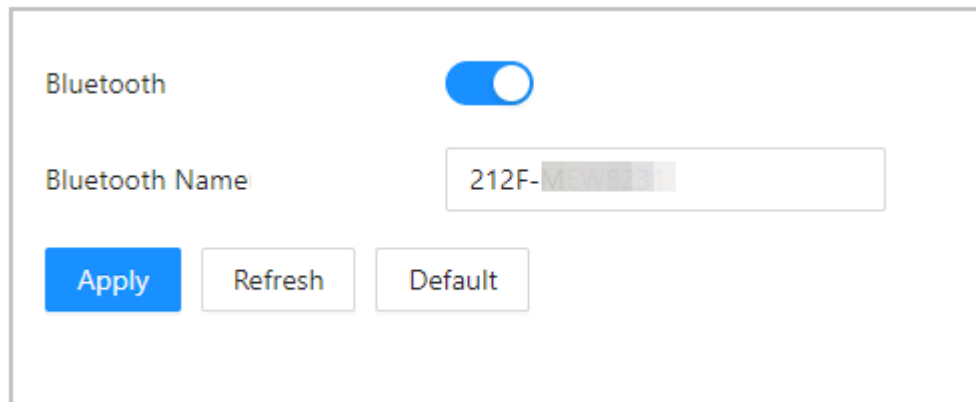
4.10.2 Bluetooth Settings

Configure the Bluetooth function of the Device. This function is only available on select models.

Procedure

- Step 1 Select **Communication Settings** > **Bluetooth Setting**.
- Step 2 Enable or turn off **Bluetooth**, configure Bluetooth name.

Figure 4-49 Bluetooth



- Step 3 Click **Apply**.

Results

You can unlock the door through the Bluetooth through the DMSS app. For details, see "3.6.3 Bluetooth".

4.10.3 Mode Settings

Log in to the webpage, and select **Communication Settings** > **Mode Settings**.

Card Reader Mode

Select **Mode** as **Card Reader**. The device serves as a card reader externally connected to an access control controller. It does not perform authentication but directly transmits access control information (such as card, password, fingerprint) to the access control controller, which then authenticates and unlocks the door.

Figure 4-50 Card reader mode

Mode

☒ Card Reader ☐ Access Controller

RS-485 Settings

Baud Rate

9600

▼

Data Bit

8

▼

Stop Bit

1

▼

Parity Code

None

▼

Wiegand Settings

Wiegand Output Type

Wiegand 34

▼

Pulse Width (μ s)

200

(20-200)

Pulse Interval (μ s)

1000

(200-5000)

The pulse width is a multiple of 10 and has a multiple relationship with the pulse interval.

Apply

Refresh

Default

Access Controller Mode

Set **Mode** as **Access Controller**.

Figure 4-51 Access controller mode

Mode

☐ Card Reader ☒ Access Controller

RS-485 Settings

External Device

Card Reader

?

Baud Rate

9600

Data Bit

8

Stop Bit

1

Parity Code

None

Wiegand Settings

Wiegand Settings

☒ Wiegand Input ☐ Wiegand Output

Card No. Inversion

☒

Apply

Refresh

Default

Table 4-22 Description of RS-485

External Device	Description
Access Controller	Select Access Controller when the Device functions as a card reader, and sends data to other external access controllers to control access. Output Data type: • Card Number: Outputs data based on card number when users swipe card to unlock door; outputs data based on user's first card number when they use other unlock methods. • ID: Outputs data based on the user ID.  • When authentication is successful, the relevant information is transmitted to the access controller. In this case, the authentication result displayed is the authentication result of the access controller. • When authentication fails, the relevant information is not transmitted to the access controller, and the authentication result displayed remains as failure.
Card Reader	The device is externally connected to a card reader and transmits access control card information to an access controller or management platform.
Card Reader (OSDP)	The device is externally connected to an OSDP card reader and transmits access control card information to an access controller or management platform.
Door Security Module	The door exit button, lock and fire linkage is not effective after the security module is enabled. • Supports authentication through face, card, fingerprint, password, and other methods to control the door security module for unlocking. • Supports unlocking through an externally connected RS-485 card reader or push-to-open button linked to the door control security module.  Remote unlock of the externally connected door lock through the door security module is not supported.
Lock Extension Module	When the Access Controller is connected to external lock extension module, if you select Lock Extension Module, the local lock is unlocked after you verify the identification on the local device, and the extension lock is unlocked after you verify the identification on the external card reader. After you select Lock Extension Module, you can select channel 2 on the Access Control Parameters and Alarm page on the webpage of the Access Controller.

Table 4-23 Description of Wiegand

Parameter		Description
Wiegand Settings		- When connecting an external card reader device, select Wiegand Input. - When the Device functions as a card reader, and you need to connect it to another access controller, and select Wiegand Output Config.
Wiegand Input	Card No. Inversion	If the card number sequence obtained through Wiegand input does not match the actual card number sequence when interfacing with third-party devices, enable this function.
Wiegand Output	Wiegand Output Type	The bit length of card numbers or ID that the device can recognize and output. - Wiegand 26: Reads 3 bytes or 6 digits. - Wiegand 34: Reads 4 bytes or 8 digits. - Wiegand 66: Reads 8 bytes or 16 digits.
	Pulse Width	Configure the pulse width and interval for wiegand output.
	Pulse Interval	
	Output Data Type	Select a Wiegand format to read card numbers or ID numbers. - User ID: Outputs data based on user ID. - Card: Outputs data based on user's first card number.
	Wiegand Format	When Output Data Type is set as ID , you can select decimal or hexadecimal output formats.

4.11 System Management

4.11.1 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.

4.11.1.1 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**.

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 4-52 Add administrators

The screenshot shows a dialog box titled "Add" with a close button (X) in the top right corner. Inside the dialog, there are four input fields arranged vertically. The first three fields are labeled with a red asterisk: "Username", "Password", and "Confirm Password". The fourth field is labeled "Remarks". Below the "Confirm Password" field, there is a horizontal bar with three segments, likely representing a password strength indicator. At the bottom right of the dialog, there are two buttons: "OK" (in blue) and "Cancel" (in white with a gray border).

Step 3 Click **OK**.



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

4.11.1.2 Adding ONVIF Users

Background Information

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

Procedure

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

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

Figure 4-53 Add ONVIF user

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

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

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

Table 4-24 ONVIF user description

Parameter	Description
Username	The username cannot be the same with existing account. The username consists of up to 31 characters and only allows for numbers, letters, underscores, midlines, dots, or @.
Password	The password must consist of 8 to 32 non-blank characters and contain at least two types of the following characters: Upper case, lower case, numbers, and special characters (excluding ' " ; : &).
Group	There three permission groups which represents different permission levels. • admin: You can view and manage other user accounts on the ONVIF Device Manager. • Operator: You cannot view or manage other user accounts on the ONVIF Device Manager. • User: You cannot view or manage other user accounts and system logs on the ONVIF Device Manager.

Step 3 Click **OK**.

4.11.1.3 Resetting the Password

Reset the password through the linked email when you forget your password.

Procedure

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

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

Step 3 Turn on the password reset function.

Figure 4-54 Reset Password

Password Reset

Enable ☒

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

Email Address

Password Expires in Days



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

Step 4 Click **Apply**.

4.11.2 Viewing Online Users

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

4.11.3 Configuring Time

Procedure

- Step 1 On the home page, select **System > Time**.
- Step 2 Configure the time of the Platform.

Figure 4-55 Date settings

Time and Time Zone



Date :

2024-11-04 Monday

Time :

5:44:03 PM

Time

☒ Manually Set

☐ NTP

System Time

2024-11-04 5:44:03 PM



Sync PC

Time Format

YYYY-MM-DD



12-Hour



Time Zone





DST

Enable

☐

Type

☒ Date

☐ Week

Start Time

Jan



1



12:00 AM



End Time

Jan



2



12:00 AM



Apply

Refresh

Default

Table 4-25 Time settings description

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

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

Step 3 Click **Apply**.

4.11.4 Configuring Always On

Procedure

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

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

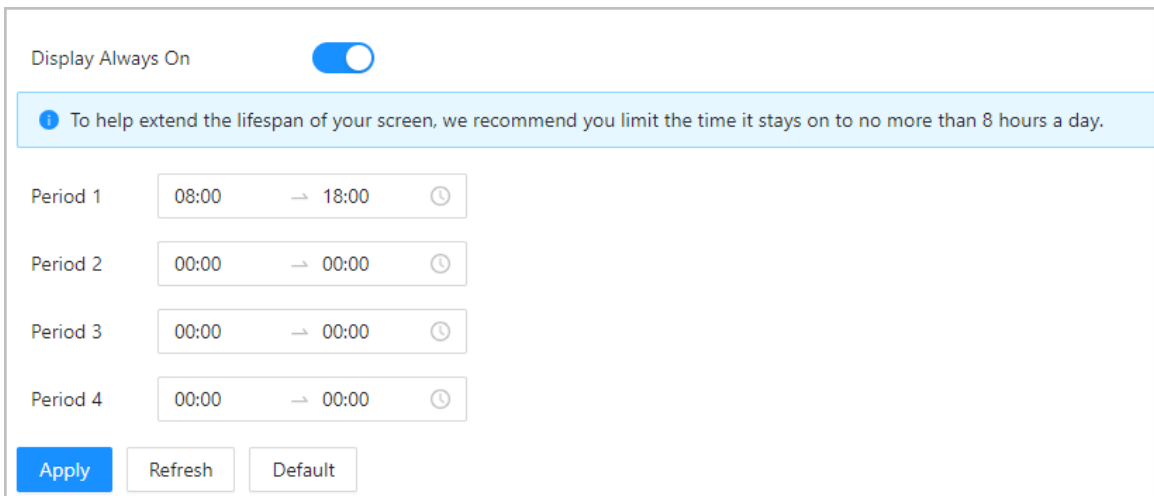
The screen will stay on during the set time period after being enabled.



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

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

Figure 4-56 Always on



4.12 Maintenance Center

4.12.1 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**.

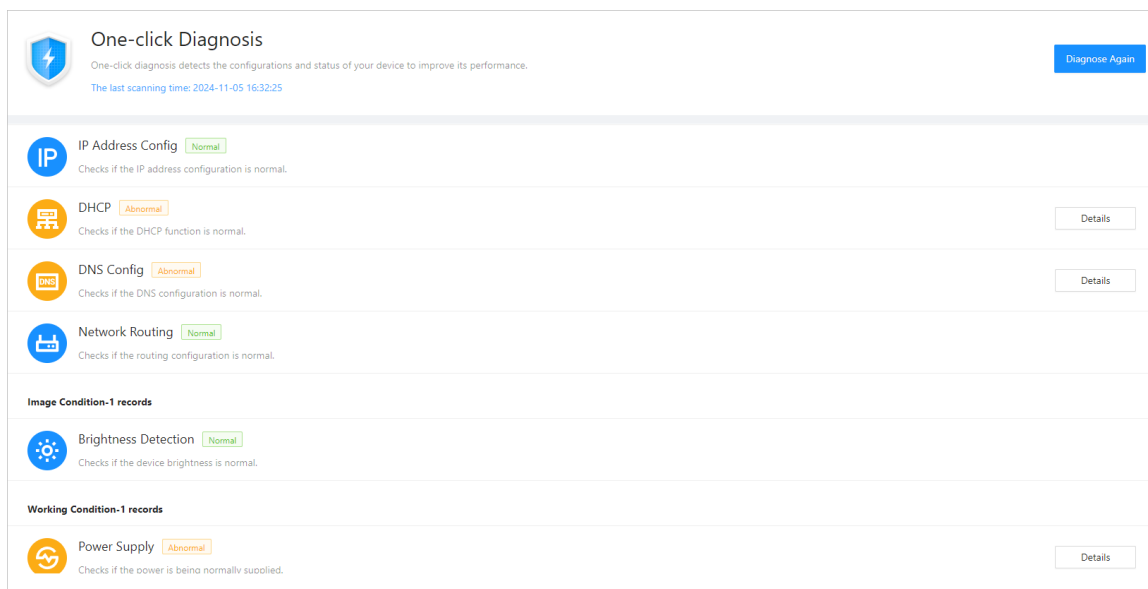
Step 2 Click **Diagnose**.

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 4-57 One-click diagnosis



4.12.2 System Information

4.12.2.1 Viewing Version Information

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

4.12.2.2 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.

4.12.3 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**.

4.12.4 Viewing Logs

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

4.12.4.1 System Logs

Search for and view 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.

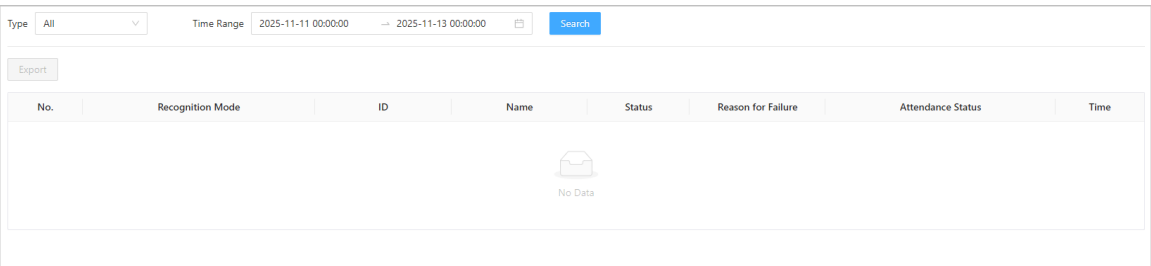
4.12.4.2 Unlock Records

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**.

Figure 4-58 Unlock records



Related Operations

Click **Export** to export the unlock records to your computer.

4.12.4.3 Call History

View call logs.

Procedure

- Step 1 Log in to the webpage.
- Step 2 Select **Maintenance Center > Log > Call History**.

4.12.4.4 Alarm Logs

View alarm logs.

Procedure

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

4.12.4.5 Admin Logs

Search for admin logs by using admin ID.

Procedure

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

4.12.4.6 USB Management

Export user information from/to USB.

Procedure

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



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

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

4.12.5 Maintenance Management

4.12.5.1 Configuration Management

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

4.12.5.1.1 Exporting and Importing Configuration Files

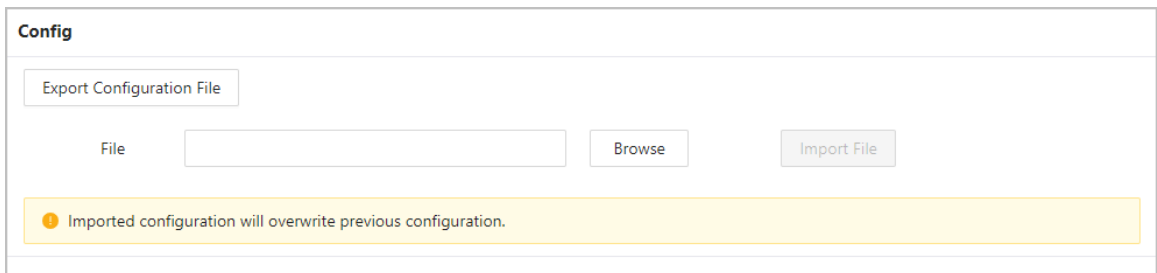
You can import and export the configuration file for the Device. When you want to apply the same configurations to multiple devices, you can import the configuration file to them.

Procedure

Step 1 Log in to the webpage.

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

Figure 4-59 Configuration management



The screenshot shows a web interface titled "Config". At the top, there is a button labeled "Export Configuration File". Below this, there is a section for importing a file. It includes a text input field labeled "File", a "Browse" button, and an "Import File" button. A yellow warning banner at the bottom of the import section states: "Imported configuration will overwrite previous configuration."

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.

4.12.5.1.2 Configuring Fingerprint Threshold

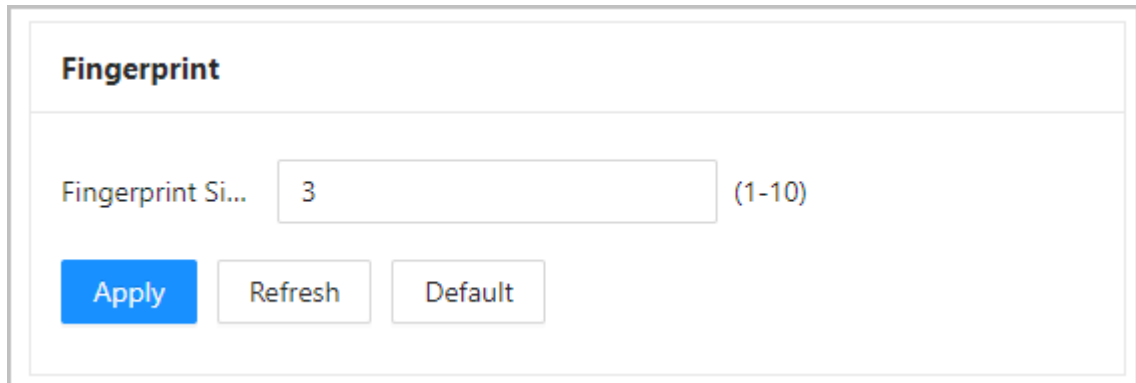
Select **Maintenance Management** > **Config**. Configure the fingerprint threshold according to the actual situation. The larger the value, the higher the fingerprint matching accuracy, the lower the false recognition rate, while the pass rate also decreases.



For the device with the fingerprint function, this configuration is displayed.

Enter the fingerprint similarity threshold, and then click **Apply**.

Figure 4-60 Fingerprint threshold



4.12.5.1.3 Restoring the Factory Default Settings

Procedure

- Step 1 Select **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.

- **Restore to Factory Settings (Keeps Network Config)** : Resets all the configurations of the Device except for the network configuration.
- **Restore to Default (Keeps Logs, User Info, and Network Config)** : Resets the configurations of the Device and deletes all the data except for user information, logs and network configurations.

4.12.5.2 Maintenance

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

Procedure

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

4.12.6 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.

4.12.6.1 File Update

Procedure

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

4.12.6.2 Online Update

Procedure

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

4.12.7 Advanced Maintenance

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

4.12.7.1 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.

4.12.7.2 Packet Capture

Packet Capture

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

Figure 4-61 Packet capture

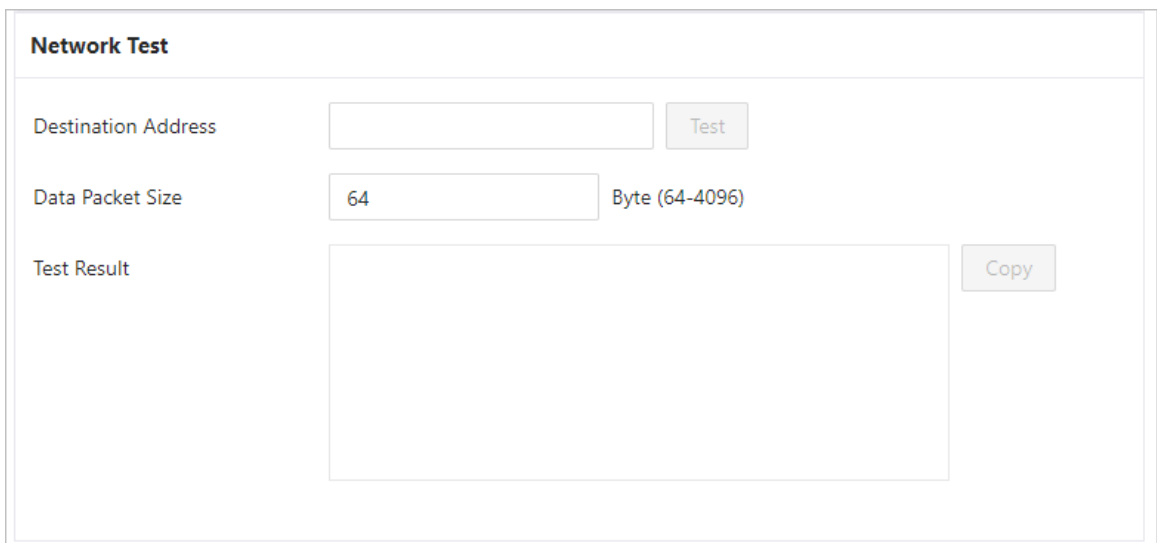
Packet Capture							
NIC	Device Address	IP 1: Port 1		IP 2: Port 2		Packet Sniffer Size	Packet Sniffer Backup
eth0	192.168.1.166	Optional	Optional	Optional	Optional	0.00MB	►
eth2	192.168.1.101	Optional	Optional	Optional	Optional	0.00MB	►

2. Enter the IP address, click .
 -  changes to .
 3. After you acquired enough data, click .
- Captured packets are automatically downloaded to your local computer.

Network Test

1. On the home page, select **Maintenance Center** > **Advanced Maintenance** > **Packet Capture**.
2. In the **Network Test** area, enter the destination address, and then configure data packet size.

Figure 4-62 Network test



Network Test

Destination Address

Data Packet Size Byte (64-4096)

Test Result

3. Click **Test**.
- The result is displayed in the **Test Result** area. You can copy the result.

4.13 Security Settings(Optional)

4.13.1 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.

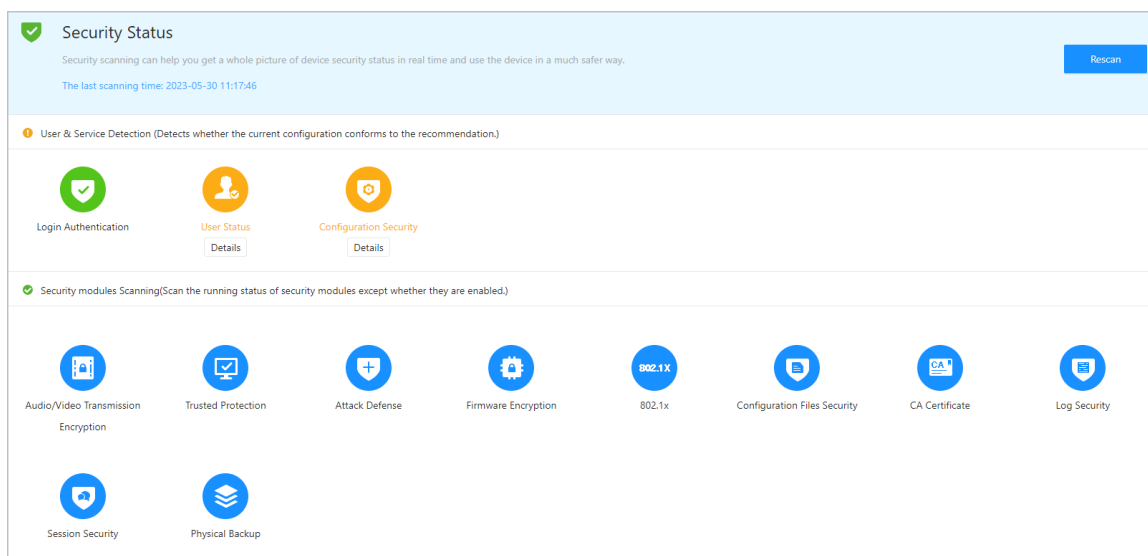
Procedure

- 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 4-63 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.

4.13.2 Configuring HTTPS

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** > **HTTPS**.

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 4-64 HTTPS

HTTPS

Enable ☒

HTTPS is a service entry based on Transport Layer Security (TLS). HTTPS provides web service, ONVIF access service and RTSP access service.

*Select a device certificate [Certificate Management](#)

No.	Custom Name	Certificate Serial Number	Validity Period	User	Issued by	Used by
1		39303032613930393531396631363835343436383232	2053-05-30 11:40:22	8C04F30YA16759	BSC	HTTPS, RTSP over TLS

Apply Refresh Default Download Root Certificate

Step 4 Click **Apply**.

Enter "https://IP address: https port" 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.

4.13.3 Attack Defense

4.13.3.1 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 4-65 Firewall

Firewall Account Lockout Anti-DoS Attack

Enable ☒

Mode ☒ Allowlist ☐ Blocklist

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

Add Delete

No.	Host IP/MAC	Port	Operation
1	15...S.0.6	All Device Ports	

Total 1 records

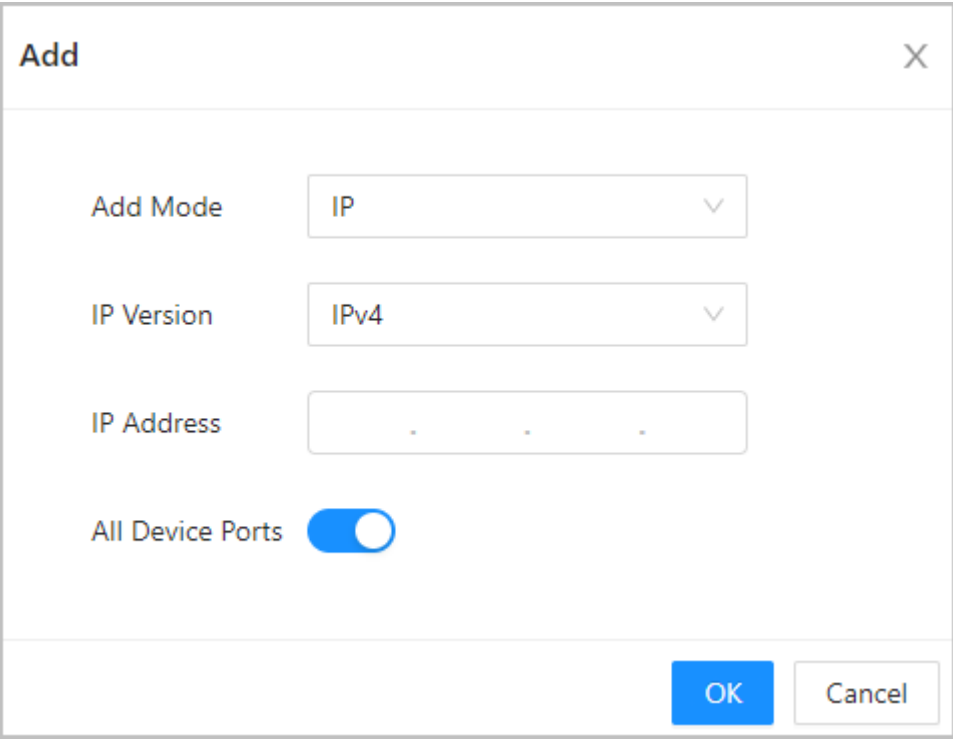
Apply Refresh Default

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

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

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

Figure 4-66 Add IP information

A dialog box titled "Add" with a close button (X) in the top right corner. It contains four fields: "Add Mode" with a dropdown menu showing "IP", "IP Version" with a dropdown menu showing "IPv4", "IP Address" with a text input field containing three dashes, and "All Device Ports" with a toggle switch that is currently turned on. At the bottom right, there are two buttons: "OK" and "Cancel".

Add X

Add Mode IP

IP Version IPv4

IP Address . . .

All Device Ports ☒

OK Cancel

Step 5 Click **OK**.

Related Operations

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

4.13.3.2 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 4-67 Account lockout

Firewall **Account Lockout** Anti-DoS Attack

Device Account

Login Attempt 5time(s) ▼

Lock Time 5 min

Apply Refresh Default

- 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**.

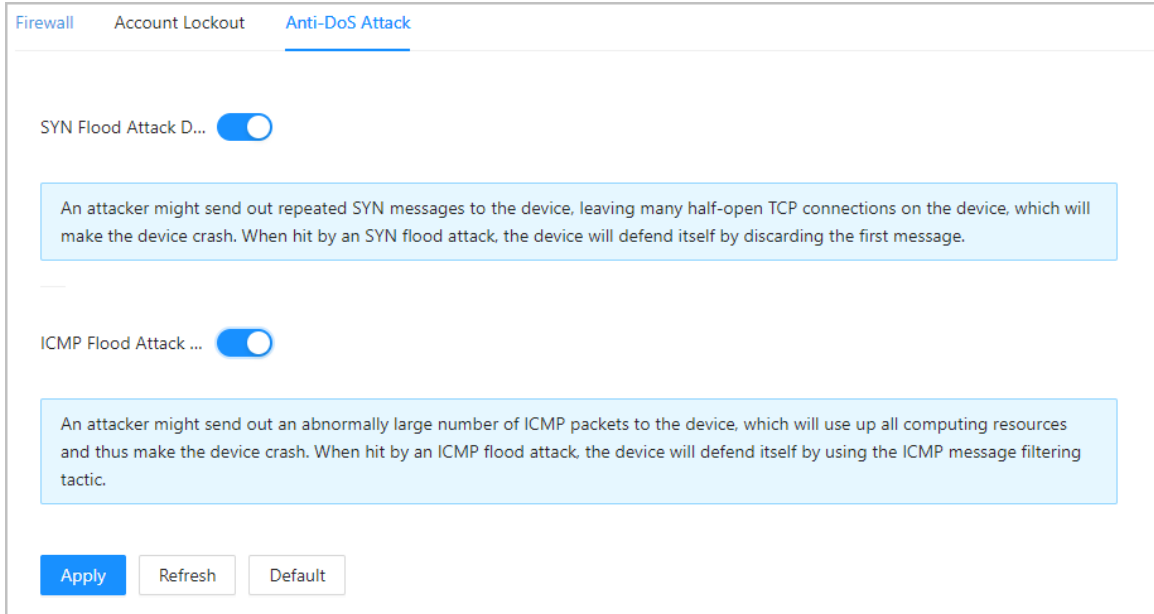
4.13.3.3 Configuring Anti-DoS Attack

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 4-68 Anti-DoS attack



Firewall Account Lockout **Anti-DoS Attack**

SYN Flood Attack D... ☒

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

ICMP Flood Attack ... ☒

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

Apply Refresh Default

Step 3 Click **Apply**.

4.13.4 Installing Device Certificate

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

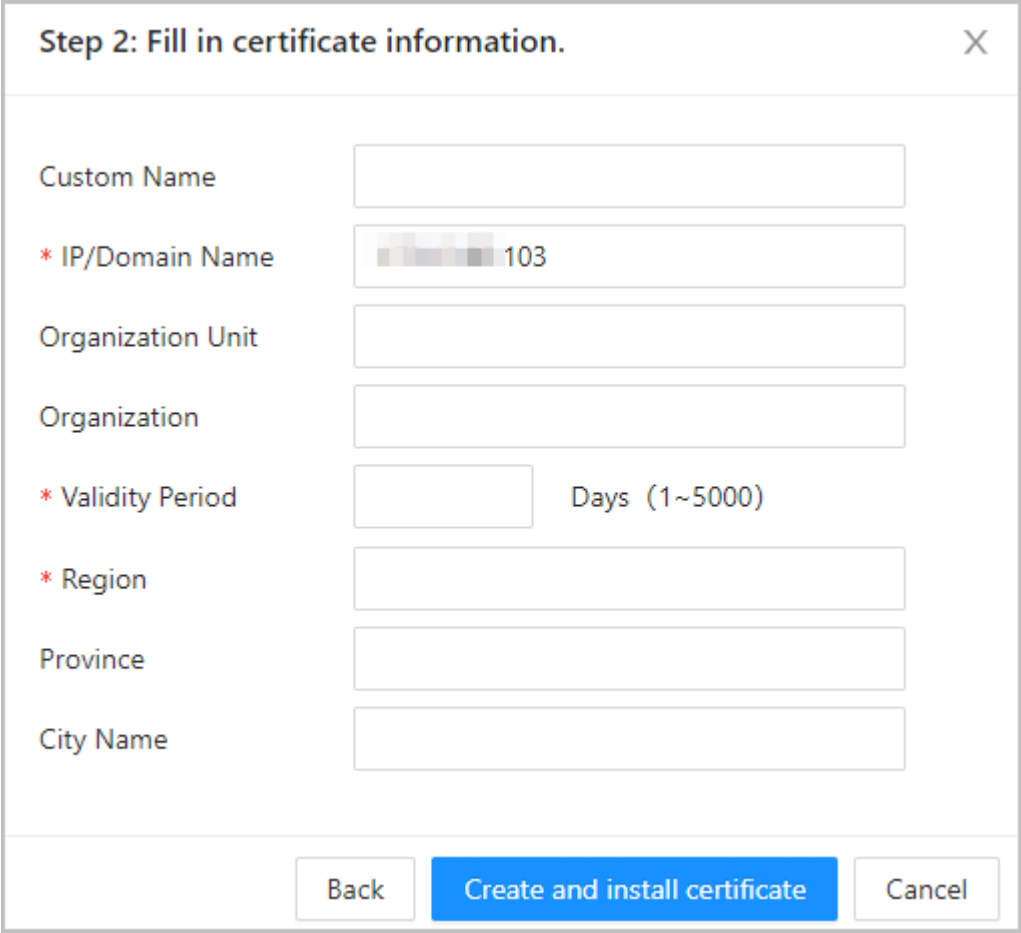
4.13.4.1 Creating Certificate

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 4-69 Certificate information



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

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

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

Related Operations

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

4.13.4.2 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 4-70 Certificate information (2)

Step 2: Fill in certificate information.

* IP/Domain Name: 172.16.0.03

Organization Unit:

Organization:

* Region:

Province:

City Name:

Back Create and Download Cancel

Step 5 Click **Create and Download**.

Save the request file to your computer.

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

Step 7 Import the signed CA certificate.

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

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

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

Related Operations

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

4.13.4.3 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 4-71 Certificate and private key

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

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

Related Operations

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

4.13.5 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.

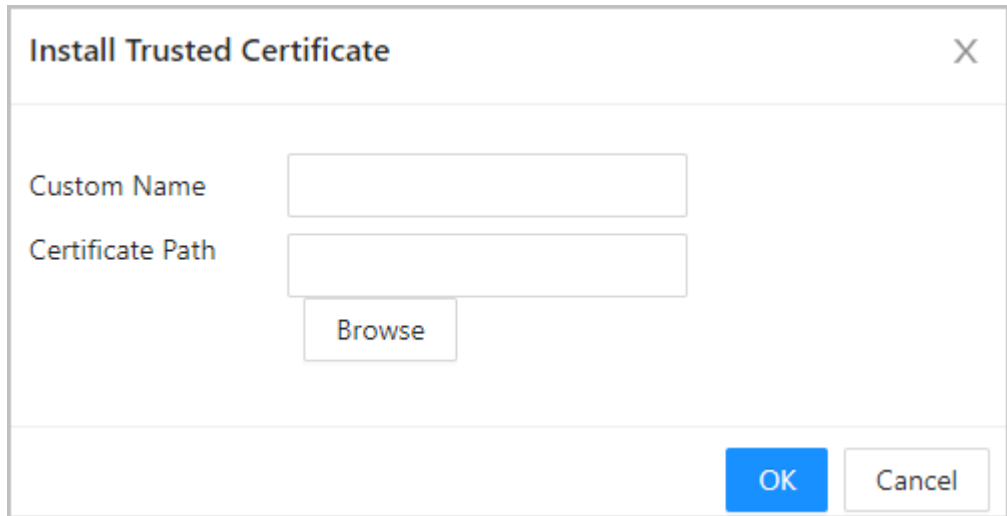
Background Information

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 4-72 Install the trusted certificate

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

Install Trusted Certificate

Custom Name

Certificate Path

Step 4 Click **OK**.

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

Related Operations

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

4.13.6 Security Warning

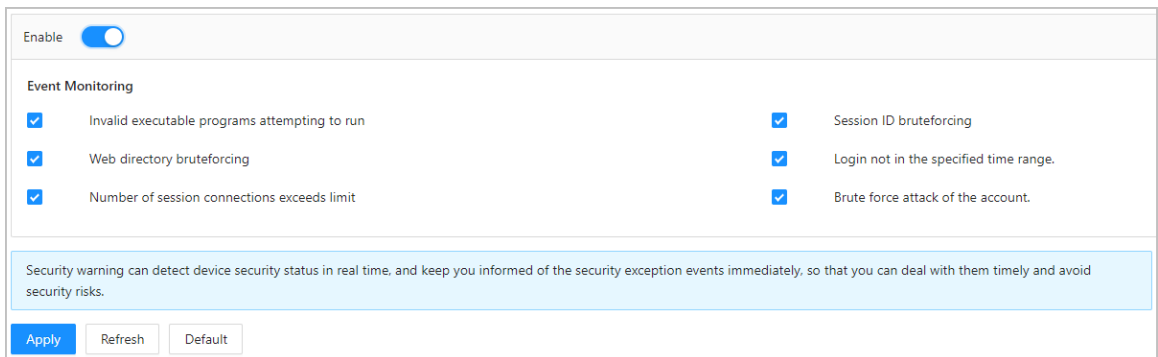
Procedure

Step 1 Select  > **Security Warning**.

Step 2 Enable the security warning function.

Step 3 Select the monitoring items.

Figure 4-73 Security warning

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

Enable ☒

Event Monitoring

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

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

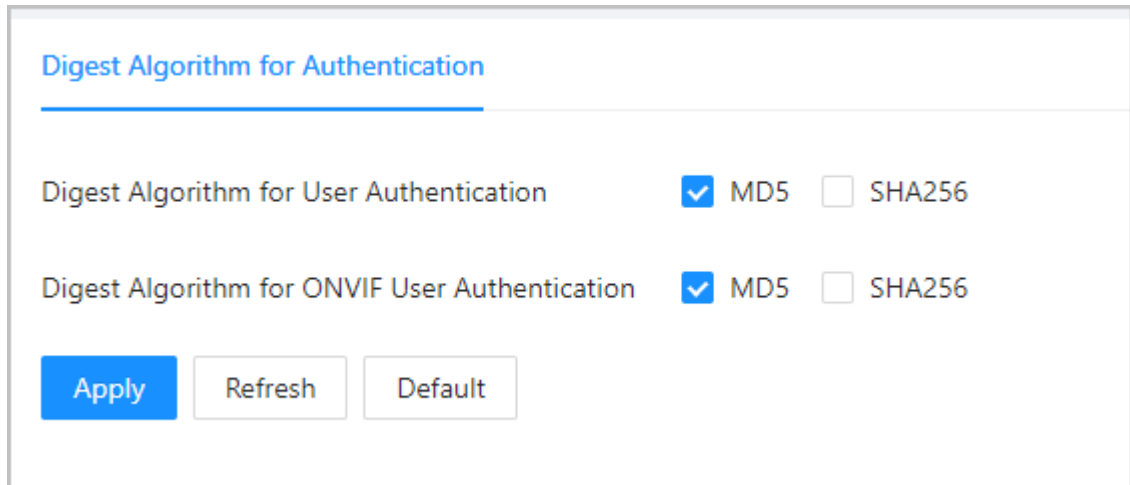
Step 4 Click **Apply**.

4.13.7 Security Authentication

Procedure

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

Figure 4-74 Security Authentication



The screenshot displays a web interface for configuring security authentication. At the top, the title "Digest Algorithm for Authentication" is underlined in blue. Below this, there are two rows of configuration options. The first row is labeled "Digest Algorithm for User Authentication" and has two radio button options: "MD5" (which is selected, indicated by a blue checkmark) and "SHA256" (which is unselected). The second row is labeled "Digest Algorithm for ONVIF User Authentication" and also has two radio button options: "MD5" (selected with a blue checkmark) and "SHA256" (unselected). At the bottom of the form, there are three buttons: "Apply" (highlighted in blue), "Refresh", and "Default".

5 Phone Operations

5.1 Initialization

When the phone is on the same LAN as the Access Controller, you can initialize the Access Controller for the first time or after the Device is restored to the factory defaults on the webpage of the phone. This section introduces initialization on the phone through Wi-Fi AP.

Prerequisites

Make sure that the Access Controller is not connected to Wi-Fi or 4G network.



The Wi-Fi and Wi-Fi AP are available on select models.

Procedure

Step 1 Power on the Device.

Step 2 30 seconds after the device enters the initialization screen, connect to the Wi-Fi hotspot on your phone. The hotspot name is **product serial number + device model**.

If you have not connected to the Wi-Fi hotspot within 30 minutes, the hotspot is off.

Step 3 Open a browser on your phone, and go to the IP address (the default address is 192.168.3.1) of the hotspot.

Step 4 Tap **Start Initialization**.

Step 5 Select the language.

Step 6 Enter and confirm the password, enter an email address, and then tap **Next**.



- 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.
- If you want to reset the administrator password by scanning the QR code, you need the linked email address to receive the security code.

Step 7 Enable **Auto Check** as needed, and then tap **Completed**.

5.2 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.

You can log in to the webpage through the following 3 methods:

- The phone and the Device are in the same LAN. Open the browser on the phone, and then enter the IP address.

- The phone and the Device are in the same LAN. Scan the QR code through **Communication Settings** > **Network Settings** > **Wi-Fi** on the webpage of your phone.
- Connect the hotspot of the Device on your phone. On the main screen of the device, tap the upper-right corner to go to **Wi-Fi AP** screen. Scan the IP address QR code through the browser on your phone, or in the browser of your phone, enter the IP address that is displayed in the **Wi-Fi AP** screen.

You can also select **Communication Settings** > **Network Settings** > **Wi-Fi AP** to go to the main menu.



Wi-Fi and Wi-Fi AP are available on select models.

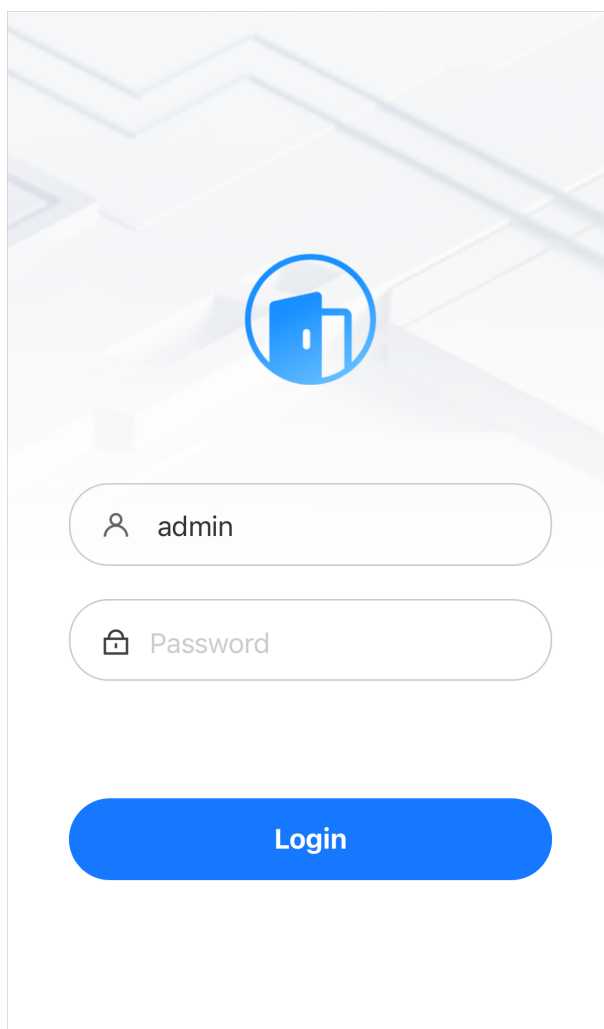
Step 2 Enter the user name and password.

Click  next to the password to view it.



- 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 "4.3 Resetting the Password".

Figure 5-1 Login page



Step 3 Tap **Login**.

5.3 Home Page

The home page is displayed after you successfully log in.

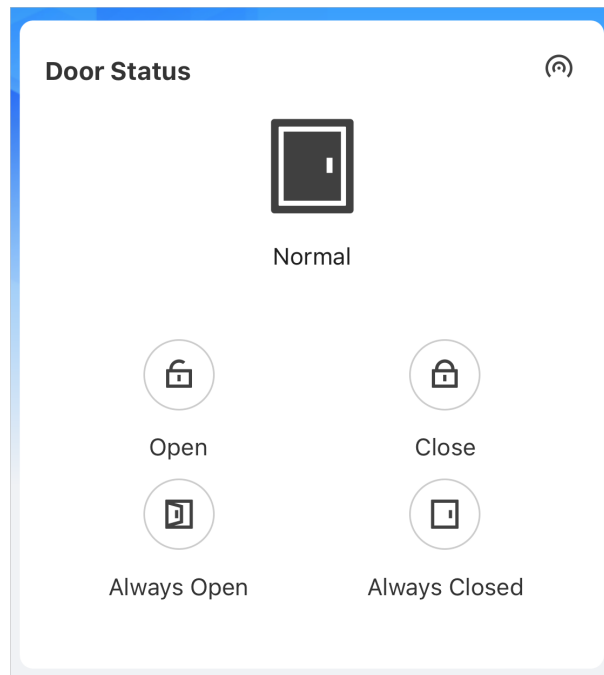
- Tap  at the upper-right corner of the webpage, and then tap **Product Documentation QR Code** to scan the QR code to get the product material or tap **Logout** to log out the account.



The product document is available on select models.

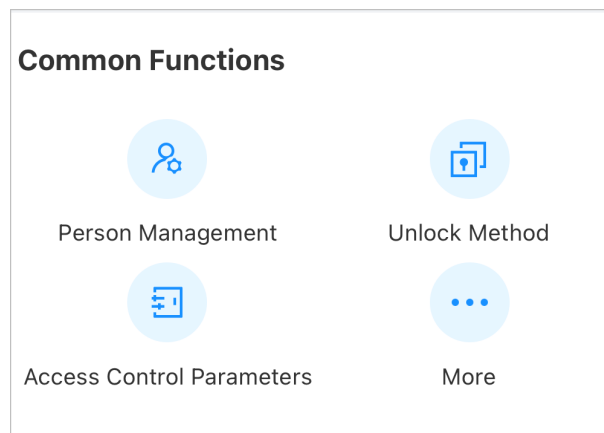
- The **Door Status** area displays the status of the door. You can remotely open or close the door. You can also configure the door status as **Always Open** or **Always Closed**.
 - ◇  indicates the wired network is connected.
 - ◇  indicates the Wi-Fi hotspot is turned on.

Figure 5-2 Door status



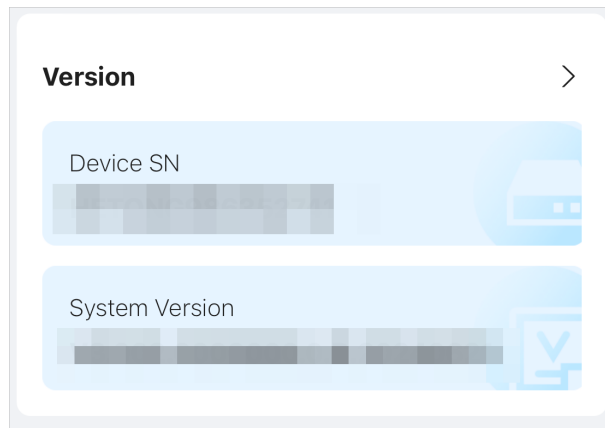
- The **Common Functions** area displays the configuration menu of the Device. Tap **More** to view all the configuration menus.

Figure 5-3 Common functions



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

Figure 5-4 Version



5.4 Person Management

Add the person and configure the permissions.

Procedure

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

Figure 5-5 Add the person (1)

A screenshot of a mobile application form titled 'Add the person (1)'. The form is divided into three main sections: 'Basic Info', 'Access Credentials', and 'Verification Mode'. The 'Basic Info' section contains two input fields: '* ID' and 'Name'. The 'Access Credentials' section contains four rows: 'Password' with the value 'Not Added', 'Card' with the value '0', 'Fingerprint' with the value '0', and 'Bluetooth Card' with the value '0'. The 'Bluetooth Card' row has a note: 'No email was configured. You cannot request a Bluetooth card through email.' The 'Verification Mode' section contains two rows: 'Verification Mode' with the value 'Same as Device' and 'Permission' with the value 'User'. Each row has a right-pointing chevron.

Figure 5-6 Add the person (2)

Validity Period	Forever >
Email	
General Plan	255-Default >
Holiday Plan	255-Default >
User Type	General User >
Times Used	Unlimited
Department	1-10-11 >
Schedule Mode	Department Schedule >
Permission Type	Unlock and Attendance >
Add	

Table 5-1 Parameters description

Parameter	Description
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 contain 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.
Card	Tap Add, manually enter the card number or swipe the card in the card swiping area of the Device. A user can register up to 5 cards at most. After adding successfully, tap the added card, you can change the card number, configure the card as the duress card or delete the card. If you turn on the duress alarm, an alarm will be triggered if a duress card is used to unlock the door.  One user can only set one duress card.

Parameter	Description
Fingerprint	Register fingerprints. A user can register up to 3 fingerprints, and you can set a fingerprint to the duress fingerprint. An alarm will be triggered when the duress fingerprint is used to unlock the door. 1. Tap Add. 2. Press finger on the scanner according to the on-screen instructions. 3. Tap OK.  • Fingerprint function is only available on select models. • We do not recommend you set the first fingerprint as the duress fingerprint. • One user can only sets one duress fingerprint.
Bluetooth Card	 Bluetooth is only available on select models. You can select Request through Email or Request through Registration Code. • Request through Email : Suitable for the first time a Bluetooth card is requested. You can request up to 5 Bluetooth cards, and have to use the email that is registered to DMSS.  You must have entered your reserved Email before you use the function. 1. Configure the Email that is registered to DMSS. 2. Click Request through Email, and then the Bluetooth cards can be requested. • Request through Registration Code : Suitable when you already have a Bluetooth card and want to reuse it on another access controller supporting Bluetooth function. 1. Copy the Bluetooth registration code from the DMSS. 2. Click Request through Registration Code, and then enter the code. 3. Click OK.
Verification Mode	Configure the verification mode for the person. You can use the mode that is the same as the device or customize the mode. • Same as Device : The mode is the same as the device. • Custom : After you select Custom, Combination Method and Unlock Method are displayed. Select the combination method and unlock methods as needed. ◇ Or: Use one of the selected unlock methods to open the door. ◇ And: Use all the selected unlock methods to open the door.  ◇ The customized verification mode is only valid for the local device. It cannot be used in external card readers. ◇ When the customized verification mode is different from the mode of the device, the customized mode takes the priority.

Parameter	Description
Permission	● User : Users only have door access or time attendance permissions. ● Admin : Administrators can configure the Device besides door access and attendance permissions.
Validity Period	Set a date on which the door access and attendance permissions of the person will be expired.
General Plan	People can unlock the door or take attendance during the defined period.  You can select more than one plan.
Holiday Plan	People can unlock the door or take attendance during the defined holiday.  You can select more than one holiday.
Lock Permission	Select the local and external lock as needed.
User Type	● General User : General users can unlock the door. ● Blocklist User : When users in the blocklist unlock the door, service personnel will receive a notification. ● Guest User : Guests can unlock the door within a defined period or for certain amount of times. After the defined period expires or the unlocking times runs out, they cannot unlock the door. ● Patrol User : Patrol users can take attendance on the Device, but they do not have door permissions. ● VIP User : When VIP unlock the door, they are not restricted by unlock modes, such as Multi-card and Time Section. ● Other User : When they unlock the door, the door will stay unlocked for 5 more seconds. ● Custom User 1/Custom User 2: Same with general users.
Time Used	Set an unlock limit for guest users. After the unlock times run out, they cannot unlock the door.
Department	Add users to a department. If a department schedule is assigned to the person, they will follow the established department schedule.
Schedule Mode	● Department Schedule: Assign department schedule to the user. ● Personal Schedule: Assign personal schedule to the user.  ◇ This function is only available on select models. ◇ If you set the schedule mode to department schedule here, the personal schedule you have configured for the user in Attendance > Schedule Config > Personal Schedule is invalid.
Permission Type	● Unlock and attendance: Person has the permission of attendance and can unlock the door using the configured verification methods. ● Attendance: Person only has the permission of attendance and cannot unlock the door. After the person successfully verifies the identification, one failed unlock record is generated.

Step 4 Tap **Add**.

5.5 Configuring the System

5.5.1 Viewing Version Information

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

5.5.2 Configuration Management

Procedure

Step 1 Log in to the webpage.

Step 2 Select **More** > **System** > **Config**.

Step 3 Restore to the factory default settings if necessary.

- **Restore to Factory Settings (Keeps Network Config)** : Resets all the configurations of the Device except for the network configuration.
- **Restore to Default (Keeps Logs, User Info, and Network Config)** : Resets the configurations of the Device and deletes all the data except for user information, logs and network configurations.

5.5.3 Maintenance

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

Procedure

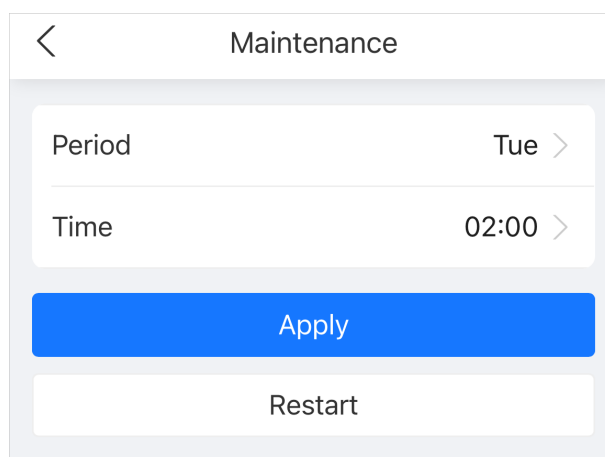
Step 1 Log in to the webpage.

Step 2 Select **More** > **System** > **Maintenance**.

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

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

Figure 5-7 Maintenance



5.5.4 Configuring Time

Procedure

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

Figure 5-8 Configure the time parameters

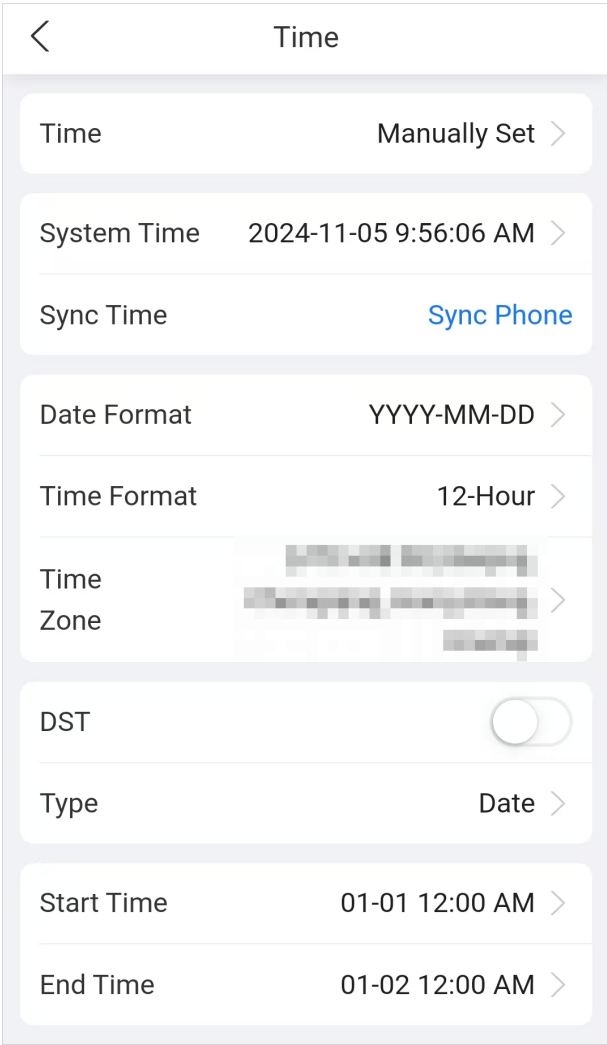


Table 5-2 Time settings description

Parameter	Description
Time	- Manual Set: Manually enter the time or you can tap Sync Phone to sync time with the phone. - NTP: The Device will automatically sync the time with the NTP server. Server : Enter the domain of the NTP server. Port : Enter the port of the NTP server. Interval : Enter its time with the synchronization interval.

Parameter	Description
Date Format	Select the date format and the time format.
Time Format	
Time Zone	Select the time zone.
DST	1. (Optional) Enable DST. 2. Select Date or Week as the Type. 3. Configure the start time and end time of the DST.

Step 4 Tap **Apply**.

5.5.5 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**.

5.5.6 Language

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

5.6 Configuring Attendance

This function is only available on select models.

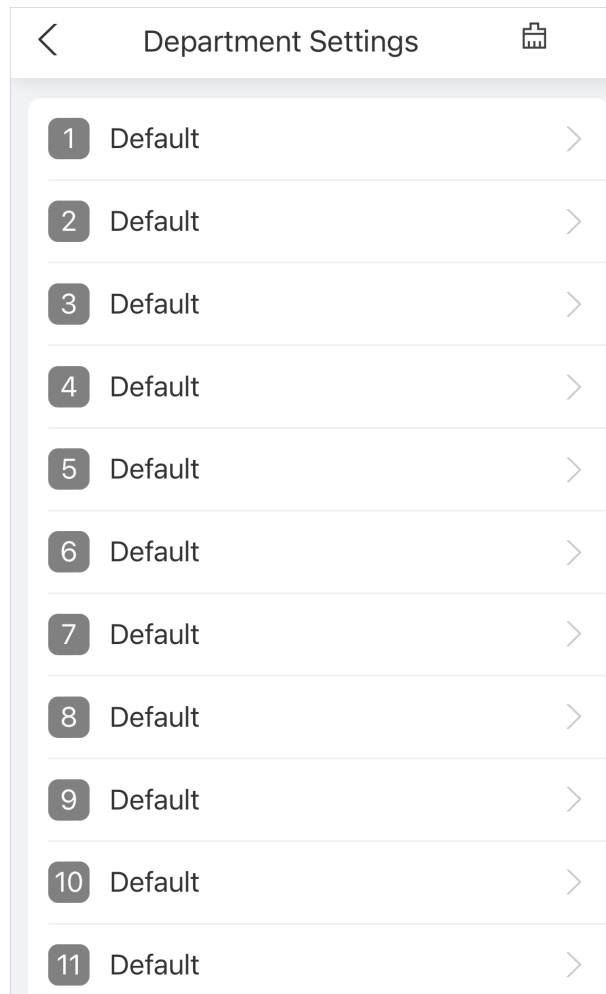
5.6.1 Configuring Departments

Procedure

Step 1 Log in to the webpage.

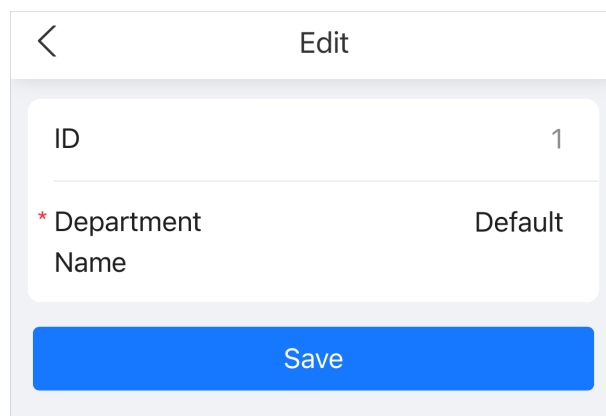
Step 2 Select **More > Attendance Config > Department Settings**.

Figure 5-9 Department settings



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

Figure 5-10 Rename the department



Related Operations

You can tap  to restore departments to default settings.

5.6.2 Configuring Shifts

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

Procedure

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

Figure 5-11 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 Tap the shift to configure the shift parameters, and then tap **Save**.

Figure 5-12 Configure the shift

Edit Shift

Shift No.1

* Shift Name

Period 1

08:00~17:00

Period 2

00:00~00:00

Period 3

00:00~00:00

Overtime Period

00:00~00:00

* Limit for Arriving Late5 min

* Limit for Leaving Early5 min

Save

Table 5-3 Shift parameters description

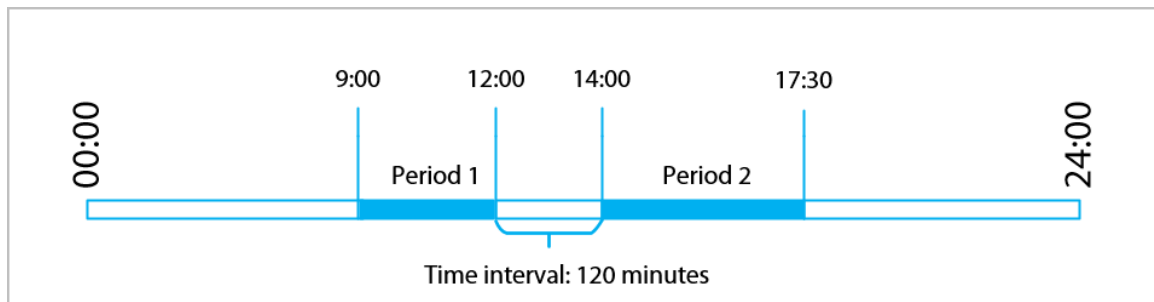
Parameter	Description
Shift Name	Enter the name of the shift.
Period 1	Specify a time range when people can clock in and clock out for the workday. You must configure at least 1 period. - If you only set one attendance period, employees need to clock in and out by the designated times to avoid an anomaly appearing on their attendance records. 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. - If you set 3 periods, the 3 periods cannot overlap. Employees need to clock in and clock out for adjacent 2 periods.  The last period can cross days. If the overtime period is the last one, you can configure it to crosses days.
Period 2	
Period 3	

Parameter	Description
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 you configure more than one periods, refer to the following instructions to perform attendance function.

- 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 5-13 Time interval (even number)



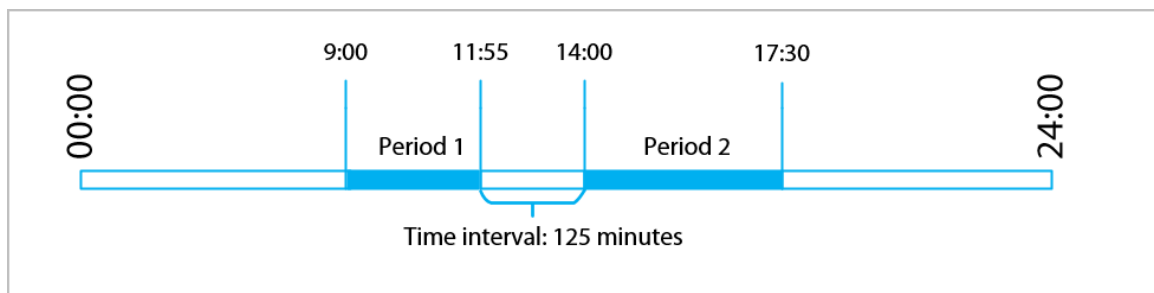
For example: If the interval is 120 minutes, then the clock-out time for period 1 is from 12:00 to 12:59, and the clock-in time for period 2 is from 13:00 to 14:00.



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 5-14 Time interval (odd 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.

- If there is only one period, and you do not clock in or out by the designated time, it is considered as absent for 1 day.
- If there are more than one period, and you do not clock in or out by the designated time of one period, it is considered as absent for 0.5 days. If you do not clock in or out by the designated time of 2 or more than 2 periods, it is considered as absent for 1 day. Attendance during overtime periods does not change the absent status of the person.

When you configure the last period to cross days, refer to the following instructions to perform attendance function.

- If the second day is the normal shift, the attendance is as normal.
- If the second day is the holiday, you can clock out in any time of 24 hours in the holiday day.



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 tap  to restore shifts to factory defaults.

5.6.3 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 Tap + to add holiday plans.
- Step 4 Configure the parameters, and then tap **Save**.

Figure 5-15 Add the holiday

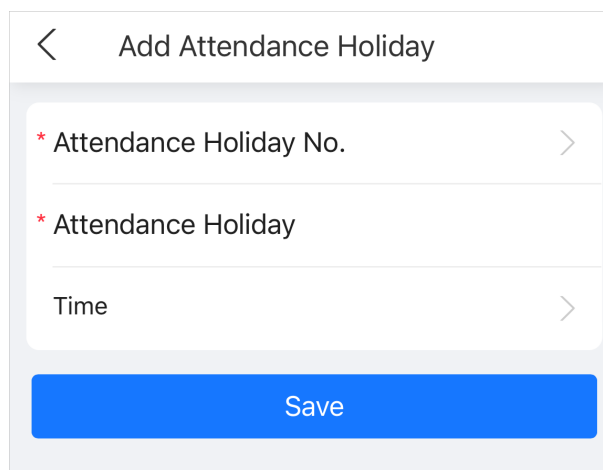


Table 5-4 Parameters description

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 Tap **OK**.

5.6.4 Configuring Work Schedules

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

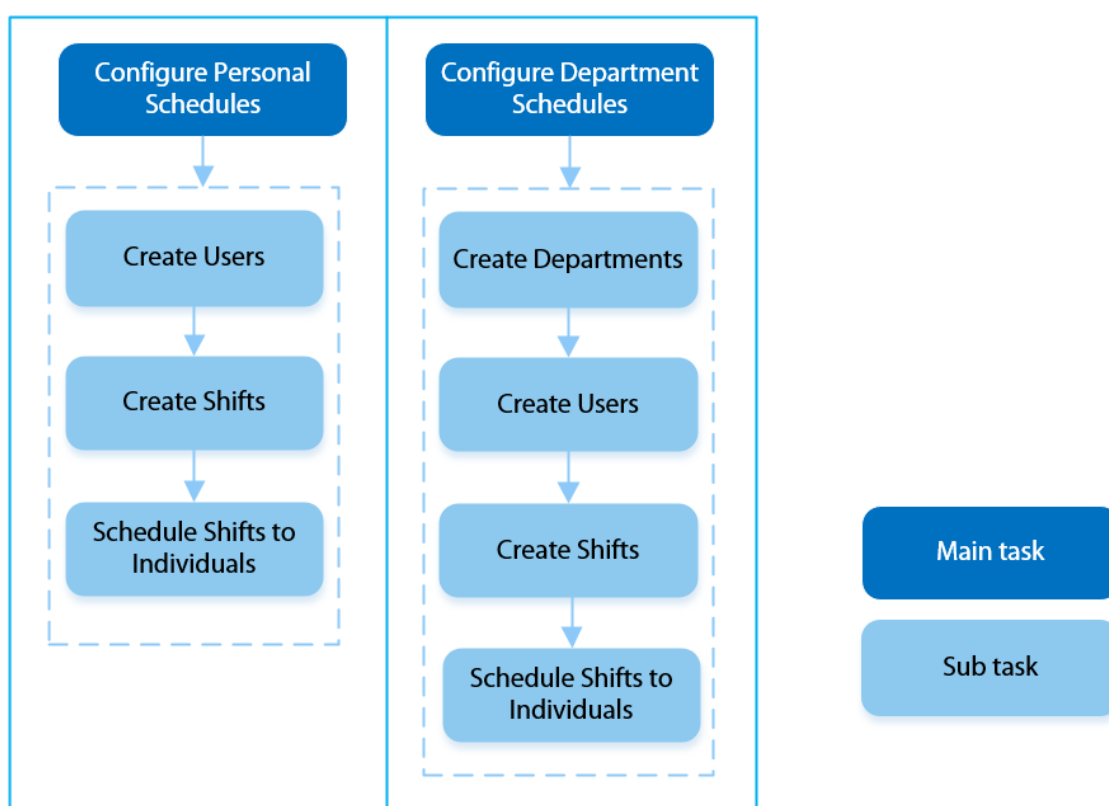
Background Information

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



When configuring the schedule, there should be no overlapping time periods on the same day and the previous or following day.

Figure 5-16 Configure 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. Tap **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.



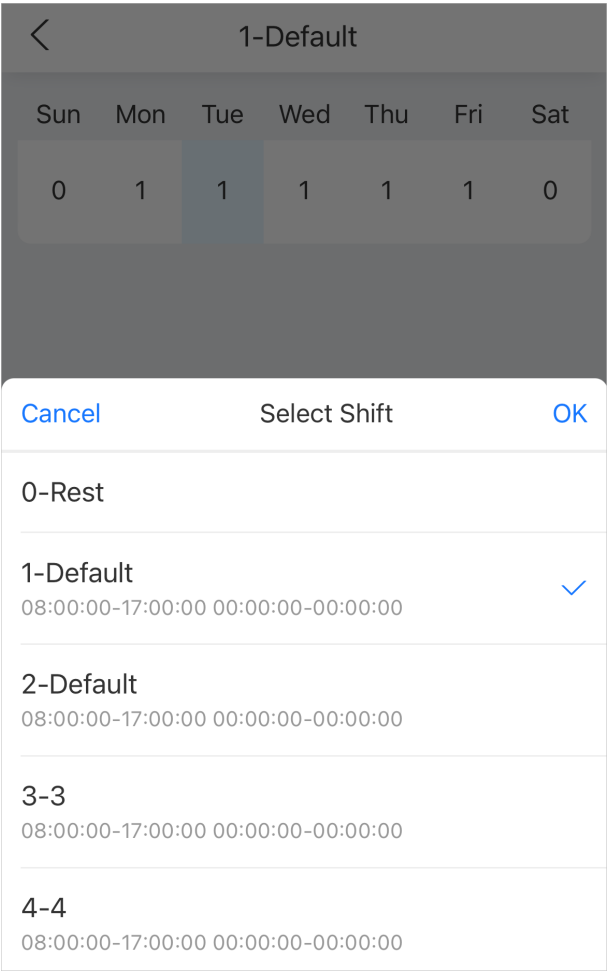
You can only set work schedules for the current month and the next month.

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

Step 4 Set work schedules for departments.

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

Figure 5-17 Department schedule



- 0 indicates rest.

- 1 to 24 indicates the number of the pre-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.

5.6.5 Configuring Attendance Modes

Procedure

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

Figure 5-18 Attendance configuration

The screenshot displays the 'Attendance Config' screen in a mobile application. At the top, there is a back arrow and the title 'Attendance Config'. Below this, a 'Local Attendance' toggle switch is shown in the 'on' position. Underneath, a section titled 'Mode Settings' shows 'Auto/Manual Mode' as the selected option. The main part of the screen contains a list of attendance-related settings, each with a right-pointing arrow to indicate further configuration options:

- Check In**: 06:00 AM~09:59 AM
- Break Out**: 10:00 AM~12:59 PM
- Break In**: 01:00 PM~03:59 PM
- Check Out**: 04:00 PM~08:59 PM
- Overtime Check In**: 12:00 AM~12:00 AM
- Overtime Check Out**: 12:00 AM~12:00 AM

Table 5-5 Description of attendance parameters

Parameter	Description
Auto/Manual Mode	The screen displays the attendance status automatically after you clock in or out, but you can also manually change your attendance status. • 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 ends. • Overtime check in: Clock in when your overtime period starts. • Overtime check out: Clock out when your overtime period ends.
Auto Mode	The screen displays your attendance status automatically after you clock in or out. • 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 ends. • Overtime check in: Clock in when your overtime period starts. • Overtime check out: Clock out when your overtime period ends.
Manual Mode	Manually select your attendance status when you clock in or out.
Fixed Mode	When you clock in or out, the screen will display the pre-defined attendance status all the time.

Step 4 Click **Apply**.

5.7 Configuring Access Control

5.7.1 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 Tap **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 tap **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 5-19 Unlock method

Unlock Method Combination Unlock

Combination Method Or >

Unlock Method Card, Fingerprint, Password, Bluetooth Card >

Apply

5.7.2 Configuring Access Control Parameters

Procedure

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

Figure 5-20 Access control parameters (1)

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

Figure 5-21 Access control parameters (2)

Unlock Settings

Unlock Method
Combination Unlock

Combination Method
Or >

Unlock Method
Card, Fingerprint, Password, Bluetooth Card

Bluetooth Mode

PIN Code Authentication

Door Unlocked Duration
3 s

Remote Verification

Apply

Table 5-6 Description of access control parameters

Parameter		Description
Basic Settings	Name	The name of the door.
	Door Status	Set the door status. - Normal: The door will be unlocked and locked according to your settings. - Always Open: The door remains unlocked all the time. - Always Closed: The door remains locked all the time.
	Verification Interval	If you verify your identity multiple times within a set period, only the earliest verification will be considered valid, and the door will not open after the second or later verifications. From the moment the door fails to open, you must wait for the configured verification time interval before attempting to verify your identity again.

Parameter		Description
	Card Swiping Interval	For first-time verification through card, you can normally unlock the door or perform attendance, and the records are generated. Within the configured period, if you swipe the card for verification again, you cannot unlock the door or perform attendance, and the records are not generated. Please verify the identification after the configured period.  The Card Swiping Interval takes priority over Verification Interval.
	Public Password	After the public password is enabled, configure the password. You can use the public password without entering the user ID to unlock the door. Only one public password is supported for one device.
Normally Open Period	General Plan/ Holiday Plan	When you select Normal , you can select a time template from the drop-down list. The door remains open or closed during the defined time. For details on how to configure general plans and holiday plans, see "4.7.4 Configuring Periods".
Normally Closed Period	General Plan/ Holiday Plan	 - When normally open period conflicts with normally closed period, normally open period takes priority over normally closed period. - When the general plan conflict with the holiday plan, the holiday plan takes priority over the general plan.
Unlock Settings	Unlock Method	Combination Unlock by default. For details on other unlock methods, see "4.7.1.2 Configuring Unlock Methods"
	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	Unlock methods might differ depending on the models of product.
	Bluebooth Mode	Select the Bluebooth mode according to your need.  This function displays only after you select Bluebooth Card in Unlock Method.

Parameter		Description
	PIN Code Authentication	When PIN code authentication is enabled, you can open the door with just the password.  You do not have to enter the user ID if this function is enabled. The remote verification is not supported.
	Door Unlocked 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.
	Remote Verification	Open the door remotely.

Step 4 Tap **Apply**.

5.7.3 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 (Optional) Select the door channel.

If you have selected **Lock Extension Module** as the **External Device** through **Communication Settings** > **RS-485 Settings** on the Access Controller, you can select the channel here.

Step 4 Configure alarm parameters, and then tap **Apply**.

Figure 5-22 Alarm settings

The screenshot displays a settings menu for alarms. The settings are as follows:

- Duress Alarm:** Enabled (blue toggle switch).
- Anti-passback:** Disabled (grey toggle switch).
- Door Detector:** Enabled (blue toggle switch).
- Door Detector Status:** Set to "NO" with a right-pointing chevron.
- Intrusion Alarm:** Disabled (grey toggle switch).
- Unlock Timeout Alarm:** Disabled (grey toggle switch).
- Unlock Timeout:** Set to "60 s".
- Excessive Attempts Alarm:** Enabled (blue toggle switch).

An "Apply" button is located at the bottom of the settings list.

Table 5-7 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
Anti-passback	Users need to verify their identities both for entry and exit; otherwise an alarm will be triggered. It helps prevents a card holder from passing an access card back to another person to gain entry. When anti-passback is enabled, the card holder must leave the secured area through an exit reader before system will grant another entry. ● If a person enters after authorization and exits without authorization, an alarm will be triggered when they attempt to enter again, and access is denied at the same time. ● If a person enters without authorization and exits after authorization, an alarm will be triggered when they attempt to enter again, and access is denied at the same time.  If the Device can only connect one lock, verifying on the Device means entry direction, and verifying on the external card reader means exit direction by default. You can modify the setting on the management platform.
Door Detector	With the door detector wired to your device, alarm can be triggered when doors are opened or closed abnormally. The door detector includes 2 types, including NC detector and NO detector. ● NC: The sensor is in a shorted position when the door or window is closed. ● NO: An open circuit is created when the window or door is actually closed.
Intrusion Alarm	If the door is opened abnormally, an intrusion alarm will be triggered and last for a defined time.  The door detector and intrusion need to be enabled at the same time.
Unlock Timeout Alarm	When the door remains unlocked for longer than the defined timeout duration, the door timeout alarm will be triggered and last for the defined time.
Unlock Timeout	 The door detector and door timed out function need to be enabled at the same time.
Excessive Attempts Alarm	If the wrong password or card is used 5 times in a row within 60 seconds, the alarm for excessive use of illegal card will be triggered and lasts for a defined time.

5.7.4 Configuring Alarm Linkages (Optional)

You can configure alarm linkages.

Procedure

- Step 1 Log in to the webpage.
- Step 2 Select **More** > **Access Control** > **Alarm Linkage Setting**.
- Step 3 Select the zone to configure alarm.

Figure 5-23 Alarm linkage

Alarm-in Port1

NameZone1

Alarm Input TypeNO >

Link Fire Safety Control☐

Alarm-out Port☐

Duration30 s

Alarm Output Channel1 >

Access Control Linkage☐

Linkage ModeWeak Execution >
When the heat alarm signal disappears, the door will automatically return to the normal authentication mode.

Local LockNO >

External LockNO >

- Step 4 Create a name for the alarm zone.
- Step 5 Enable **Link Fire Safety Control**, and select a type for the alarm input device.
 - NC: The alarm input is in a normally closed (NC) circuit state when the alarm has not been tripped. Opening a normally closed circuit sets off the alarm.
 - NO: The alarm input device is in a normally open (NO) circuit state when the alarm has not been tripped. Closing the circuit sets off the alarm.
- Step 6 If you want to link access control when the fire alarm is triggered, enable **Access Control Linkage**.



This function takes effect only after **Link Fire Safety Control** is enabled.

Step 7 Select a linkage mode.

- Strong Execution: When the fire alarm signal disappears, the door remains the current status. Please manually changes to its previous door status settings if you want to.
- Weak Execution: When the fire alarm signal disappears, the door automatically returns to its previous door status.

Step 8 Select the type for the local lock and external lock.

- NO: The door automatically opens when fire alarm is triggered.
- NC: The door automatically closes when fire alarm is triggered.

Step 9 Tap **OK**.

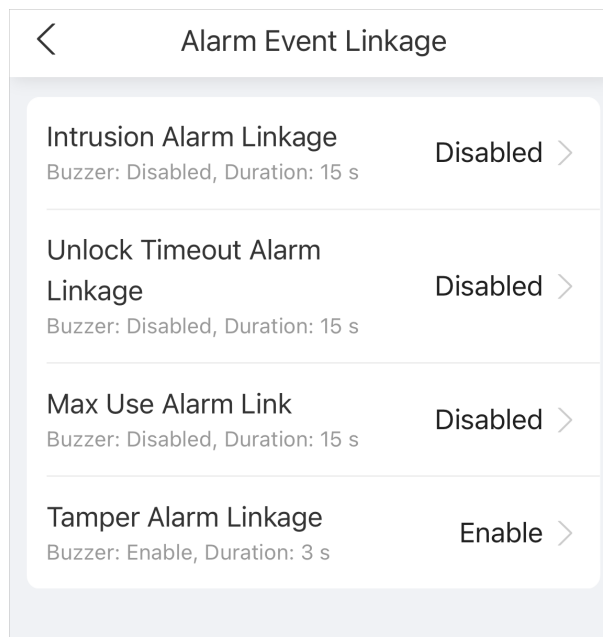
5.7.5 Configuring Alarm Event Linkage

Procedure

Step 1 Log in to the webpage.

Step 2 Select **More** > **Access Control** > **Alarm Event Linkage**.

Figure 5-24 Alarm event linkage



Step 3 Tap the linkage to configure the alarm linkage, and then tap **OK**.

Table 5-8 Alarm event linkage

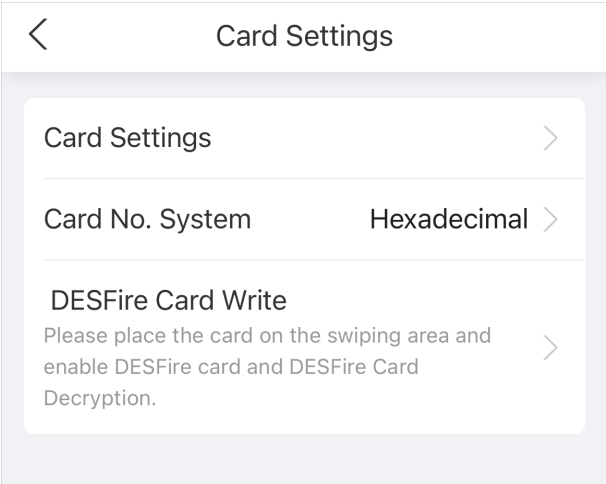
Parameter	Description
Intrusion Alarm Linkage	If the door is opened abnormally, an intrusion alarm will be triggered. ● Buzzer: The buzzer sounds when an intrusion alarm is triggered. You can configure the alarm duration. ● Link Alarm Output: The external alarm device generates alarms when the intrusion 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. The duration supports Custom Time and Until the Door Locks. ◇ Until the Door Locks: The alarm sound stops after the door is closed. ◇ Custom Time: You can configure the duration. ● Local Alarm Output: The external alarm device generates alarms when the unlock timeout alarm is triggered. The duration supports Custom Time and Until the Door Locks. ◇ Until the Door Locks: The alarm output stops after the door is closed. ◇ Custom Time: You can configure the duration.
Max Use Alarm Link	If the wrong password or card is used 5 times in a row within 60 seconds, the alarm for excessive use of illegal card will be triggered and lasts for a defined time. ● Buzzer: The buzzer sounds when the excessive use alarm is triggered. You can configure the alarm duration. ● Link Alarm Output: The external alarm device generates alarms when the unlock timeout alarm is triggered. You can configure the alarm duration.
Tamper Alarm Linkage	The tamper alarm is triggered when someone has tried to physically damage the Device. ● Buzzer: The buzzer sounds when the tamper alarm is triggered. You can configure the alarm duration. ● Link Alarm Output: The external alarm device generates alarms when the tamper alarm is triggered. You can configure the alarm duration.

5.7.6 Configuring Card Settings

Procedure

- Step 1 Log in to the webpage.
- Step 2 Select **More > Access Control > Card Settings**.

Figure 5-25 Card settings



Step 3 Tap **Card Settings** , configure the card parameters, and then tap **Apply**.

Figure 5-26 Card parameters

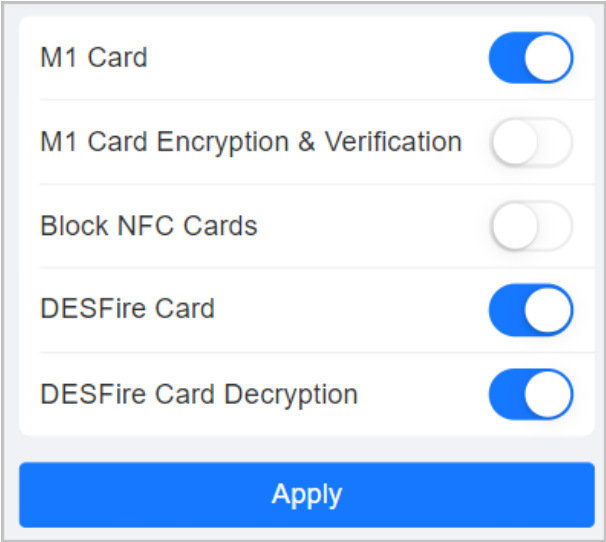


Table 5-9 Card parameters description

Parameter	Description
M1 Card	The M1 card can be read when this function is enabled.  This function is only available on select models.
M1 Card Encryption & Verification	Only the encrypted IC card can be read when this function is enabled.  Make sure M1 Card is enabled.

Parameter	Description
Block NFC Cards	Prevent unlocking through duplicated NFC card after this function is enabled.  • This function is only available on models that support IC cards. • Make sure M1 Card is enabled. • NFC function is only available on select models of phones.
Desfire Card	The Device can read the card number of Desfire card when this function is enabled.  • This function is only available on models that support IC cards. • Only supports hexadecimal format.
Desfire Card Decryption	Information in the Desfire card can be read when Enable Desfire Card and Desfire Card Decryption are enabled at the same time.  • This function is only available on models that support IC cards. • Make sure that Desfire card is enabled.

Step 4 Tap **Card No. System**, select the format, and then click **Apply**.

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

Step 5 Tap **DESFire Card Write**.

Place the card on the reader, enter the card number, and then click **Write** to write card number to the card.



- Desfire card function and Desfire card decryption function must be enabled.
- Only supports hexadecimal format.
- Supports up to 8 characters.

5.7.7 Configuring Screen Settings

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

Procedure

Step 1 Log in to the webpage.

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

Step 3 Configure the always-on screen.

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

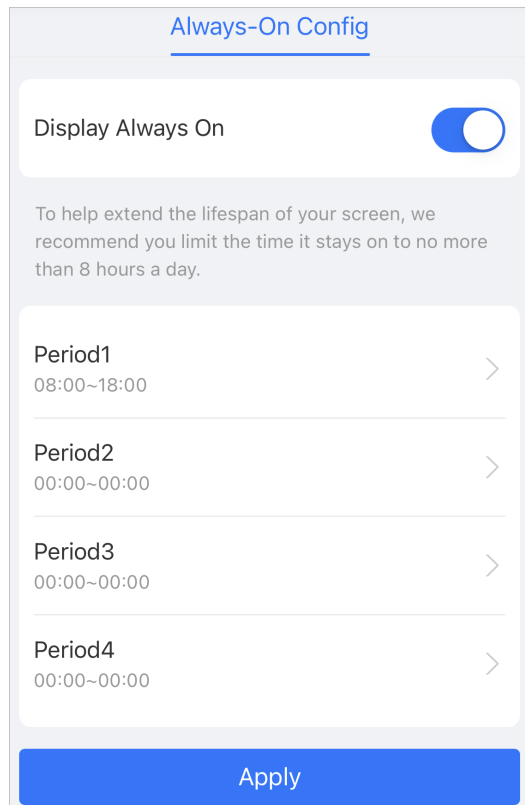
1. Tap **Always-On Config**.

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



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

Figure 5-27 Display always on



5.8 Communication Settings

5.8.1 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 tap **Apply**.

Figure 5-28 TCP/IP

< TCP/IP

NIC NIC 1 >

Mode Static >

MAC Address [blurred]

IP Version IPv4 >

* IP Address [blurred]

* Subnet Mask [blurred]

* Default Gateway [blurred]

* Preferred DNS [blurred]

* Alternate DNS [blurred]

MTU 1500

Transmission Mode Multicast >

Table 5-10 Description of TCP/IP

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

Parameter	Description
Preferred DNS	Set IP address of the preferred DNS server.
Alternate DNS	Set IP address of the alternate DNS server.
MTU	MTU (Maximum Transmission Unit) refers to the maximum size of data that can be transmitted in a single network packet in computer networks. It is 1500 by default.

5.8.2 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 Tap the Wi-Fi, and then enter the password.

The Wi-Fi is connected.

Related Operations

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

5.8.3 Configuring Wi-Fi AP

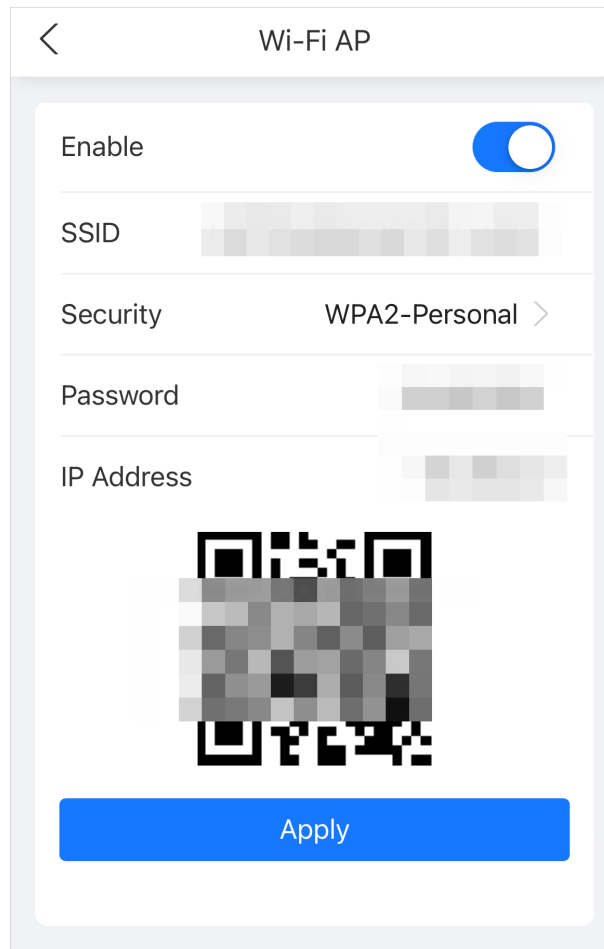


- The Wi-Fi function is available on select models.
- The Wi-Fi and Wi-Fi AP cannot be enabled at the same time.

Procedure

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

Figure 5-29 Wi-Fi AP



5.8.4 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 Tap **Apply**.

5.8.5 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 tap **Apply**.

Figure 5-30 Auto registration

The screenshot shows a mobile application interface for 'Auto Registration'. It includes a back arrow in the top left corner. The settings are as follows:

- Enable:** A toggle switch that is currently turned off.
- Status:** Displays a red dot followed by the text 'Offline'.
- Server Address:** A text input field that has been blurred for security.
- Port:** A text input field containing the value '7000'.
- Registration ID:** A text input field containing the value 'none'.

A blue button labeled 'Apply' is located at the bottom of the settings list.

Table 5-11 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.

5.8.6 Configuring Mode

Log in to the webpage, and select **Communication Settings** > **Mode Settings**.

Card Reader Mode

Select **Mode** as **Card Reader**. The device serves as a card reader externally connected to an access control controller. It does not perform authentication but directly transmits access control information (such as card, password, fingerprint) to the access control controller, which then authenticates and unlocks the door.

Figure 5-31 Card reader mode

Mode

Card Reader >

RS-485 Settings

Baud Rate

9600 >

Data Bit

8 >

Stop Bit

1 >

Parity Code

None >

Wiegand Settings

Wiegand Output Type

Wiegand 34 >

Pulse Width (μs)

200

The pulse width is a multiple of 10 and has a multiple relationship with the pulse interval.

Pulse Interval (μs)

1000

The pulse width is a multiple of 10 and has a multiple relationship with the pulse interval.

Apply

Access Controller Mode

Set **Mode** as **Access Controller**.

Figure 5-32 Access controller mode

External Device

Access Controller >

Access controller: This device acts as a card reader, and connects to an access controller, which manages the opening of doors.

Baud Rate

9600 >

Data Bit

8 >

Stop Bit

1 >

Parity Code

None >

Output Data Type

Card Number >

Wiegand Settings

Wiegand Settings

Wiegand Input >

Card No. Inversion

☒

Table 5-12 Description of RS-485

External Device	Description
Access Controller	Select Access Controller when the Device functions as a card reader, and sends data to other external access controllers to control access. Output Data type: • Card Number: Outputs data based on card number when users swipe card to unlock door; outputs data based on user's first card number when they use other unlock methods. • ID: Outputs data based on the user ID.  • When authentication is successful, the relevant information is transmitted to the access controller. In this case, the authentication result displayed is the authentication result of the access controller. • When authentication fails, the relevant information is not transmitted to the access controller, and the authentication result displayed remains as failure.
Card Reader	The device is externally connected to a card reader and transmits access control card information to an access controller or management platform.
Card Reader (OSDP)	The device is externally connected to an OSDP card reader and transmits access control card information to an access controller or management platform.
Door Security Module	The door exit button, lock and fire linkage is not effective after the security module is enabled. • Supports authentication through face, card, fingerprint, password, and other methods to control the door security module for unlocking. • Supports unlocking through an externally connected RS-485 card reader or push-to-open button linked to the door control security module.  Remote unlock of the externally connected door lock through the door security module is not supported.
Lock Extension Module	When the Access Controller is connected to external lock extension module, if you select Lock Extension Module, the local lock is unlocked after you verify the identification on the local device, and the extension lock is unlocked after you verify the identification on the external card reader. After you select Lock Extension Module, you can select channel 2 on the Access Control Parameters and Alarm page on the webpage of the Access Controller.

Table 5-13 Description of Wiegand

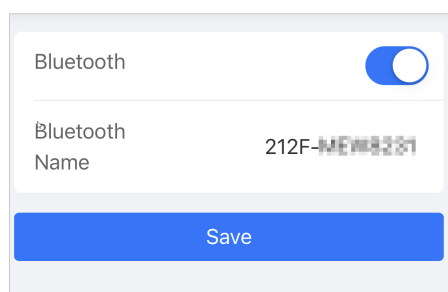
Parameter		Description
Wiegand Settings		- When connecting an external card reader device, select Wiegand Input. - When the Device functions as a card reader, and you need to connect it to another access controller, and select Wiegand Output Config.
Wiegand Input	Card No. Inversion	If the card number sequence obtained through Wiegand input does not match the actual card number sequence when interfacing with third-party devices, enable this function.
Wiegand Output	Wiegand Output Type	The bit length of card numbers or ID that the device can recognize and output. - Wiegand 26: Reads 3 bytes or 6 digits. - Wiegand 34: Reads 4 bytes or 8 digits. - Wiegand 66: Reads 8 bytes or 16 digits.
	Pulse Width	Configure the pulse width and interval for wiegand output.
	Pulse Interval	
	Output Data Type	Select a Wiegand format to read card numbers or ID numbers. - User ID: Outputs data based on user ID. - Card: Outputs data based on user's first card number.
	Wiegand Format	When Output Data Type is set as ID , you can select decimal or hexadecimal output formats.

5.8.7 Configuring Bluetooth

Procedure

- Step 1 Log in to the webpage.
- Step 2 Select **Communication** > **Bluetooth Settings**.
- Step 3 Enable or turn off **Bluetooth**.

Figure 5-33 Bluetooth



- Step 4 Tap **Save**.

Results

You can unlock the door through the Bluetooth through the DMSS app. For details, see "3.6.3 Bluetooth".

5.9 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 tap **Apply**.

Figure 5-34 Configure the audio parameters

Speaker Volume80
Only enter a multiple of 10.

Key Sound☐

Voice Broadcast Settings

TypeSuccessfully verified. >

Period1Disabled >

Period2Disabled >

Period3Disabled >

Period4Disabled >

Period5Disabled >

Period6Disabled >

DND Mode

DND Mode☐

Apply

Table 5-14 Parameters description

Parameters	Description
Speaker	Set the volume of the speaker.
Screen Tap Sound	When this function is enabled, touch screen devices will produce tap sound and non-touch screen devices will produce mouse tap sound.
Audio Collection	If this function is enabled, the sound from the device mic will be captured during live view and recording.

Parameters	Description
DND Mode	No voice prompts during the set time when you verify your identity on the Device. You can set up to 4 periods.

5.10 Viewing Logs

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

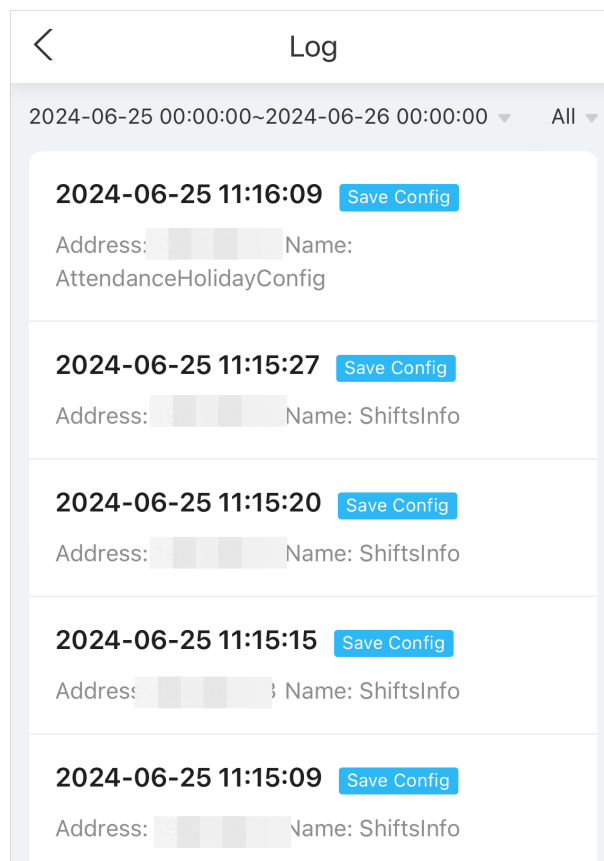
5.10.1 System Logs

View and search for system logs.

Procedure

- Step 1 Log in to the webpage.
- Step 2 Select **More > Log > Log**.
- Step 3 Select the time and the record type.

Figure 5-35 Logs



5.10.2 Unlock Records

Search for unlock records.

Procedure

- Step 1 Log in to the webpage.

Step 2 Select **More** > **Log** > **Unlock Records**.

Step 3 Select the time and the record type.

Step 4 Tap a record to view the details.

5.10.3 Call History

Search for the call history.

Procedure

Step 1 Log in to the webpage.

Step 2 Select **More** > **Log** > **Call History**.

5.10.4 Alarm Logs

View alarm logs.

Procedure

Step 1 Log in to the webpage.

Step 2 Select **More** > **Log** > **Alarm Log**.

Step 3 Select the time and the log type.

6 Smart PSS Lite Configuration

This section introduces how to manage and configure the device through Smart PSS Lite. For details, see the user's manual of Smart PSS Lite.

6.1 Installation

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

6.2 Initialization and Logging In

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

Procedure

- Step 1 Double-click SmartPSSLite.exe.
- Step 2 Select the language from the drop-down list, select **I have read and agree the software agreement**, and then click **Next**.
- Step 3 Click **Browse** to select installation path, and then click **Install**.
- Step 4 Click **Finish** to complete the installation.

Select **Run SmartPSSLite** to start SmartPSS Lite.
- Step 5 Select the application scenes you want to add, and then click **OK**.
- Step 6 Click **I have read and agree to the terms of software license agreement** to agree **SOFTWARE LICENSE AGREEMENT**.
- Step 7 Click **I have read and agree to the terms of software privacy policy** to agree **Product Privacy Policy**.
- Step 8 Set password on the **Initialize** page, and then click **Next**.

Table 6-1 Parameters of setting password

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

- Step 9 Set security questions, and then click **Complete**.
- Step 10 Double-click SmartPSSLite.exe.
- Step 11 Enter user name and password, and then click **Login**.

If multiple networks are available on your computer, you can select one from them.

6.3 Adding Devices

There are 3 available methods of adding devices.

- Automatically search
- Manually adding
- Import in batches

6.3.1 Adding Device by Searching

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



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

Procedure

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

Step 2 Select a search method.

- Click **Auto Search** to automatically search for devices that are on the same network segment to your computer.
- Enter the start IP and the end IP near the **Device Network Segment**, click **Search**, and then the system will automatically search for devices in this IP range.

Step 3 Select devices, and then click **Add**.

Step 4 Enter the login user name and password, and then click **OK**.

The devices will be added to the platform.

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

Related Operations

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



Enter the start IP, and the system will automatically assign IP to devices through increasing by 1 in the IP address based on the start IP. For example, if the start IP is 10.XX.XXX.52, and the following IP of devices will be 10.XX.XXX.53, 10.XX.XXX.54, and more.

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



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

6.3.2 Adding Device One by One

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

Procedure

- Step 1 On the home page, click **Devices**.
- Step 2 Click **Add**, and then enter the device information.
- Step 3 Click **Add**.
You can also click **Add and Continue** to add more devices.

Appendix 1 Important Points of Fingerprint Registration Instructions

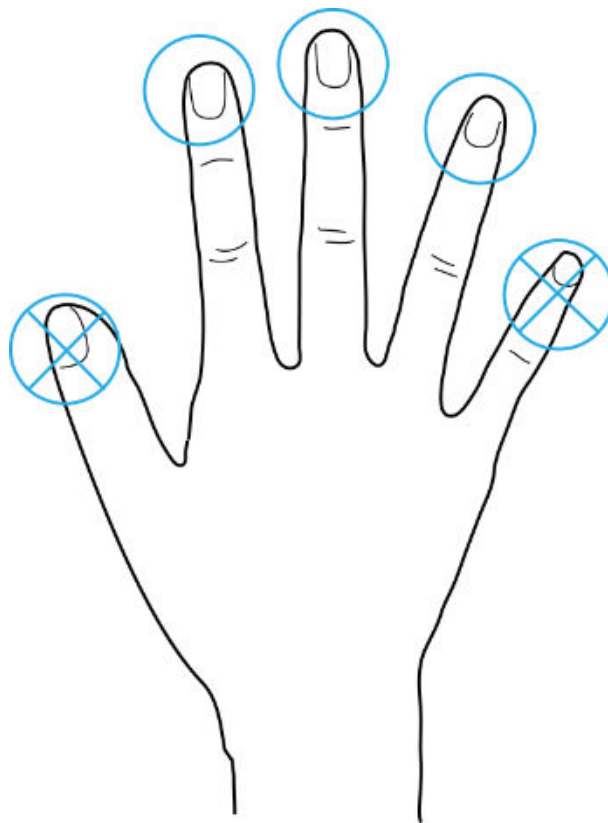
When you register the fingerprint, pay attention to the following points:

- 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

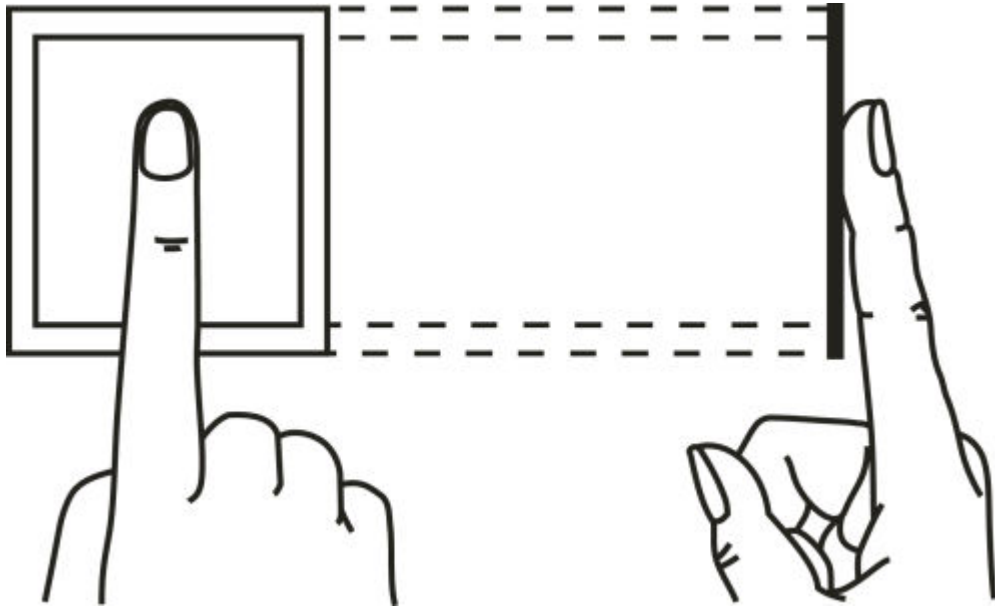
Forefingers, middle fingers, and ring fingers are recommended. Thumbs and little fingers cannot be put at the recording center easily.

Appendix Figure 1-1 Recommended fingers

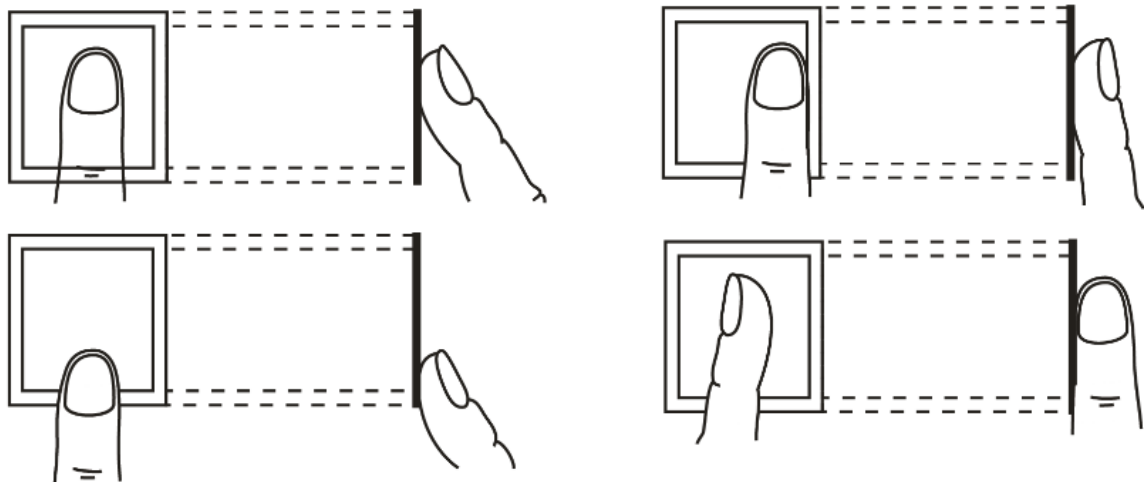


How to Press Your Fingerprint on the Scanner

Appendix Figure 1-2 Correct placement



Appendix Figure 1-3 Wrong placement



Appendix 2 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 Allowlist**

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

2. **MAC address binding**

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

3. **Build a secure network environment**

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

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

Security Auditing

1. **Check online users**

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

2. **Check device log**

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

3. **Configure network log**

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

Software Security

1. **Update firmware in time**

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

2. **Update client software in time**

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

Physical Protection

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

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