Face Recognition Access Controller

User's Manual

V1.0.1

Foreword

General

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

Safety Instructions

The following signal words might appear in the manual.

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

Revision History

Version	Revision Content	Release Time
V1.0.1	Revised important safeguards and warnings.	August 2024
V1.0.0	First release.	July 2024

Privacy Protection Notice

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

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.

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

Important Safeguards and Warnings

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

Transportation Requirement

⚠

Transport, use and store the Device under allowed humidity and temperature conditions.

Storage Requirement

⚠

Store the Device under allowed humidity and temperature conditions.

Installation Requirements

⚠ WARNING

- Do not connect the power adapter to the Device while the adapter is powered on.
- Strictly comply with the local electric safety code and standards. Make sure the ambient voltage is stable and meets the power supply requirements of the Device.
- Do not connect the Device to two or more kinds of power supplies, to avoid damage to the Device.
- Improper use of the battery might result in a fire or explosion.
- Please follow the electrical requirements to power the Device.
  - Following are the requirements for selecting a power adapter.
    - The power supply must conform to the requirements of IEC 60950-1 and IEC 62368-1 standards.
    - The voltage must meet the SELV (Safety Extra Low Voltage) requirements and not exceed ES-1 standards.
    - When the power of the device does not exceed 100 W, the power supply must meet LPS requirements and be no higher than PS2.
  - We recommend using the power adapter provided with the Device.
  - When selecting the power adapter, the power supply requirements (such as rated voltage) are subject to the Device label.

⚠

- Personnel working at heights must take all necessary measures to ensure personal safety including wearing a helmet and safety belts.
- Do not place the Device in a place exposed to sunlight or near heat sources.
- Keep the Device away from dampness, dust, and soot.
- Install the Device on a stable surface to prevent it from falling.
- Install the Device in a well-ventilated place, and do not block its ventilation.

- Use an adapter or cabinet power supply provided by the manufacturer.
- Use the power cords that are recommended for the region and conform to the rated power specifications.
- The Device is a class I electrical appliance. Make sure that the power supply of the Device is connected to a power socket with protective earthing.
- The Device must be installed at a height of 2 meters or below.

Operation Requirements

⚠

- Check whether the power supply is correct before use.
- Ground the device to protective ground before you power it on.
- Do not unplug the power cord on the side of the Device while the adapter is powered on.
- Operate the Device within the rated range of power input and output.
- Use the Device under allowed humidity and temperature conditions.
- Do not drop or splash liquid onto the Device, and make sure that there is no object filled with liquid on the Device to prevent liquid from flowing into it.
- Do not disassemble the Device without professional instruction.
- This product is professional equipment.
- The Device is not suitable for use in locations where children are likely to be present.

Table of Contents

1 Overview

The Device is an access control panel that supports unlocking through faces, passwords, fingerprints, cards, and their combinations. Based on the deep-learning algorithm, it features faster recognition and higher accuracy. It can work with management platform which meets various needs of customers.

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

- Configurations might differ depending on the models of the product.
- Some models support connecting extension modules like fingerprint module and more. The type of extension modules that the Device supports might differ.

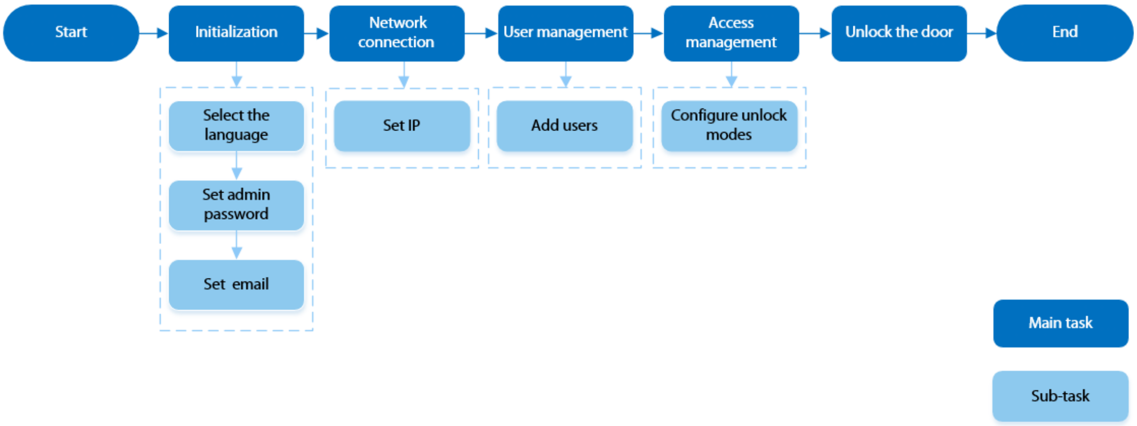
2 Local Operations

- Configurations might differ depending on the actual product.
- External expansion modules are only available on select models.

2.1 Preparation

2.1.1 Basic Configuration Procedure

Figure 2-1 Basic configuration procedure



2.1.2 Button Description

The Device has non-touch screen. Operate the Device through the buttons. When the device screen is off, press any button except the door bell button to light up the screen.

Figure 2-2 Buttons

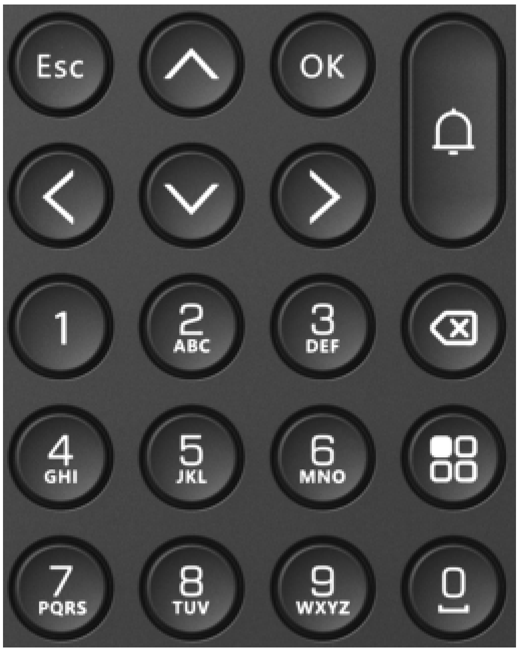


Table 2-1 Button description

Button	Description
ESC	Return to the previous menu.
OK	Confirm button
∧/∨	The selected option can be shifted in both upward and downward directions on the screen using the buttons.
</>	The selected option can be shifted left or right on the screen using the buttons. You can also turn to the previous page or the next page using the buttons.
🔔	Door bell: Press the button, and the connected external door bell device rings.
0-9	● 0: Indicates the number 0 and space. ● 1: Indicates the number 1. ● 2-9: The buttons are shared by number and letter.
⌫	Delete the content in the input box.
⊞	● Change the input method in the input box. ● On the home screen, press the button to view the background login screen. ● On the configuration screen, press the button to go back to the home screen.

2.1.3 Input Method Introduction

Change the input method

Press ⊞ on the input box to change the input method.

Input the letter

This part uses entering M as the example.

1. Press the 6 button on the input box.
2. Press the 4 button.

Input the number

Change to the number input method, and then press the corresponding number button.

Input the character

Change to the character input method, and then press the corresponding number button.

Press ⌃ or ⌄ to change to previous or next page of characters.

2.2 Initialization

Background Information

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

Procedure

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

Step 2 Press ⌄ to select **Enter Password**, and then press OK.

Step 3 Configure the password, and then press OK.

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

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

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

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

Step 5 Repeat Step 3 , enter the same password, and then press OK.

Step 6 Enter the email address, and then select the time zone.

Step 7 Press ⌄ to select ✓, and then press OK.

2.3 Home Screen

Figure 2-3 Home screen

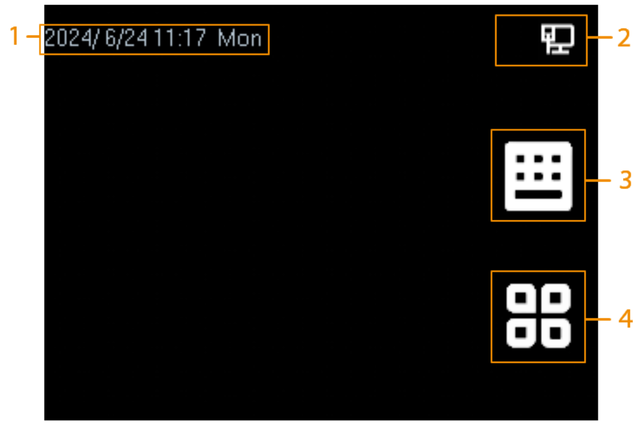


Table 2-2 Home screen description

No.	Description
1	Displays the current date, time and day.
2	Displays the network connection status. 📖 The Wi-Fi and Wi-Fi AP function are available on select models.
3	Unlock by password: Enter the user password, temporary password or admin password to open the door.
4	Main menu: Select the icon using the button, and then select the verification method to view the main menu.

2.4 Unlocking Methods

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

2.4.1 Unlocking by Cards

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

📖

This function is only available on select models.

2.4.2 Unlocking by Fingerprint

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

📖

This function is only available on select models.

2.4.3 Unlocking by Face

Verify the identity of an individual by detecting the face. Make sure that the face is centered on the face detection frame.

📖

Do not wear the mask during the verification.

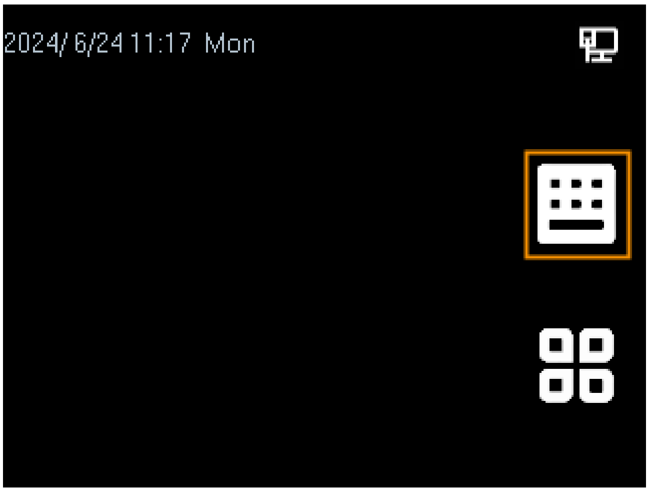
2.4.4 Unlocking by User Password

Enter the user ID and password to unlock the door.

Procedure

Step 1 Press ⌃ or ⌄ to select ⌨, and then press OK.

Figure 2-4 Home screen



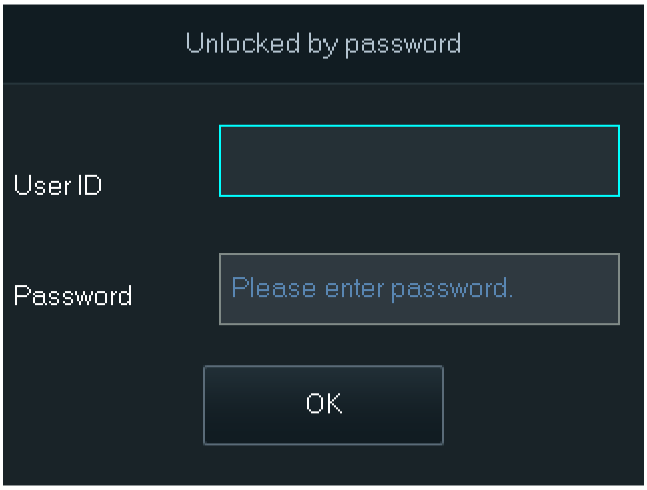
2024/ 6/24 11:17 Mon

Step 2 Select **Unlocked by password**, and then press OK.

Step 3 Enter the registered or delivered user ID and password.

After the successful verification, you can unlock the door.

Figure 2-5 Unlock by password



Unlocked by password

User ID

Password

Please enter password.

OK

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

2.4.5 Unlocking by Admin Password

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

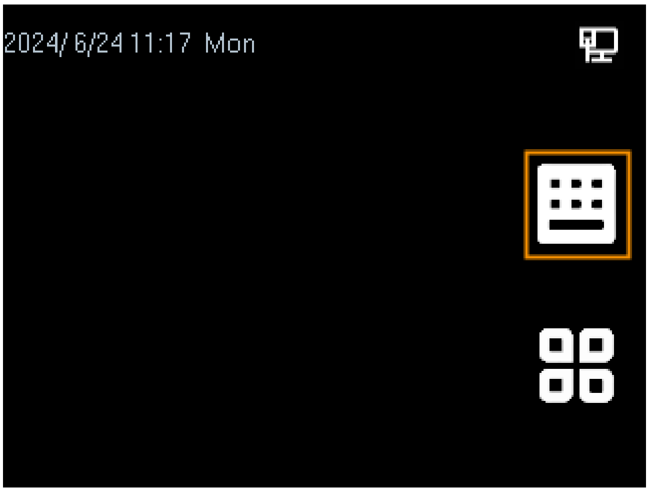
Prerequisites

The admin password was configured. For details, see "2.6.3 Configuring the Admin Unlock Password".

Procedure

Step 1 Press ⌃ or ⌄ to select ⌨, and then press OK.

Figure 2-6 Home screen



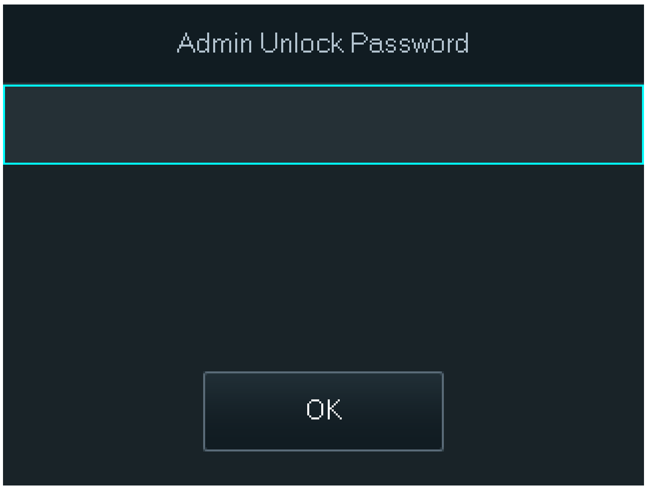
2024/ 6/24 11:17 Mon

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

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

After the successful verification, you can unlock the door.

Figure 2-7 Unlock by admin password



2.4.6 Unlocking by Temporary Password

Unlock the door by the temporary password.

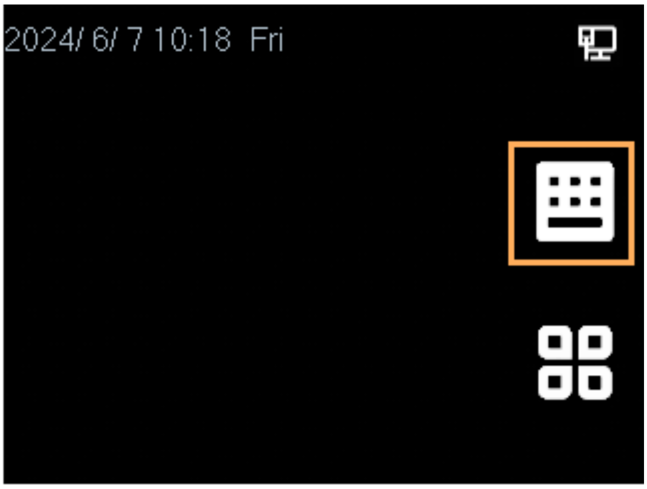
Procedure

Step 1 Add the Device to DMSS.

DMSS will generate a temporary password, which allows you unlock the door before it expires.

Step 2 Press ⌃ or ⌄ to select ⌨, and then press OK.

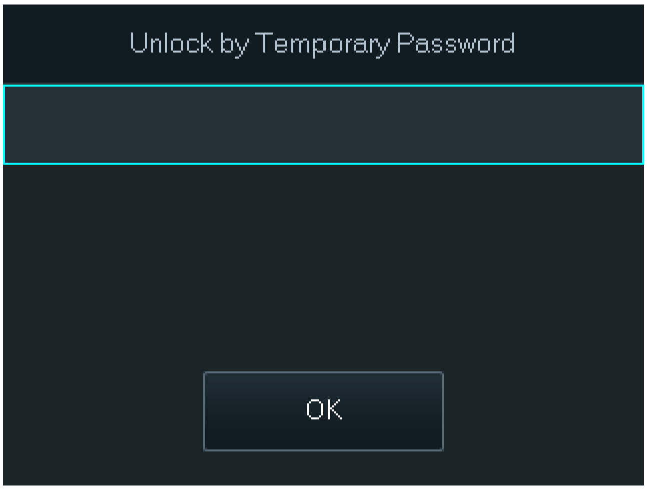
Figure 2-8 Home screen



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

Step 4 Enter the temporary password, select **OK**, and then press OK.

Figure 2-9 Unlock by temporary password



Unlock by Temporary Password

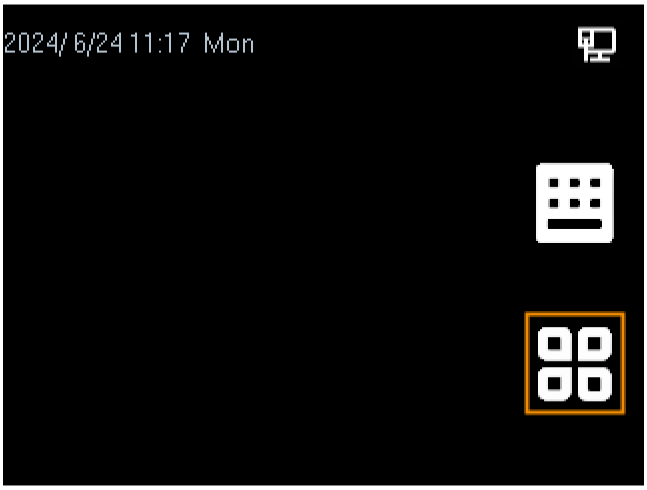
2.5 Logging in

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

Procedure

Step 1 Press ∧ or ∨ to select ⊞, and then press OK.

Figure 2-10 Home screen



2024/ 6/24 11:17 Mon

Step 2 Press ∧, ∨, < or > to select **admin**, and then press OK.

Step 3 Press OK, and then enter the password that is configured during the initialization.

Step 4 Press ∧ or ∨ to select **OK**, and then press OK.

2.6 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.

2.6.1 Adding Users

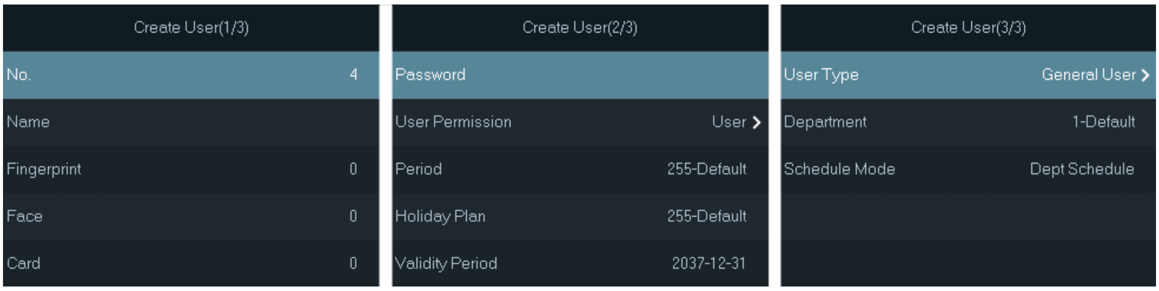
Add the new user, configure the name, face, fingerprint, permission, validity period, and other information.

Procedure

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

Step 2 Configure the parameters on the interface.

Figure 2-11 Add the user



Create User(1/3)

No. 4

Name

Fingerprint 0

Face 0

Card 0

Create User(2/3)

Password

User Permission User >

Period 255-Default

Holiday Plan 255-Default

Validity Period 2037-12-31

Create User(3/3)

User Type General User >

Department 1-Default

Schedule Mode Dept Schedule

Table 2-3 Parameters description

Parameter	Description
No.	The No. is like employee ID, which can be numbers, letters, and their combinations, and the maximum length of the No. is 32 characters.
Name	The name can have up to 30 characters (including numbers, symbols, and letters).
Fingerprint	Register fingerprints. A user can register up to 3 fingerprints, and you can set a fingerprint to the duress fingerprint. An alarm will be triggered when the duress fingerprint is used to unlock the door. ● 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 set one duress fingerprint. ● Fingerprint function is available if the Access Controller supports connecting a fingerprint extension module.
Face	Position your face inside the frame, and a face image will be captured automatically. You can register again if you are not satisfied with the outcome.

Parameter	Description
Card	A user can register up to 5 cards at most. Enter your card number or swipe your card, and then the card information will be read by the Access Controller. You can enable the **Duress Card** function. An alarm will be triggered if a duress card is used to unlock the door. 📖 One user can only set one duress card.
Password	Enter the user password. The maximum length of the password is 8 digits. The duress password is the unlock password + 1. For example, if the user password is 12345, the duress password will be 12346. A duress alarm will be triggered when a duress password is used to unlock the door.
User Permission	● **User** : Users only have door access or time attendance permissions. ● **Admin** : Administrators can configure the Access Controller besides door access and attendance permissions.
Period	People can unlock the door or take attendance during the defined period.
Holiday Plan	People can unlock the door or take attendance during the defined holiday.
Validity Period	Set a date on which the door access and attendance permissions of the person will be expired.
User Type	● **General User** : General users can unlock the door. ● **Blocklist User** : When users on the blocklist unlock the door, a blocklist alarm will be triggered. ● **Guest User** : Guests can unlock the door within a defined period or for a designated number of times. After the defined period expires or the unlocking times run out, they cannot unlock the door. ● **Patrol User** : Patrol users can take attendance on the Access Controller, but they do not have door permissions. ● **VIP User** : When VIP users unlock the door, service personnel will receive a notification. ● **Other User** : When they unlock the door, the door will stay unlocked for 5 more seconds. 📖 The delay time is not available for remote verification methods. ● **Custom User 1/Custom User 2** : Same with general users.

Parameter	Description
Department	Select departments, which is useful when configuring department schedules. This function is only available on select models.
Schedule Mode	● Department Schedule: Apply department schedules to the user. ● Personal Schedule: Apply personal schedules 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** becomes invalid.

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

2.6.2 Viewing User Information

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

Procedure

Step 1 On the **Main Menu**, select **Users** .

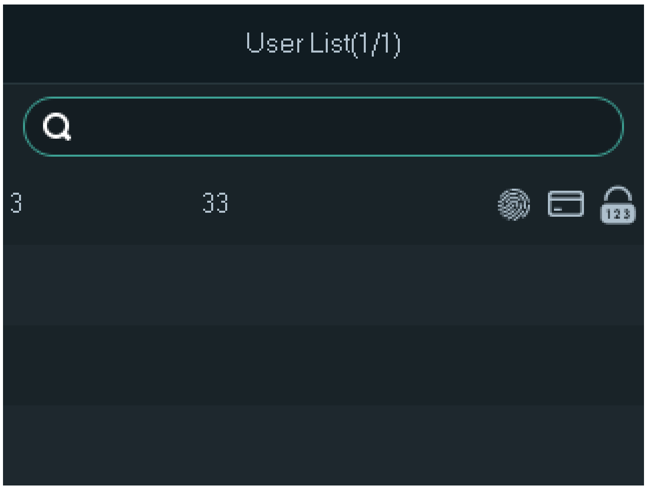
Step 2 Select **User List** , or select **Admin List**.

- The user list displays all the user information in the Device.
- The admin list displays all the administrator information in the device.

Step 3 View all added users or admin accounts.

- 🔒: Unlock through password.
- 💳: Unlock through swiping card.
- 👤: Unlock through face recognition.
- ▨: Unlock through fingerprint.

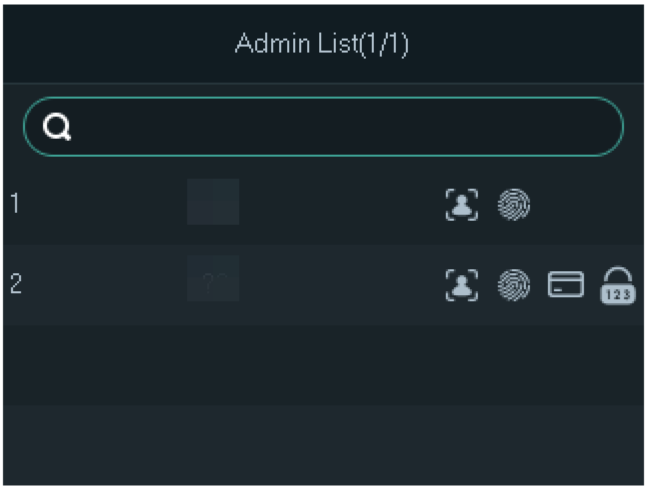
Figure 2-12 User list



User List(1/1)

3 33

Figure 2-13 Admin list



Admin List(1/1)

1 [redacted]

2 [redacted]

Related Operations

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

2.6.3 Configuring the Admin Unlock Password

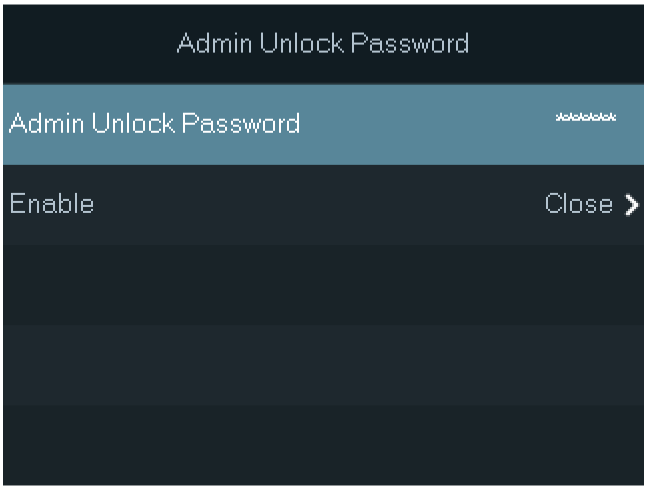
You can unlock the door by only entering the admin password. This password is not limited by user types. Only one admin unlock password is allowed for one device.

Procedure

Step 1 On the **Main Menu** screen, select **Users** > **Admin Unlock Password**.

Step 2 Enter the password, and then press OK.

Figure 2-14 Admin unlock password



Admin Unlock Password

Admin Unlock Password ******

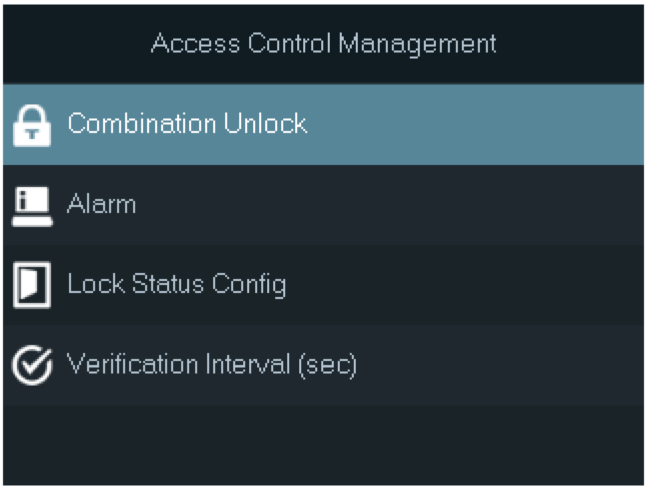
Enable Close ›

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

2.7 Access Control Management

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

Figure 2-15 Access control management



2.7.1 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

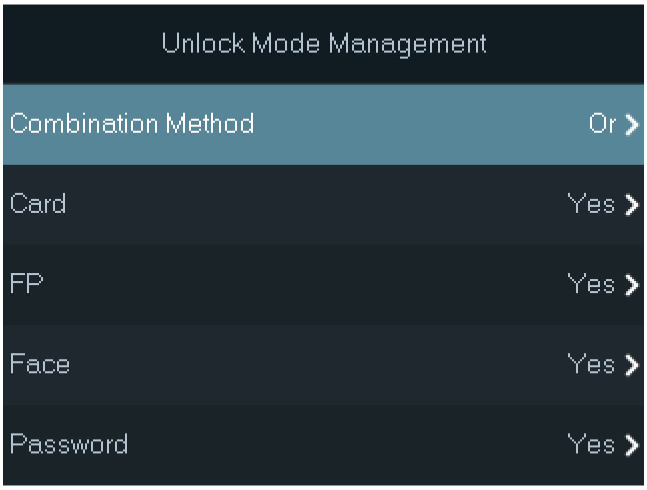
Step 1 On the **Main Menu**, select **Access Control Management** > **Combination Unlock**.

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

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

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

Figure 2-16 Combination unlock



Unlock Mode Management

Combination Method	Or
Card	Yes
FP	Yes
Face	Yes
Password	Yes

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

2.7.2 Configuring Alarms

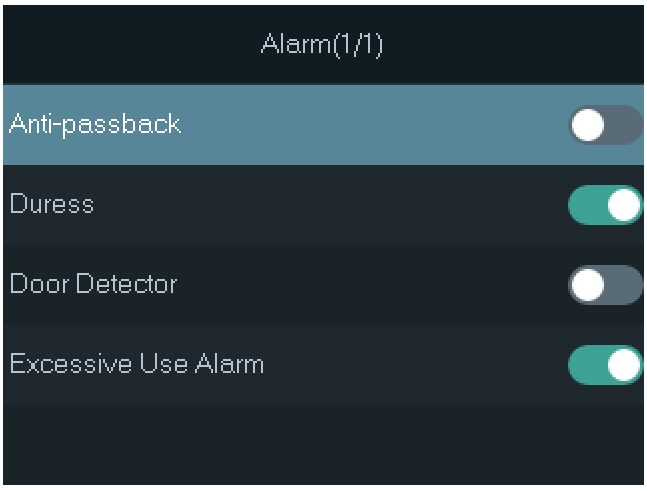
An alarm will be triggered when the entrance or exit is abnormally accessed.

Procedure

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

Step 2 Configure the alarm parameters.

Figure 2-17 Alarm settings



Alarm(1/1)

Anti-passback

Duress

Door Detector

Excessive Use Alarm

Table 2-4 Description of alarm parameters

Parameter	Description
Anti-passback	Users need to verify their identities both for entry and exit; otherwise an alarm will be triggered. This helps prevent card holders from being able to give their card to other people to allow them access. When anti-passback is enabled, the card holder must leave the secure area through an exit reader before the system will grant them access again. People need to swipe their card at the "in" reader to enter a secure area and swipe it at the "out" reader to get out of it. ● If a person enters after being verified, but exits without being verified, an alarm will be triggered if they attempt to enter again, and they will be denied access. ● If a person enters without being verified, an alarm will be triggered if they attempt to exit, and they will be denied access. If the Device can only connect to one lock, verification through the Device means a person entered in the "in" direction, and verification through the external card reader means they exited in the "out" direction. You can modify the configuration on the platform.
Duress	An alarm will be triggered when a duress card, duress password or duress fingerprint is used to unlock the door.
Door Detector	With the door detector wired to your device, alarms can be triggered when doors are opened or closed abnormally. There are 2 types of door detectors: NC detector and NO detector. ● **Normally Closed** : The sensor is in a shorted position when the door or window is closed. ● **Normally Open** : An open circuit is created when the window or door is actually closed.
Door Detector Type	

Parameter	Description
Excessive Use Alarm	If the wrong password or card is used 5 times in a row within 60 seconds, the alarm for excessive use of illegal card will be triggered and lasts for a defined time.

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

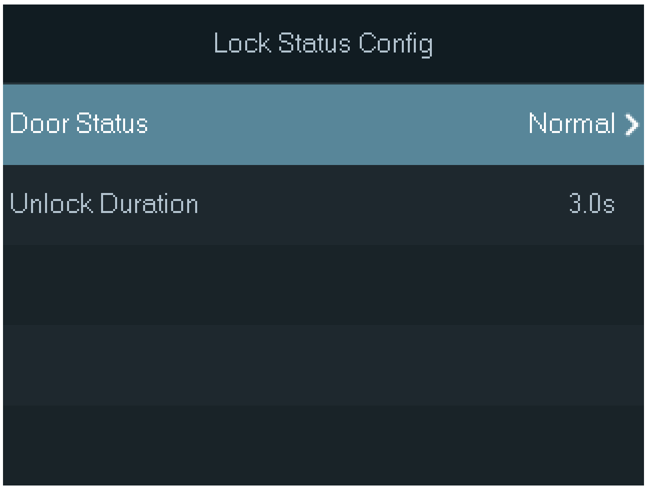
2.7.3 Configuring the Door Status

Procedure

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

Step 2 Configure the parameters.

Figure 2-18 Lock status



Lock Status Config

Door Status Normal

Unlock Duration 3.0s

Table 2-5 Parameters description

Parameter	Description
Door Status	● **Normally Open** : The door remains unlocked all the time. ● **Normally Closed** : The door remains locked all the time. ● **Normal** : If **Normal** is selected, the door will be locked and unlocked according to your settings.
Unlock Duration	After a person is granted access, the door will remain unlocked for a defined time for them to pass through.

2.7.4 Configuring the Verification Time Interval

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

Procedure

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

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

2.8 Communication Settings

Configure the network, serial port and Wiegand port to connect the Device to the network.

The serial port and the Wiegand port might differ depending on the models of Device.

2.8.1 Configuring Network

2.8.1.1 Configuring the IP Address

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

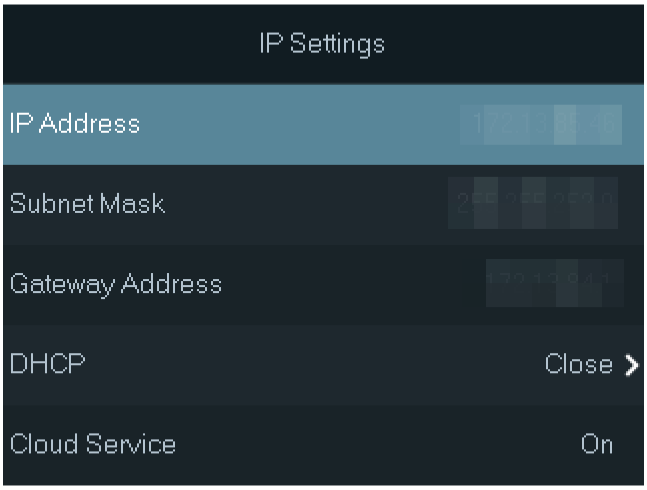
Procedure

Step 1 On the **Main Menu**, select **Communication Settings** > **IP Settings**.

Step 2 Set the IP Address.

The displayed parameters may differ according to different device models.

Figure 2-19 IP settings



IP Settings

IP Address [redacted]

Subnet Mask [redacted]

Gateway Address [redacted]

DHCP Close >

Cloud Service On

Table 2-6 IP configuration parameters

Parameter	Description
IP Address/Subnet Mask/Gateway Address	Enter the IP address, subnet mask, and gateway IP address. They must be on the same network segment.
DHCP	It stands for Dynamic Host Configuration Protocol. When DHCP is turned on, the Device will automatically be assigned the IP address, subnet mask, and gateway.

Parameter	Description
Cloud Service	If this function is turned on, you can manage devices without applying for DDNS, setting port mapping or deploying transit servers.

2.8.1.2 Configuring Wi-Fi

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

Background Information

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

Procedure

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

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

Step 3 Press OK to turn on Wi-Fi.

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

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

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

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

Results

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

Related Operations

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

2.8.1.3 Configuring Wi-Fi AP

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

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

Procedure

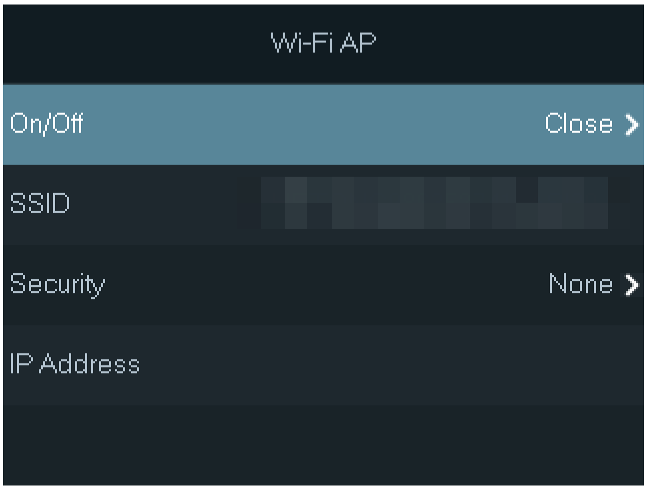
Step 1 On the **Main Menu**, select **Communication Settings** > **Wi-Fi AP**.

Step 2 Turn on Wi-Fi AP.

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

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

Figure 2-20 Connect to Wi-Fi AP



Wi-Fi AP

On/Off Close

SSID [redacted]

Security None

IP Address

Results

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

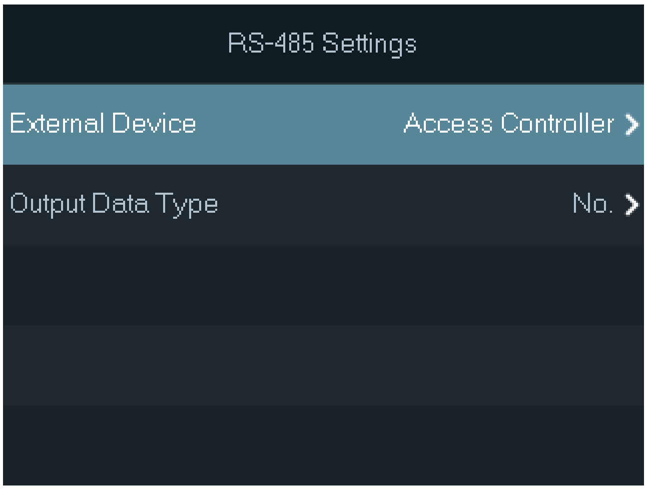
2.8.2 Configuring RS-485

Procedure

Step 1 On the **Main Menu**, select **Communication Settings** > **RS-485 Settings**.

Step 2 Select the external device.

Figure 2-21 External device type



RS-485 Settings

External Device Access Controller

Output Data Type No.

Table 2-7 Parameter description

External device	Description
Access Controller	The Device functions as a card reader and sends data to other external access controllers to control access. Output Data type: ● Select **Card Number**. Outputs data based on the card number when users swipe their cards to unlock doors; outputs data based on user's first card number when users use other unlock methods. ● Select **No.**. Outputs data based on the user ID.
Card Reader	The Device connects to an external card reader. The card information is sent to the access controller or the management platform.
Reader (OSDP)	The Device is connected to a card reader based on the OSDP protocol. The card information is sent to the access controller or the management platform.
Door Control Security Module	After the security module is enabled, the door exit button, lock control and fire linkage of the Device become invalid, but the door exit button and lock control that connects to the security module become effective. You can unlock the door (only swiping the card is supported) through the external card reader that is connected to the door control security module.

2.8.3 Configuring Wiegand

The Device allows for both Wiegand input and output mode.

Select the Wiegand type according to the connected device.

- Select **Wiegand Input** when you connect an external card reader to the Device.
- Select **Wiegand Output** when the Device functions as a card reader, and you need to connect it to a controller or another access terminal.

🕮

This function is only available on select models.

Procedure

Step 1 On the **Main Menu**, select **Communication Settings** > **Wiegand Settings**.

Step 2 Select a Wiegand type, and then configure the parameters.

Figure 2-22 Wiegand settings

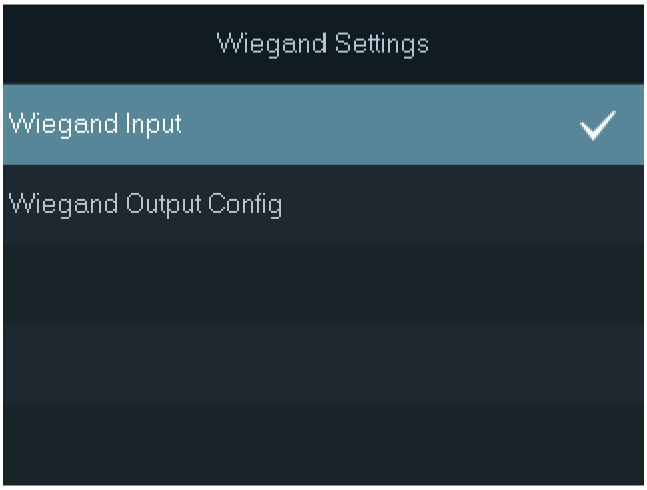
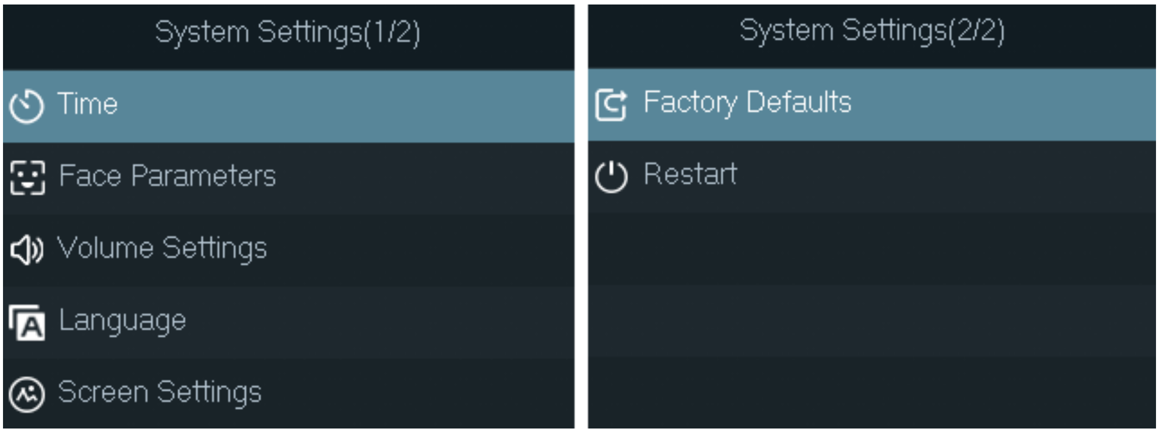


Table 2-8 Description of Wiegand settings

Parameter		Description
Wiegand Input	Card No. Inversion	When the Device connects to a third-party device through the Wiegand input port, and the card number read by the Device is in the reverse order from the actual card number. In this case, you can turn on **Card No. Inversion** function.
Wiegand Output Config	Wiegand Output Type	Select a Wiegand format to read card numbers or ID numbers. ● **Wiegand26** : Reads 3 bytes or 6 digits. ● **Wiegand34** : Reads 4 bytes or 8 digits. ● **Wiegand66** : Reads 8 bytes or 16 digits.
	Pulse Width	Enter the pulse width and pulse interval of Wiegand output.
	Pulse Interval	
	Output Data Type	Select the type of output data. ● **No.** : The system outputs data based on the user ID. The data format is hexadecimal or decimal. ● **Card Number** : The system outputs data based on user's first card number.
	Output Format	When the **Output Data Type** is configured as **No.**, you can select **Hexadecimal** or **Decimal** as the output format.

2.9 System Settings

Figure 2-23 System settings



2.9.1 Configuring Time

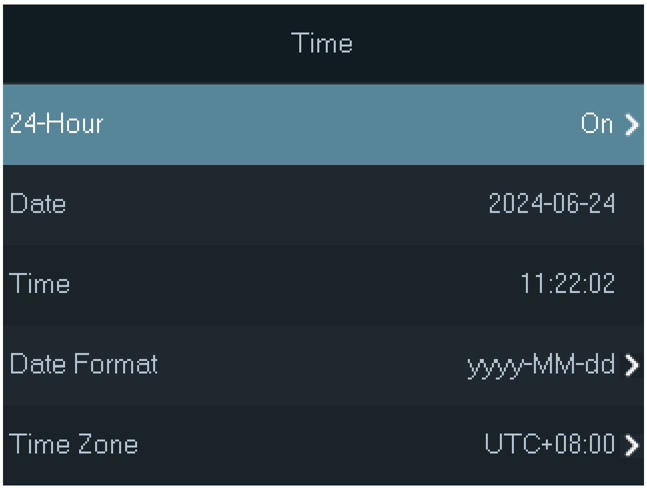
Configure system time, such as date and time.

Procedure

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

Step 2 Configure the time parameters.

Figure 2-24 Time settings



Time

24-Hour	On
Date	2024-06-24
Time	11:22:02
Date Format	yyyy-MM-dd
Time Zone	UTC+08:00

Table 2-9 Description of time parameters

Parameter	Description
24-Hour	Press <, > or OK to turn on or turn off the 24-hour format. Turn on it, the time is displayed in the 24-hour format. Turn off it, the time is displayed in the 12-hour format.

Parameter	Description
Date & Time	1. Press ▲ or ▼ to select **Date&Time**, and then press OK. 2. Press the number button to enter the date, and then press Esc.
Time	1. Press ▲ or ▼ to select **Time**, and then press OK. 2. Press the number button to enter the time, and then press Esc.
Date Format	1. Press ▲ or ▼ to select **Date Format**. 2. Press ◀, ▶ or OK to select the date format.
Time Zone	1. Press ▲ or ▼ to select **Time Zone**. 2. Press ◀, ▶ or OK to select the time zone.

2.9.2 Configuring Face Parameters

Configure the face parameters to change the accuracy of reorganization and improve the protection ability of the access control.

Background Information

⚠

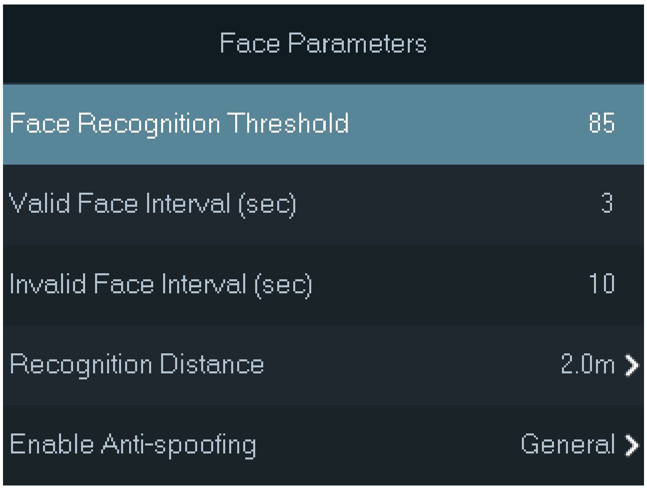
We recommend that this function be used by professional person for debugging.

Procedure

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

Step 2 Configure the face parameters.

Figure 2-25 Face parameters



Face Parameters

Face Recognition Threshold	85
Valid Face Interval (sec)	3
Invalid Face Interval (sec)	10
Recognition Distance	2.0m ›
Enable Anti-spoofing	General ›

Table 2-10 Description of face parameters

Name	Description
Face Recognition Threshold	Adjust the accuracy level of face recognition. Higher threshold means higher accuracy and lower false recognition rate. ⚠ When the threshold is too low such as 0, the false recognition rate will be extremely high. Please be advised.
Valid Face Interval (sec)	When the same face remains in front of the lens after the first successful recognition, the Device will perform recognition again for the face after a defined interval.
Invalid Face Interval (sec)	When the same face remains in front of the lens after the first failed recognition, the Device will perform recognition again for the face after a defined interval.
Recognition Distance	The distance between the face and the lens.
Enable Anti-spoofing	This prevents people from being able to use photos, videos, mask and other substitutes to gain unauthorized access.

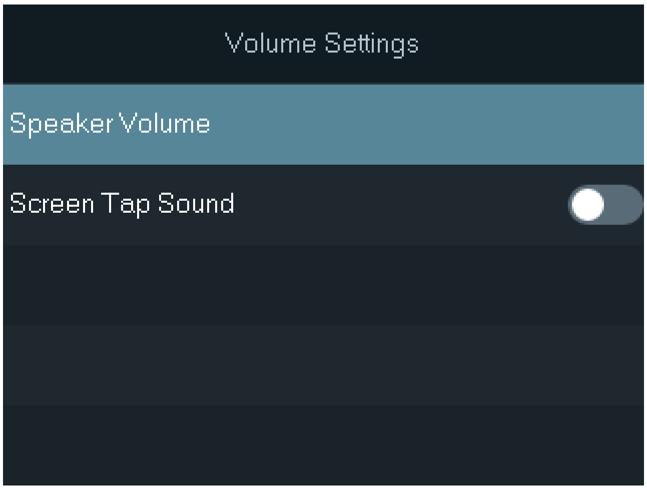
2.9.3 Configuring the Volume

Procedure

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

Step 2 Configure the parameters.

Figure 2-26 Volume settings



Volume Settings

Speaker Volume

Screen Tap Sound ○

Table 2-11 Parameters description

Parameters	Description
Speaker Volume	Select **Speaker Volume**, press OK, and then press ⌃ or ⌄ to adjust the volume.

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

2.9.4 Configuring the Language

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

2.9.5 Configuring Screen Parameters

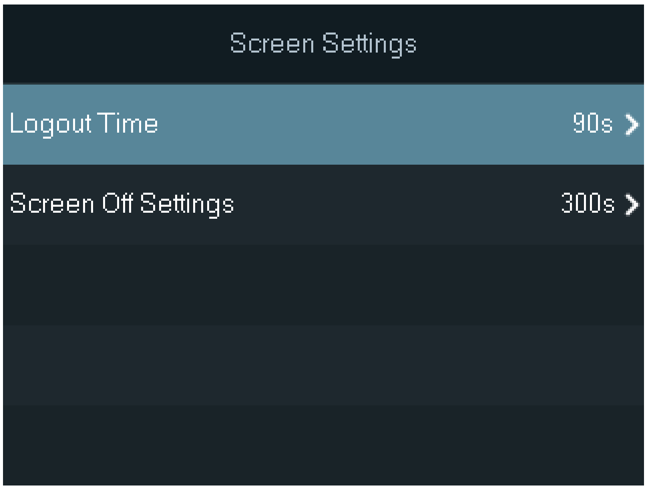
Configure when the display should turn off and the logout time.

Procedure

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

Step 2 Configure the parameters.

Figure 2-27 Screen settings



Logout Time 90s

Screen Off Settings 300s

Table 2-12 Parameters description

Parameters	Description
Logout Time	The system goes back to the standby screen after a defined time of inactivity.
Screen Off Settings	The system goes back to the standby screen and then the screen turns off after a defined time of inactivity.

Example

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

The logout time must be less than the screen off time.

2.9.6 Restoring Factory Defaults

Background Information

⚠

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

Procedure

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

Step 2 Restore factory defaults if necessary. Restore the factory default settings if necessary.

- **Factory Defaults** : Resets all configurations and data except for IP settings and the type of the extension module.
- **Restore to Default Settings (except for user information and logs)** : Resets all the configurations except for user information and logs.

2.9.7 Restarting the Device

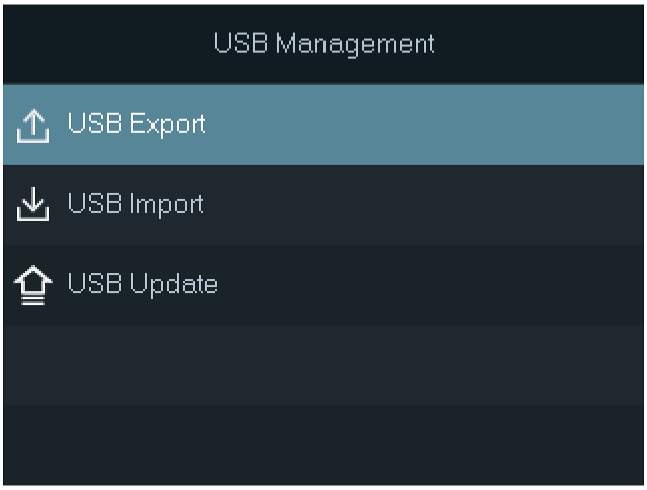
On the **Main Menu**, select **System** > **Restart**, press OK, and then press OK for the prompt. The Device will be restarted.

2.10 USB Management

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

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

Figure 2-28 USB management



2.10.1 Exporting to USB

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

Procedure

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

Step 2 Select the data type you want to export.

- When the data is exported in Excel, it can be edited.
- The USB disk supports the format in FAT32, and the storage capacity is 4 GB –128 GB.

  Personnel information, facial features, card data, fingerprint data are encrypted when exporting.

Step 3 Press OK to confirm.

The exported data is saved to the USB.

2.10.2 Importing from USB

You can import data from USB to the Device.

Procedure

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

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

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

2.10.3 Updating the System

Update the system of the Device through USB.

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

Procedure

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

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

Step 3 Press **OK**.

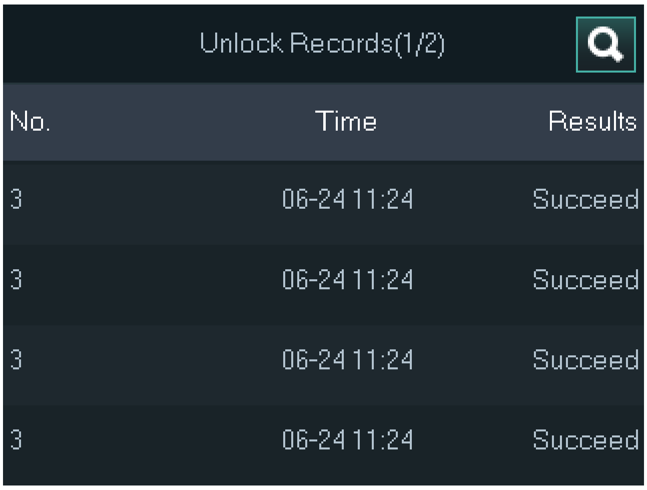
The Device will restart when the updating completes.

Do not power off the Device during the update.

2.11 Record Management

On the main menu, select **Records** > **Search for Unlock Records**. The unlock records are displayed. You can search for record by user ID.

Figure 2-29 Unlock records



Unlock Records(1/2)

No.	Time	Results
3	06-24 11:24	Succeed
3	06-24 11:24	Succeed
3	06-24 11:24	Succeed
3	06-24 11:24	Succeed

2.12 System Information

You can view data capacity and device version.

2.12.1 Viewing Data Capacity

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

2.12.2 Viewing Device Version

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

Related Operations

Select **Product Material QR Code**, press OK, and then scan the QR code with your phone to view the product documents.

This function is only available on select models.

3 Webpage Operations

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

Web configurations differ depending on models of the Device.

3.1 Initialization

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

Prerequisites

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

Procedure

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

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

Step 2 Select a language 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.

3.2 Resetting the Password

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

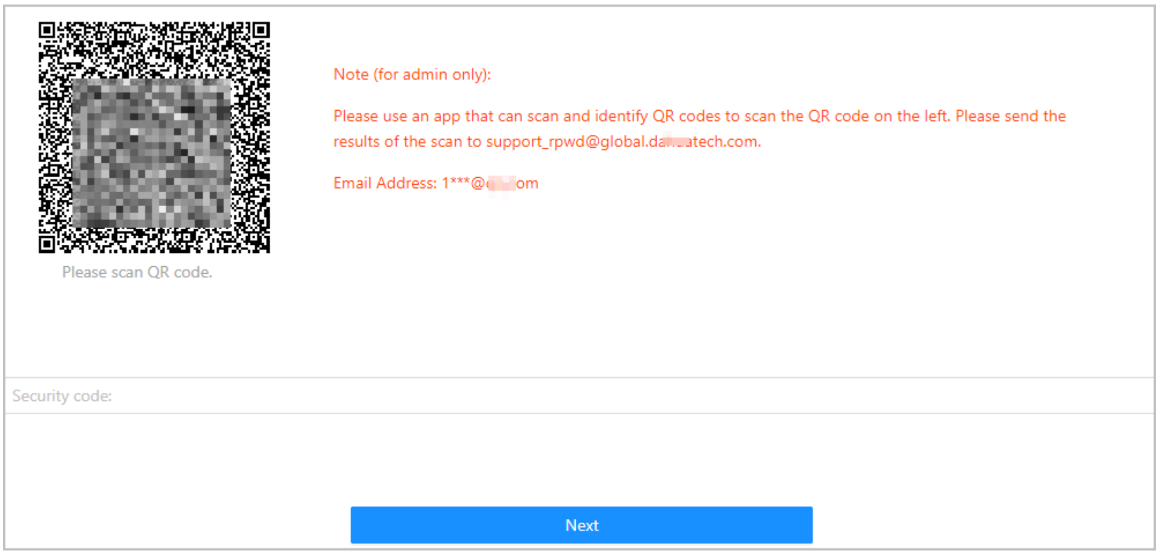
Procedure

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

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

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

Figure 3-1 Reset password



Note (for admin only):

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

Email Address: 1***@[redacted]om

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

Step 4 Enter the security code.

Step 5 Click **Next**.

Step 6 Reset and confirm the password.

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

Step 7 Click **OK**.

3.3 Home Page

The home page is displayed after you successfully log in.

Figure 3-2 Home page

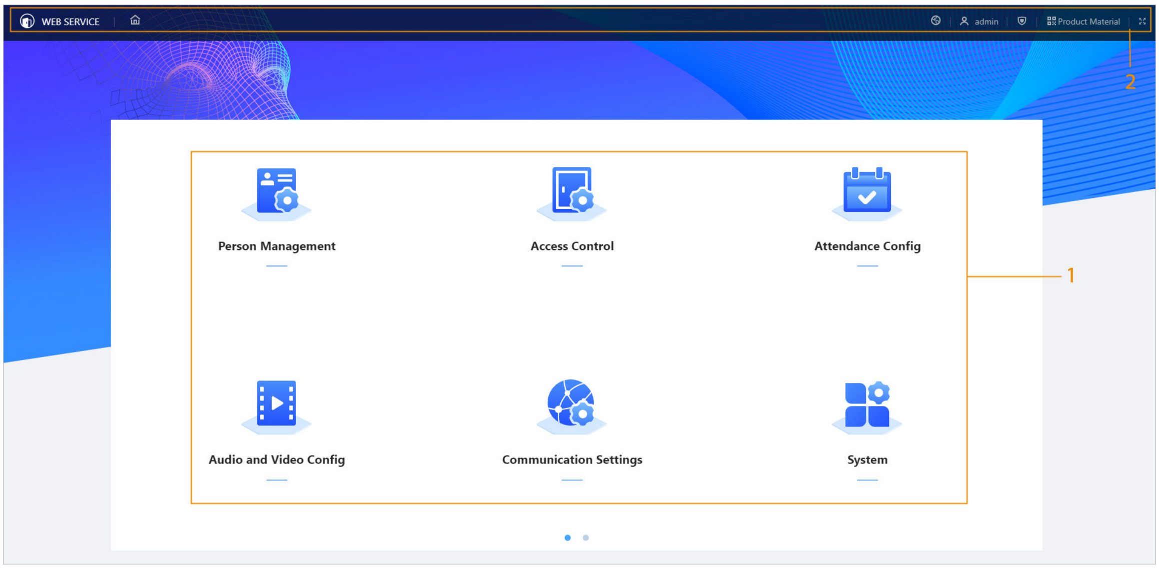


Table 3-1 Home page description

No.	Description
1	Main menu.
2	● ⌂: Enter the home page. ● ⛶: Display in full screen. ● 🛡: Enter the **Security** page. ● Product Material: Scan the QR code with your phone to view the product documents. 📖 This function is only available on select models ● admin: Log out or restart the device. ● 🌐: Select a language on the device.

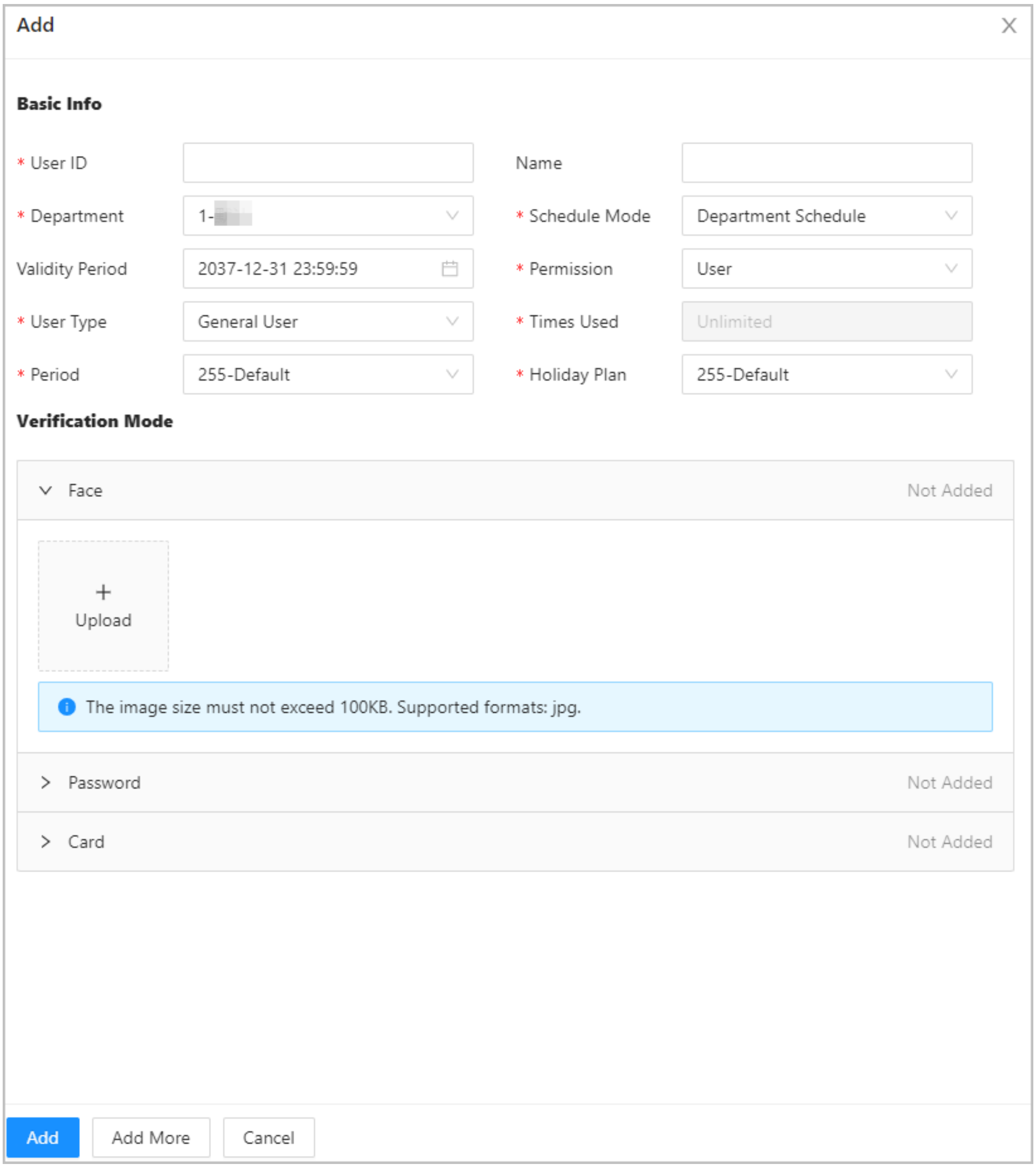
3.4 Person Management

Procedure

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

Step 2 Configure user information.

Figure 3-3 Add users



Add

Basic Info

* User ID

Name

* Department 1-[redacted]

* Schedule Mode Department Schedule

Validity Period 2037-12-31 23:59:59

* Permission User

* User Type General User

* Times Used Unlimited

* Period 255-Default

* Holiday Plan 255-Default

Verification Mode

Face Not Added

The image size must not exceed 100KB. Supported formats: jpg.

Password Not Added

Card Not Added

Table 3-2 Parameters description

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

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

Parameter	Description
Face	Click **Upload** to upload a face image. Each person can only add up to 2 face images. You can view or delete the face image after you upload it. The face image is in jpg, jpeg, png format and must be less than 100 KB.
Card	This function is only available on select models. - 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. 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. 3. Click **Add**. A user can register up to 5 cards at most. Enter your card number or swipe your card, and then the card information will be read by the Device. You can enable the **Duress Card** function. An alarm will be triggered if a duress card is used to unlock the door. - : Set duress card. - : Change card number. One user can only set one duress card.
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
Fingerprint	Register fingerprints. A user can register up to 3 fingerprints, and you can set a fingerprint to the duress fingerprint. An alarm will be triggered when the duress fingerprint is used to unlock the door. Enroll fingerprints through an enrollment reader or the Device. 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.

Step 3 Click **OK**.

Related Operations

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

  Up to 10,000 users can be imported at a time.
- Clear: Clear all users.
- Refresh: Refresh the user list.
- Search: Search by user name or user ID.

3.5 Configuring Access Control

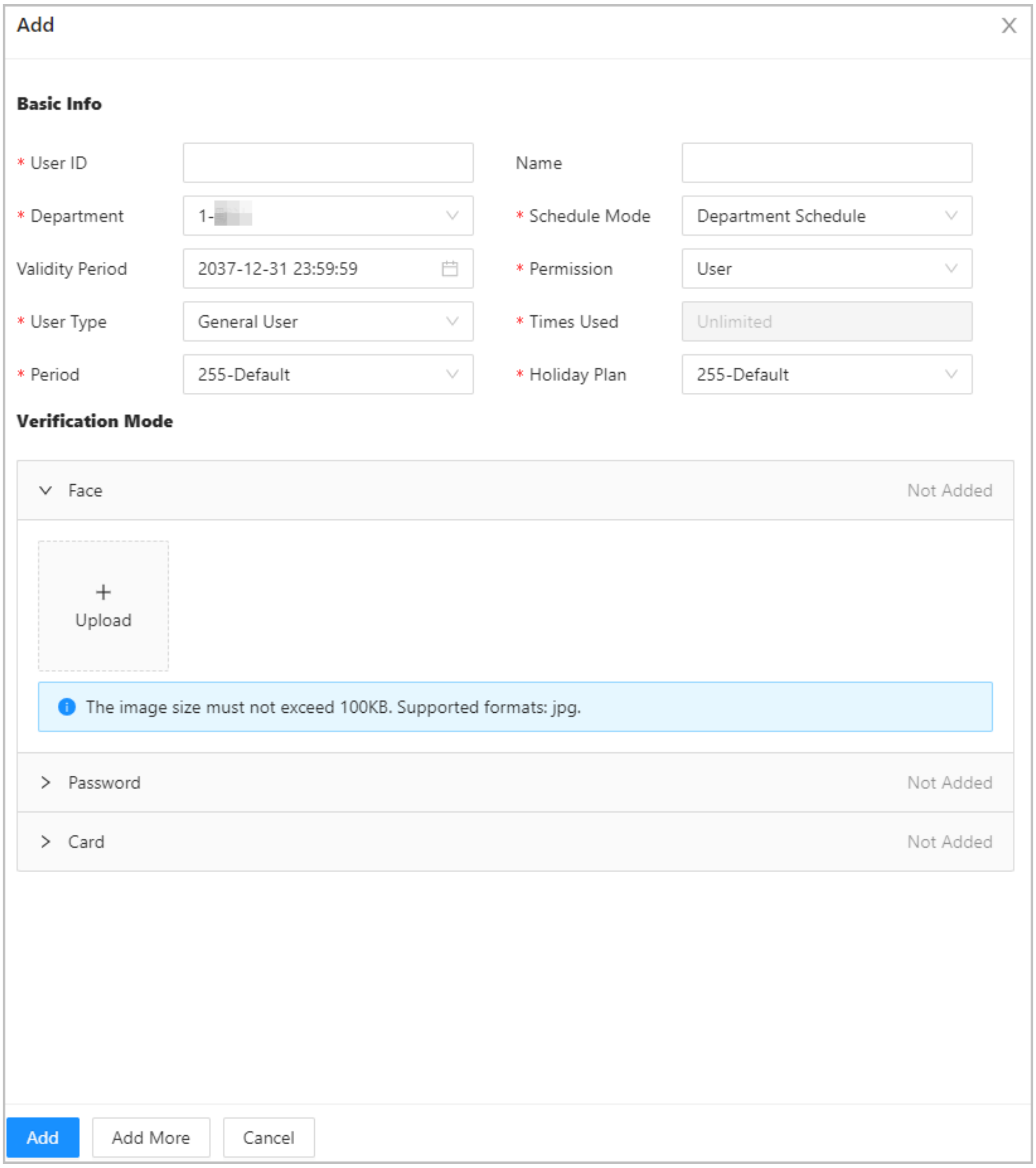
3.5.1 Person Management

Procedure

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

Step 2 Configure user information.

Figure 3-4 Add users



Add

Basic Info

* User ID		Name	
* Department	1-[redacted]	* Schedule Mode	Department Schedule
Validity Period	2037-12-31 23:59:59	* Permission	User
* User Type	General User	* Times Used	Unlimited
* Period	255-Default	* Holiday Plan	255-Default

Verification Mode

Face: Not Added

The image size must not exceed 100KB. Supported formats: jpg.

Password: Not Added

Card: Not Added

Table 3-3 Parameters description

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

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

Parameter	Description
Face	Click **Upload** to upload a face image. Each person can only add up to 2 face images. You can view or delete the face image after you upload it. The face image is in jpg, jpeg, png format and must be less than 100 KB.
Card	This function is only available on select models. - 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. 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. 3. Click **Add**. A user can register up to 5 cards at most. Enter your card number or swipe your card, and then the card information will be read by the Device. You can enable the **Duress Card** function. An alarm will be triggered if a duress card is used to unlock the door. - : Set duress card. - : Change card number. One user can only set one duress card.
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
Fingerprint	Register fingerprints. A user can register up to 3 fingerprints, and you can set a fingerprint to the duress fingerprint. An alarm will be triggered when the duress fingerprint is used to unlock the door. Enroll fingerprints through an enrollment reader or the Device. 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.

Step 3 Click **OK**.

Related Operations

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

  Up to 10,000 users can be imported at a time.
- Clear: Clear all users.
- Refresh: Refresh the user list.
- Search: Search by user name or user ID.

3.5.2 Configuring Access Control Parameters

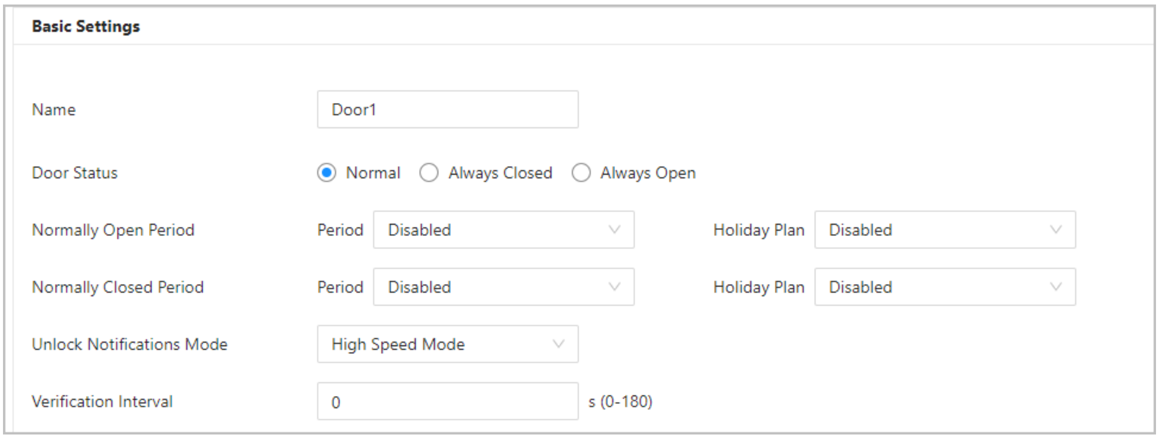
3.5.2.1 Configuring Basic Parameters

Procedure

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

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

Figure 3-5 Basic parameters



Basic Settings

Name: Door1

Door Status: ● Normal ○ Always Closed ○ Always Open

Normally Open Period: Period Disabled; Holiday Plan Disabled

Normally Closed Period: Period Disabled; Holiday Plan Disabled

Unlock Notifications Mode: High Speed Mode

Verification Interval: 0 s (0-180)

Table 3-4 Basic parameters description

Parameter	Description
Name	The name of the door.
Door Status	Set the door status. ● Normal: The door will be unlocked and locked according to your settings. ● Always Open: The door remains unlocked all the time. ● Always Closed: The door remains locked all the time.
Normally Open Period	When you select **Normal**, you can select a time template from the drop-down list. The door remains open or closed during the defined time. For details on how to configure periods and holiday plans, see "3.5.7 Configuring Schedules". ● When normally open period conflicts with normally closed period, normally open period takes priority over normally closed period. ● When period conflict with holiday plan, holiday plans takes priority over periods.
Normally Closed Period	
Unlock Notification	Displays the notification on the screen when a person verifying their identity on the Device. ● High Speed Mode: The system prompts **Successfully verified** or **Not authorized** on the screen. ● Simple Mode: Displays user ID, name and verification time after access granted; displays **Not authorized** and authorization time after access denied. ● Standard: Displays user's registered face image, user ID, name and verification time after access granted; displays **Not authorized** and verification time after access denied. ● Contrast Mode: Displays the captured face image and a registered face image of a user, user ID, name and authorization time after access granted; displays **Not authorized** and authorization time after access denied.

Parameter	Description
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.

Step 3 Click **Apply**.

3.5.2.2 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.

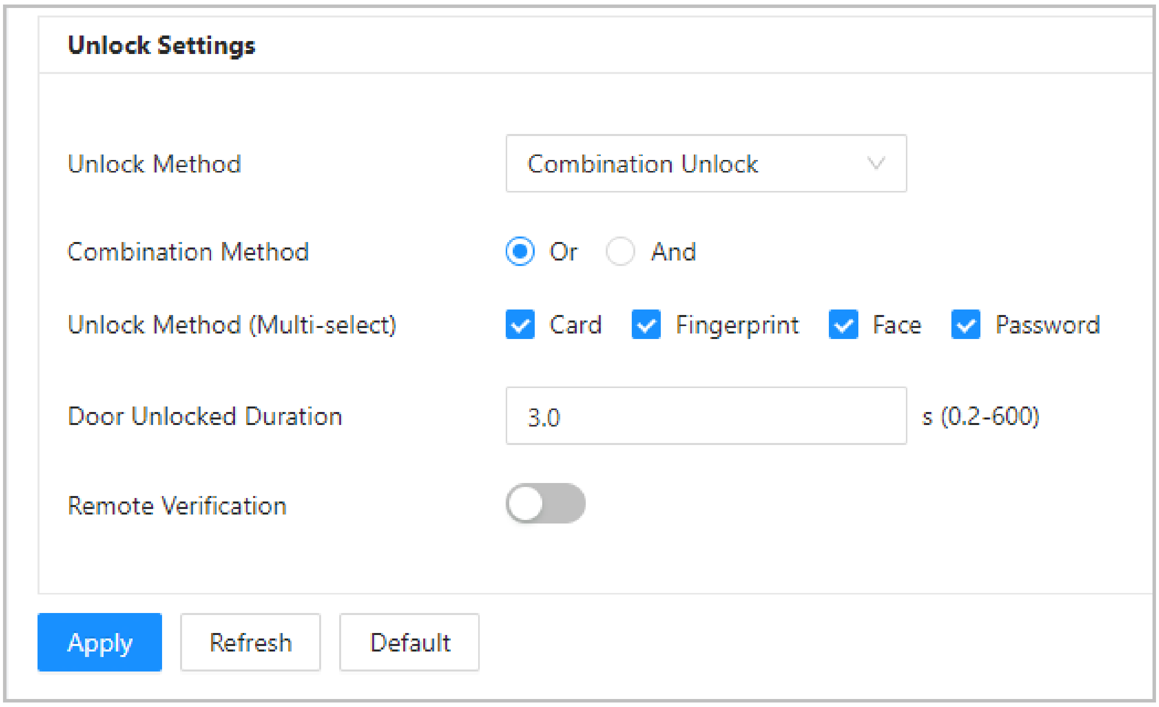
Procedure

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

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

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

Figure 3-6 Unlock settings



Unlock Settings

Unlock Method: Combination Unlock

Combination Method: ● Or ○ And

Unlock Method (Multi-select): ☑ Card ☑ Fingerprint ☑ Face ☑ Password

Door Unlocked Duration: 3.0 s (0.2-600)

Remote Verification: off

Table 3-5 Unlock settings description

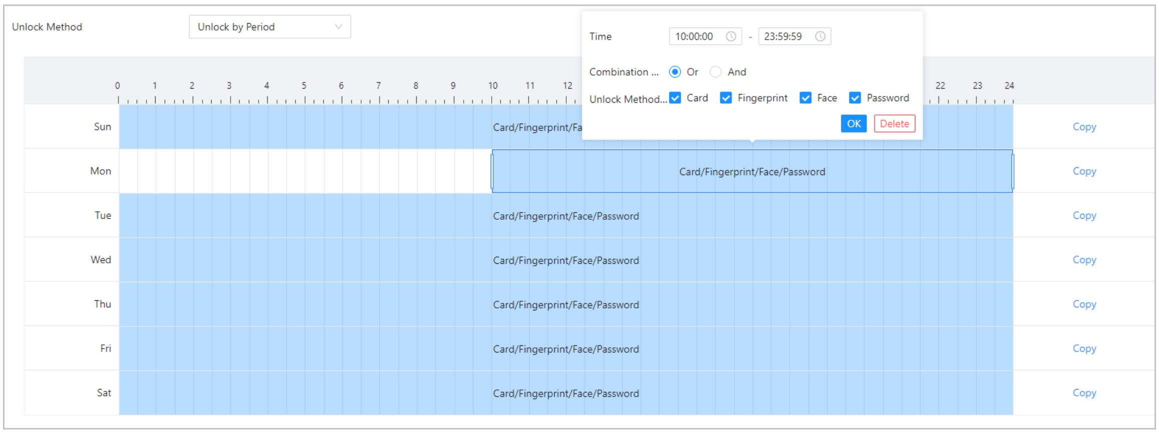
Parameter	Description
Unlock Method (Multi-select)	Unlock methods might differ depending on the models of product.
Door Unlock Duration	After a person is granted access, the door will remain unlocked for a defined time for them to pass through. It ranges from 0.2 to 600 seconds.
Unlock Timeout	When the door detector and the unlock timeout alarm are enabled, a timeout alarm will be triggered if the door remains unlocked longer than the defined unlock time.
Remote Verification	Open the door remotely.

- Unlock by period

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

   You can also click **Copy** to apply the configured time period to other days.
3. Select an unlock method for the time period, and then configure other parameters.

Figure 3-7 Unlock by period



Unlock Method: Unlock by Period

Time: 10:00:00 - 23:59:59

Combination ...: ● Or ○ And

Unlock Method...: ☑ Card ☑ Fingerprint ☑ Face ☑ Password

OK Delete

Sun	Card/Fingerprint/Fa	Copy
Mon	Card/Fingerprint/Face/Password	Copy
Tue	Card/Fingerprint/Face/Password	Copy
Wed	Card/Fingerprint/Face/Password	Copy
Thu	Card/Fingerprint/Face/Password	Copy
Fri	Card/Fingerprint/Face/Password	Copy
Sat	Card/Fingerprint/Face/Password	Copy

- Unlock by multiple users.

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

- ◇ You can add up to 4 groups.
- ◇ 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.

Step 3 Click **Apply**.

3.5.3 Configuring Alarms

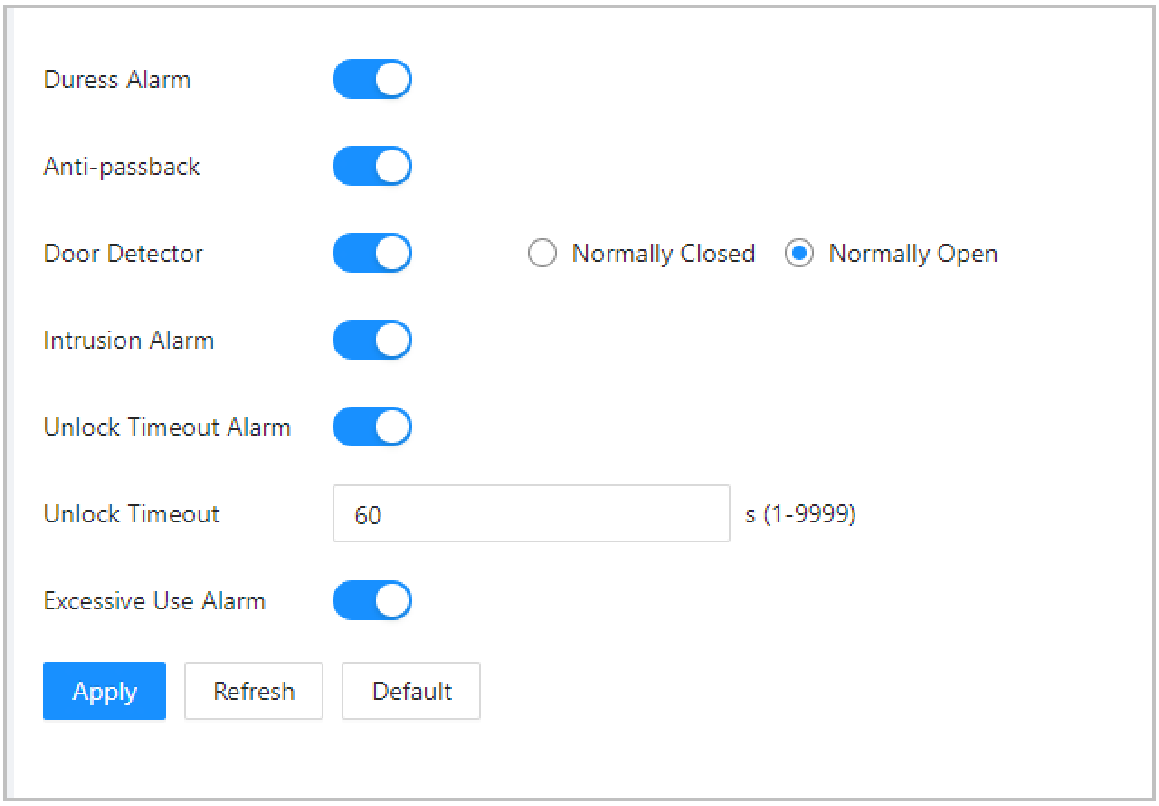
An alarm will be triggered when an abnormal access event occurs.

Procedure

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

Step 2 Configure alarm parameters.

Figure 3-8 Alarm



Duress Alarm

Anti-passback

Door Detector ○ Normally Closed ● Normally Open

Intrusion Alarm

Unlock Timeout Alarm

Unlock Timeout 60 s (1-9999)

Excessive Use Alarm

Table 3-6 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. ● Normally Closed: The sensor is in a shorted position when the door or window is closed. ● Normally Open: 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. 🕮 The door detector and door timed out function need to be enabled at the same time.
Unlock Timeout	
Excessive Use Alarm	If the wrong password or card is used 5 times in a row within 60 seconds, the alarm for excessive use of illegal card will be triggered and lasts for a defined time.

Step 3 Click **Apply**.

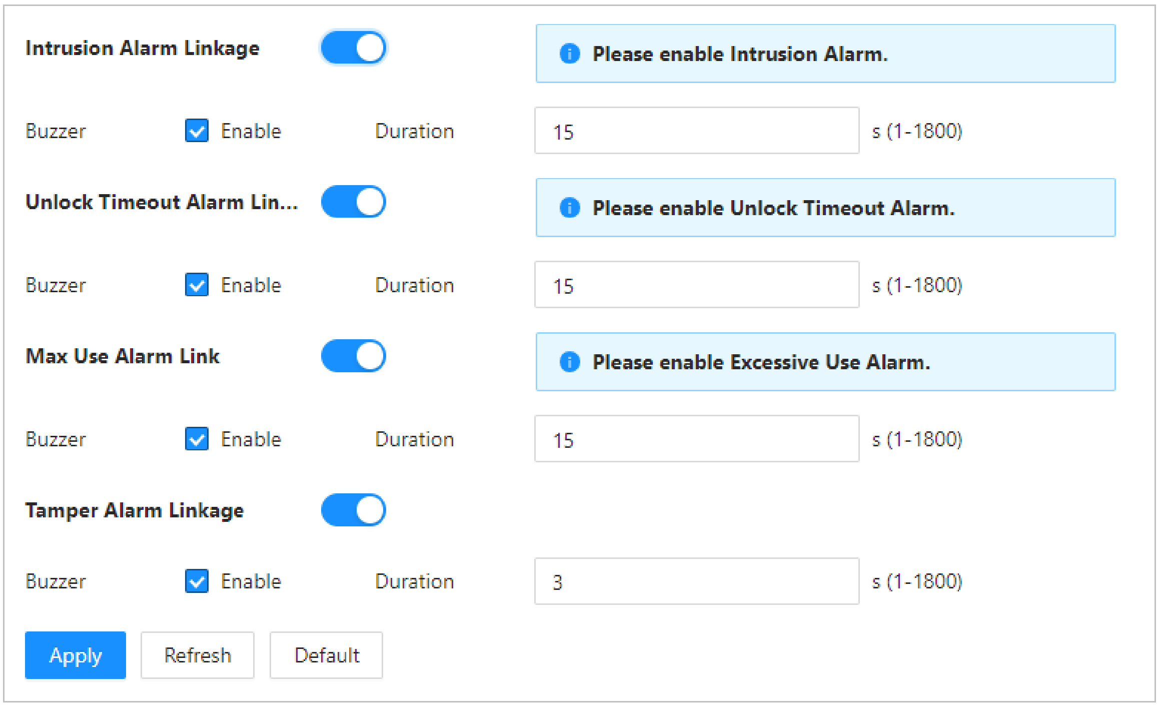
3.5.4 Configuring Alarm Event Linkage

Procedure

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

Step 2 Configure alarm event linkages.

Figure 3-9 Alarm event linkage



Intrusion Alarm Linkage — on — Please enable Intrusion Alarm.

Buzzer ☑ Enable Duration 15 s (1-1800)

Unlock Timeout Alarm Lin... — on — Please enable Unlock Timeout Alarm.

Buzzer ☑ Enable Duration 15 s (1-1800)

Max Use Alarm Link — on — Please enable Excessive Use Alarm.

Buzzer ☑ Enable Duration 15 s (1-1800)

Tamper Alarm Linkage — on

Buzzer ☑ Enable Duration 3 s (1-1800)

Table 3-7 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.
Unlock Timeout Alarm Linkage	When the door remains unlocked for longer than the defined timeout duration, the door timeout alarm will be triggered and last for the defined time. Buzzer: The buzzer sounds when the unlock timeout alarm is triggered. You can configure the alarm duration.
Excessive Use Alarm Linkage	If the wrong password or card is used 5 times in a row within 60 seconds, the alarm for excessive use of illegal card will be triggered and lasts for a defined time. Buzzer: The buzzer sounds when the excessive use alarm is triggered. You can configure the alarm duration.

Parameter	Description
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.

3.5.5 Configuring Face Parameters

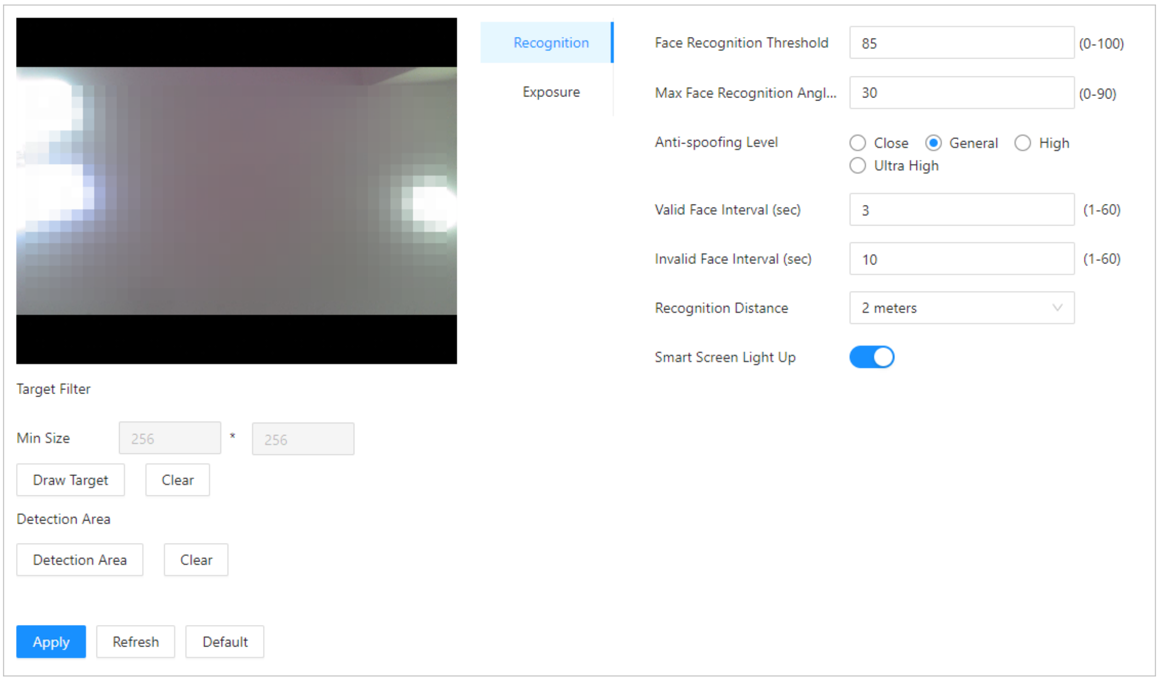
Configure face detection parameters. Face parameters might differ depending on models of the product.

Procedure

Step 1 Log in to the webpage.

Step 2 Select **Access Control** > **Face Parameters**.

Figure 3-10 Face detection parameters



Face Recognition Threshold 85 (0-100)

Max Face Recognition Angl... 30 (0-90)

Anti-spoofing Level ○ Close ● General ○ High ○ Ultra High

Valid Face Interval (sec) 3 (1-60)

Invalid Face Interval (sec) 10 (1-60)

Recognition Distance 2 meters

Smart Screen Light Up ●

Min Size 256 * 256

Step 3 Configure the parameters.

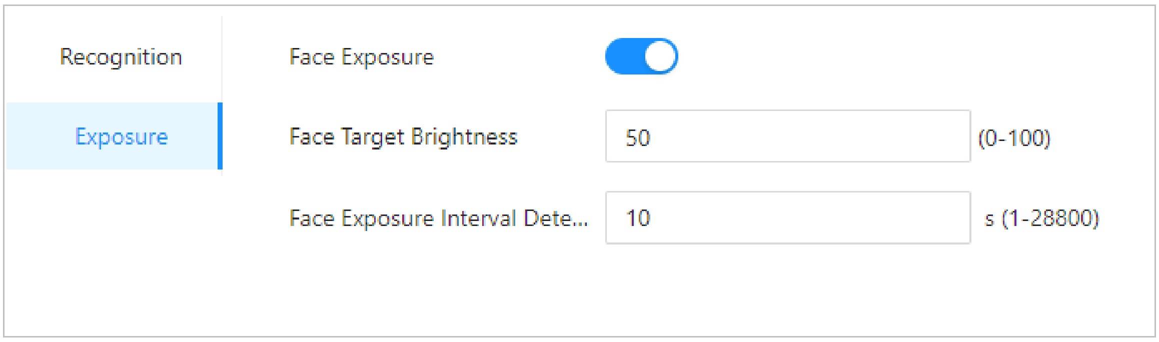
Table 3-8 Description of face parameters

Name	Description
Face Recognition Threshold	Adjust the accuracy level of face recognition. Higher threshold means higher accuracy and lower false recognition rate. When the threshold is too low such as 0, the false recognition rate will be extremely high. Please be advised.

Name	Description
Max Face Recognition Angle Deviation	Set the largest angle that a face can be posed in for face detection. The larger the value, the larger the range for the face angle. If the angle a face is positioned in is not within the defined range, it might not be detected properly.
Anti-spoofing Level	This prevents people from being able to use photos, videos, mask and other substitutes to gain unauthorized access.
Valid Face Interval (sec)	When the same face remains in front of the lens after the first successful recognition, the Device will perform recognition again for the face after a defined interval.
Invalid Face Interval (sec)	When the same face remains in front of the lens after the first failed recognition, the Device will perform recognition again for the face after a defined interval.
Recognition Distance	The distance between the face and the lens.
Smart Screen Light Up	When enabled, in the screen-off status, the screen will light up when a face is detected.

Step 4 Configure the exposure parameters.

Figure 3-11 Exposure parameters



Face Exposure ●

Face Target Brightness 50 (0-100)

Face Exposure Interval Dete... 10 s (1-28800)

Table 3-9 Exposure parameters description

Parameter	Description
Face Exposure	After the face exposure function is enabled, the face will be exposed at the defined brightness to detect the face image clearly.
Face Target Brightness	
Face Exposure Interval Detection	The face will be exposed only once in a defined interval.

Step 5 Click **Apply**.

Related Operations

- Draw the face detection area.
  1. Click **Detection Area**.
  2. Right-click to draw the detection area, and then release the left button of the mouse to complete drawing.

     The face in the defined area will be detected.
  3. Click **Apply**.
- Draw the target size.

1. Click **Draw Target**.
2. Draw the face recognition box to define the minimum size of detected face.

   Only when the size of the face is larger than the defined size, the face can be detected by the Device.
3. Click **Apply**.

3.5.6 Configuring Card Settings

Background Information

This function is only available on select models.

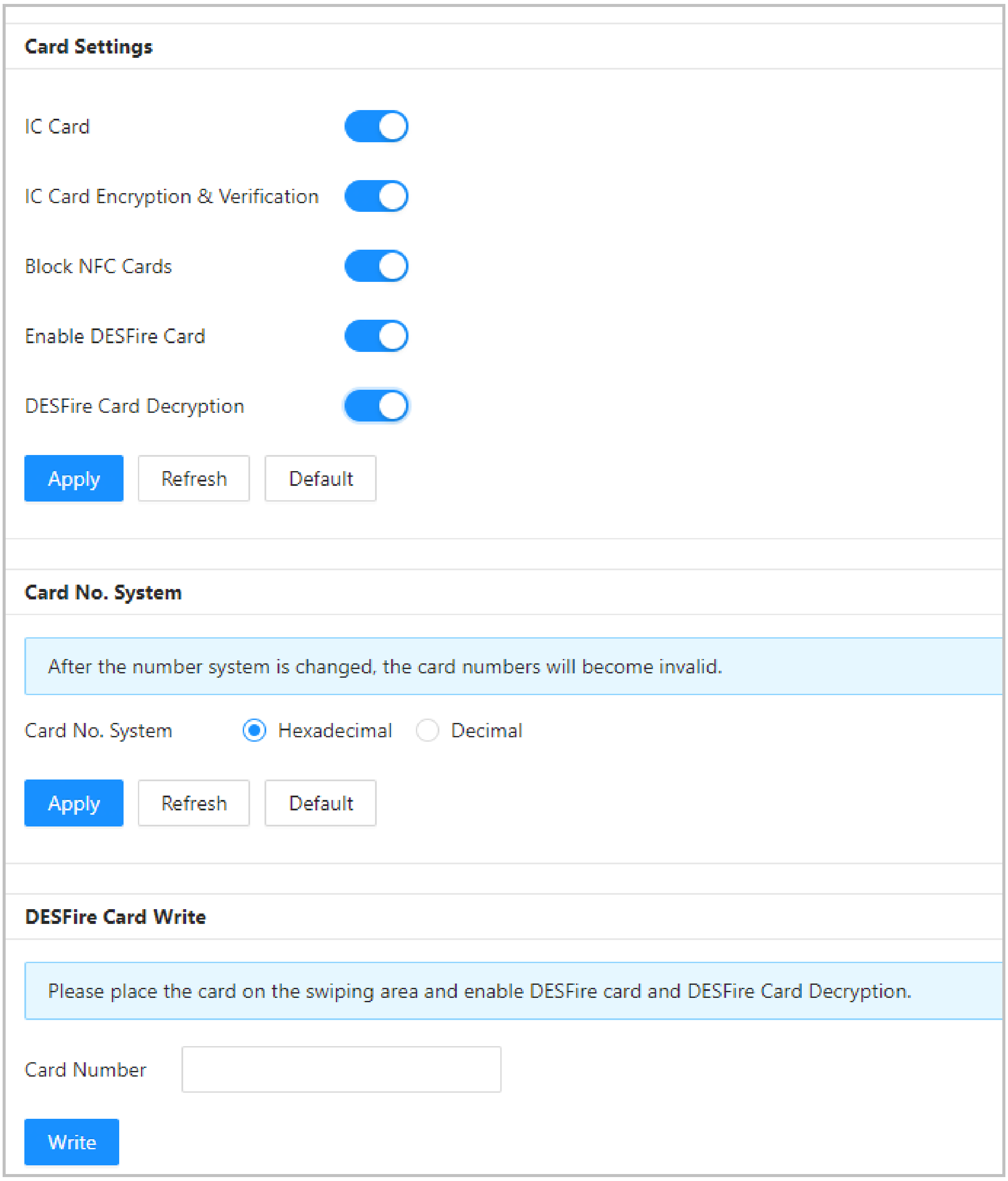
Procedure

Step 1 Log in to the webpage.

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

Step 3 Configure the card parameters.

Figure 3-12 Card parameters



Card Settings

IC Card: on

IC Card Encryption & Verification: on

Block NFC Cards: on

Enable DESFire Card: on

DESFire Card Decryption: on

Card No. System

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

Card No. System ● Hexadecimal ○ Decimal

DESFire Card Write

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

Card Number

Table 3-10 Card parameters description

Item	Parameter	Description
Card Settings	IC Card	The IC card can be read when this function is enabled. 📖 This function is only available on select models.

Item	Parameter	Description
	IC Card Encryption & Verification	The encrypted card can be read when this function is enabled. Make sure **IC Card** is enabled.
	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 **IC Card** is enabled. ● NFC function is only available on select models of phones.
	Enable 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	Card Number	Place the card on the reader, enter the card number, and then click **Write** to write card number to the card. ● Desfire card function must be enabled. ● Only supports hexadecimal format. ● Supports up to 8 characters.

Step 4 Click **Apply**.

3.5.7 Configuring Schedules

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

3.5.7.1 Configuring Time Periods

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.

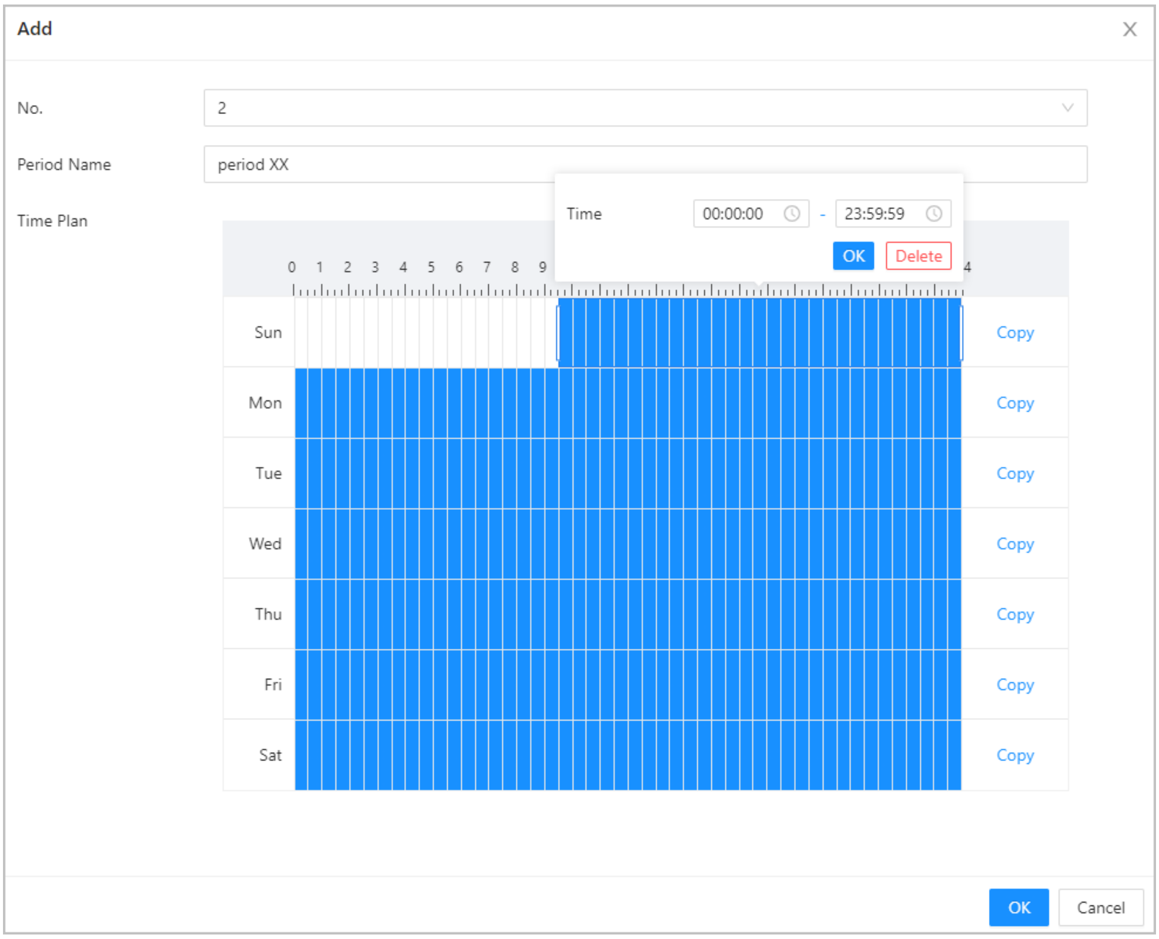
Procedure

Step 1 Log in to the webpage.

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

Step 3 Click **Add**.

Figure 3-13 Configure time periods



Add

No. 2

Period Name period XX

Time Plan

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

Step 4 Drag the time slider to configure time for each day.

Step 5 (Optional) Click **Copy** to copy the configuration to the rest of days.

Step 6 Click **OK**.

3.5.7.2 Configuring Holiday Plans

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

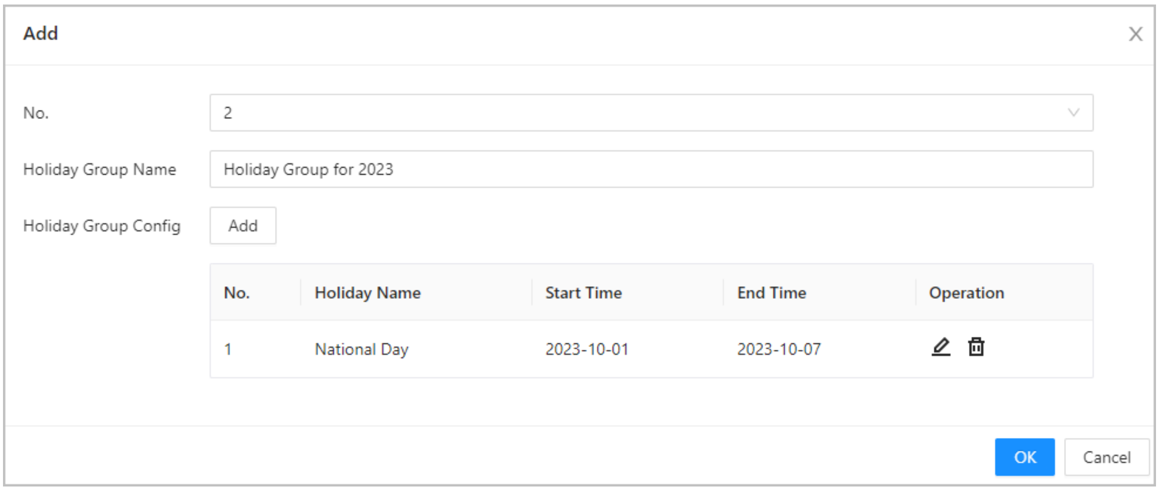
Step 1 Log in to the webpage.

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

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

Step 4 Select a number for the holiday group, and then enter a name for the group.

Figure 3-14 Add a holiday group



No. 2

Holiday Group Name Holiday Group for 2023

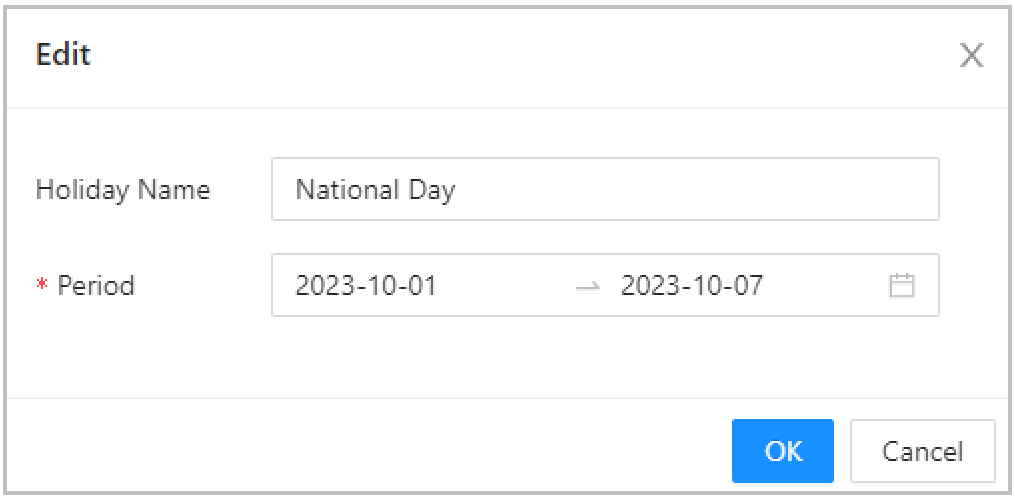
Holiday Group Config

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

Step 5 Click **Add**, and then add a holiday to a holiday group.

Step 6 Click **OK**.

Figure 3-15 Add a holiday to a holiday group



Holiday Name National Day

* Period 2023-10-01 → 2023-10-07

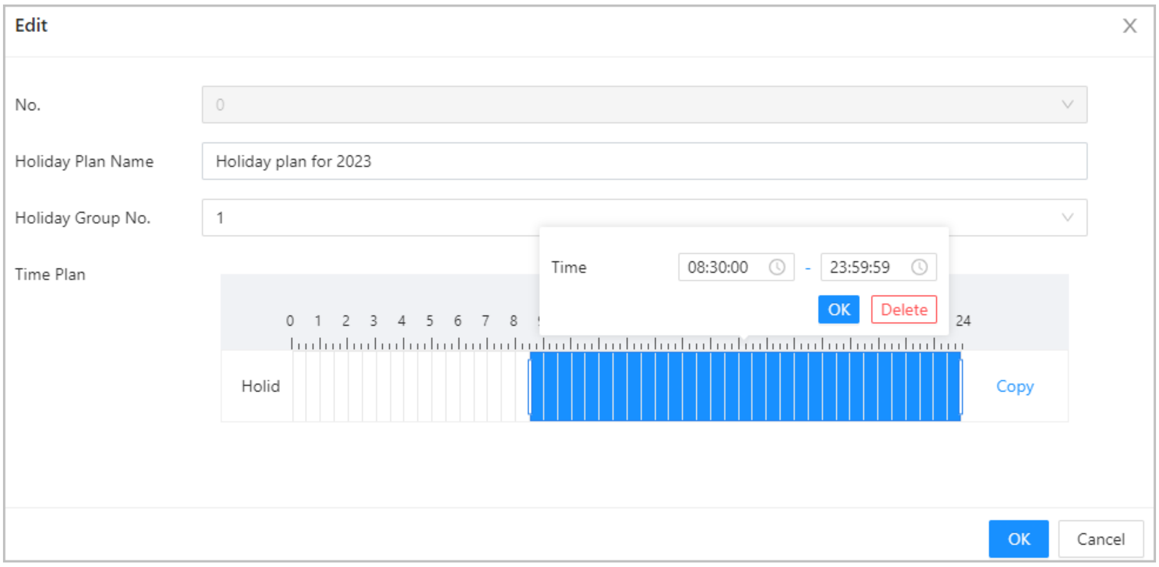
Step 7 Click **Plan Management** , and then click **Add**.

Step 8 Select a number for the holiday plan, and then enter a name for it.

Step 9 Select a holiday group, and then drag the slider to configure time for each day.

Supports adding up to 4 time sections on a day.

Figure 3-16 Add holiday plan


Edit

No. 0

Holiday Plan Name: Holiday plan for 2023

Holiday Group No. 1

Time Plan

Time 08:30:00 - 23:59:59

Step 10 Click **OK**.

3.5.8 Privacy Settings

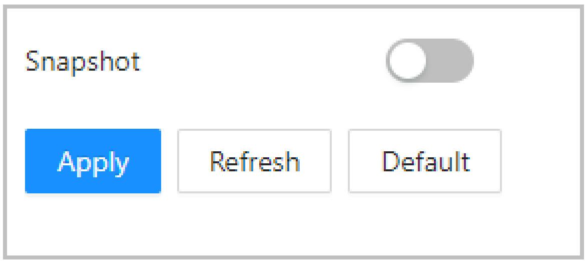
Procedure

Step 1 On the webpage, select **Access Control** > **Privacy Settings**.

Step 2 Enable snapshot function.

Face images will be captured automatically when people unlock the door.

Figure 3-17 Enable snapshot



Step 3 Click **Apply**.

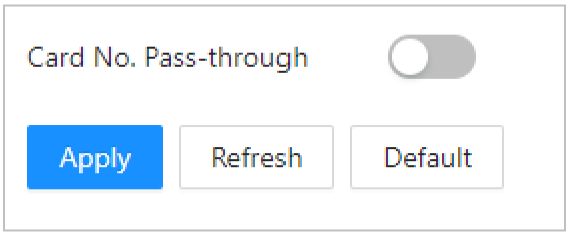
3.5.9 Configuring Back-end Comparison

Directly pass data such as card number to the third-party platform for data validation rather than validating data on the Device.

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

After the function is enabled, the card number passed to the third-party platform for data validation.

Figure 3-18 Back-end comparison



Card No. Pass-through

3.6 Configuring Attendance

This function is only available on select models.

3.6.1 Configuring Departments

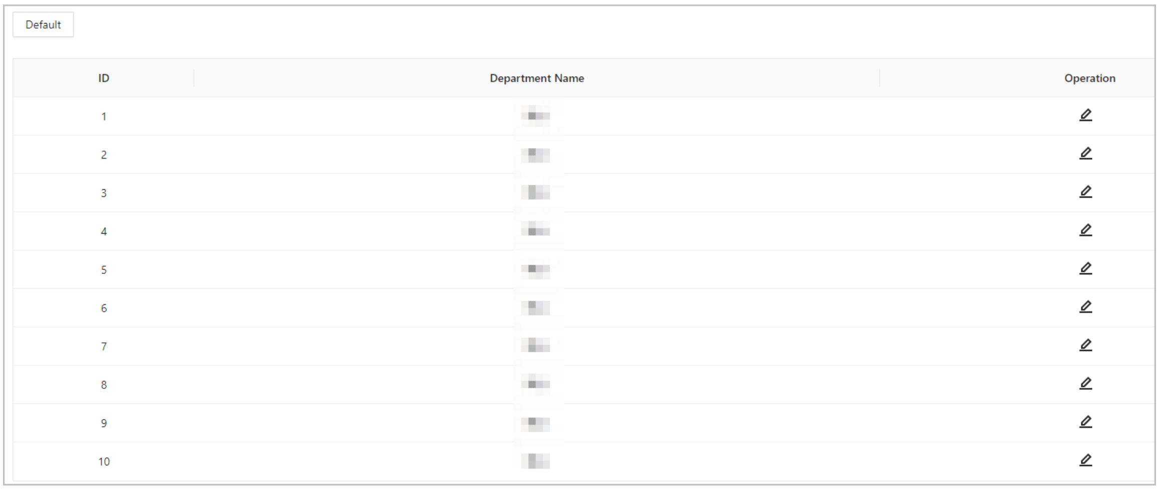
Procedure

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

Step 2 Click ✎ to rename the department.

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

Figure 3-19 Create departments



Default

ID	Department Name	Operation
1	[redacted]	✎
2	[redacted]	✎
3	[redacted]	✎
4	[redacted]	✎
5	[redacted]	✎
6	[redacted]	✎
7	[redacted]	✎
8	[redacted]	✎
9	[redacted]	✎
10	[redacted]	✎

Related Operations

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

3.6.2 Configuring Shifts

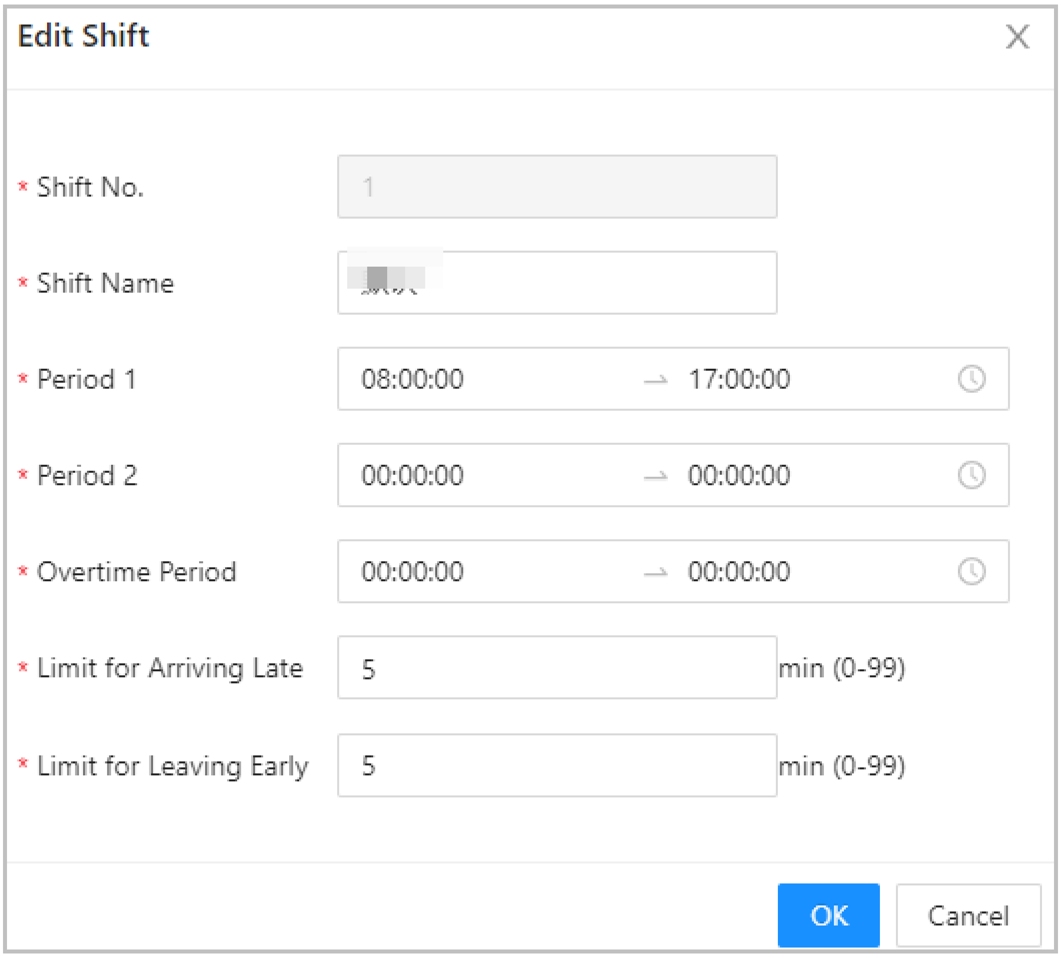
Configure shifts to define time attendance rules. Employees need to work at the time scheduled for their shift to start, and leave at the end time, except when they choose to work overtime.

Procedure

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

Step 2 Click ✎ to configure the shift.

Figure 3-20 Create shifts



Edit Shift

* Shift No. 1

* Shift Name [redacted]

* Period 1 08:00:00 → 17:00:00

* Period 2 00:00:00 → 00:00:00

* Overtime Period 00:00:00 → 00:00:00

* Limit for Arriving Late 5 min (0-99)

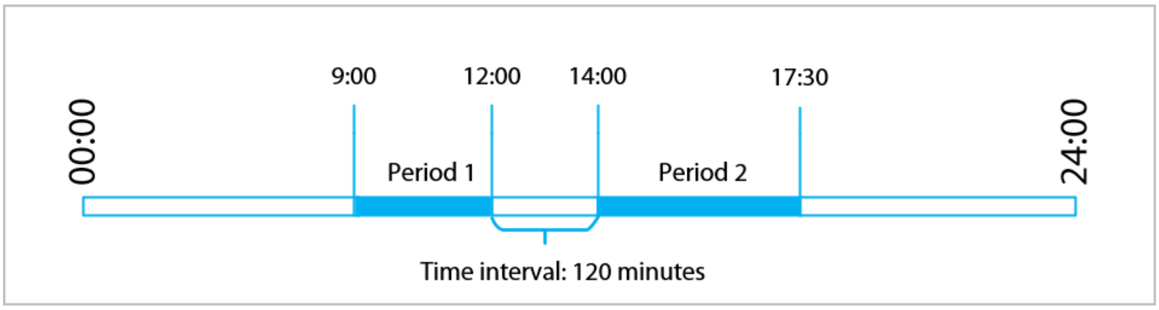
* Limit for Leaving Early 5 min (0-99)

Table 3-11 Shift parameters description

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

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

Figure 3-21 Time interval (even number)

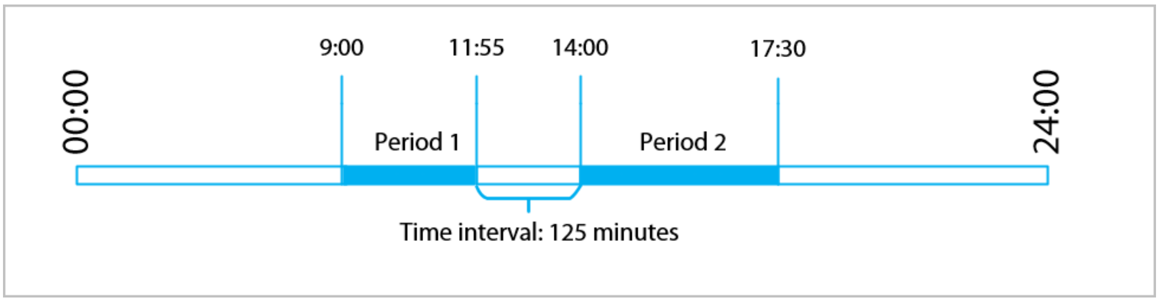


For example: If the interval is 120 minutes, then the clock-out time for period 1 is from 12:00 to 12:59, and the clock-in time for period 2 is from 13:00 to 14:00.

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

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

Figure 3-22 Time interval (even number)



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

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

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

Step 3 Click **OK**.

Related Operations

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

3.6.3 Configuring Holiday

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

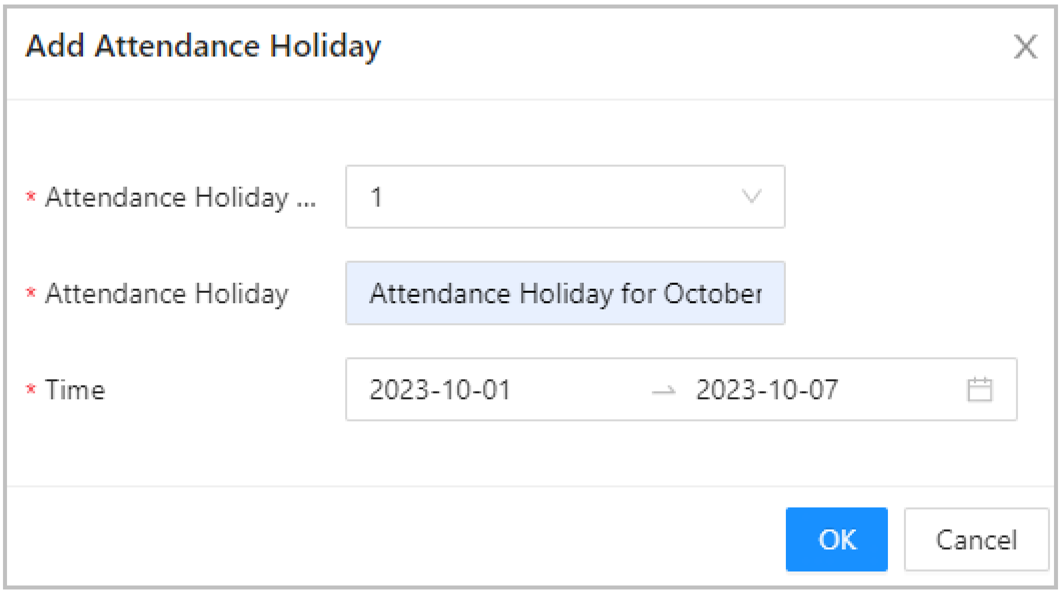
Procedure

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

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

Step 3 Configure the parameters.

Figure 3-23 Create holiday plans



Add Attendance Holiday

* Attendance Holiday ...: 1

* Attendance Holiday: Attendance Holiday for October

* Time: 2023-10-01 → 2023-10-07

Table 3-12 Parameters description

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

Step 4 Click **OK**.

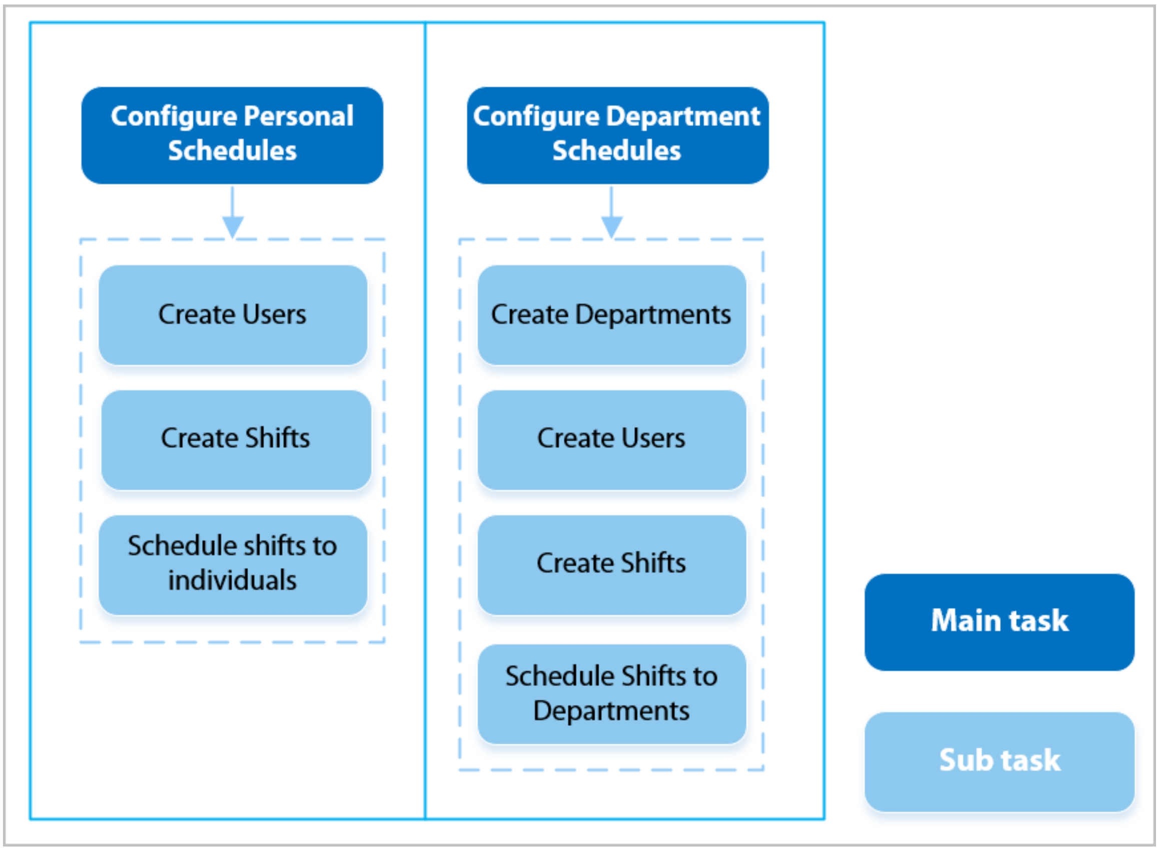
3.6.4 Configuring Work Schedules

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

Background Information

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

Figure 3-24 Configuring work schedules


Configure Personal Schedules
Create Users
Create Shifts
Schedule shifts to individuals
Configure Department Schedules
Create Departments
Create Users
Create Shifts
Schedule Shifts to Departments
Main task
Sub task

Procedure

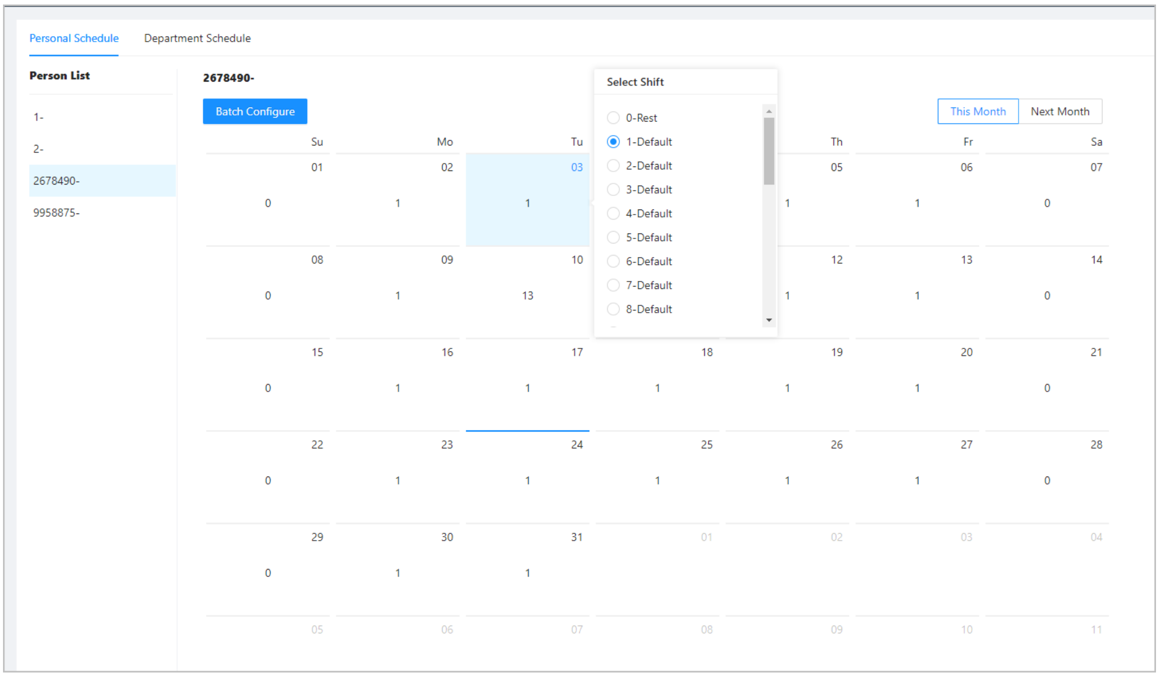
Step 1 Select **Attendance Config** > **Schedule Config**.

Step 2 Set work schedules for individuals.

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

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

Figure 3-25 Personal schedule



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

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

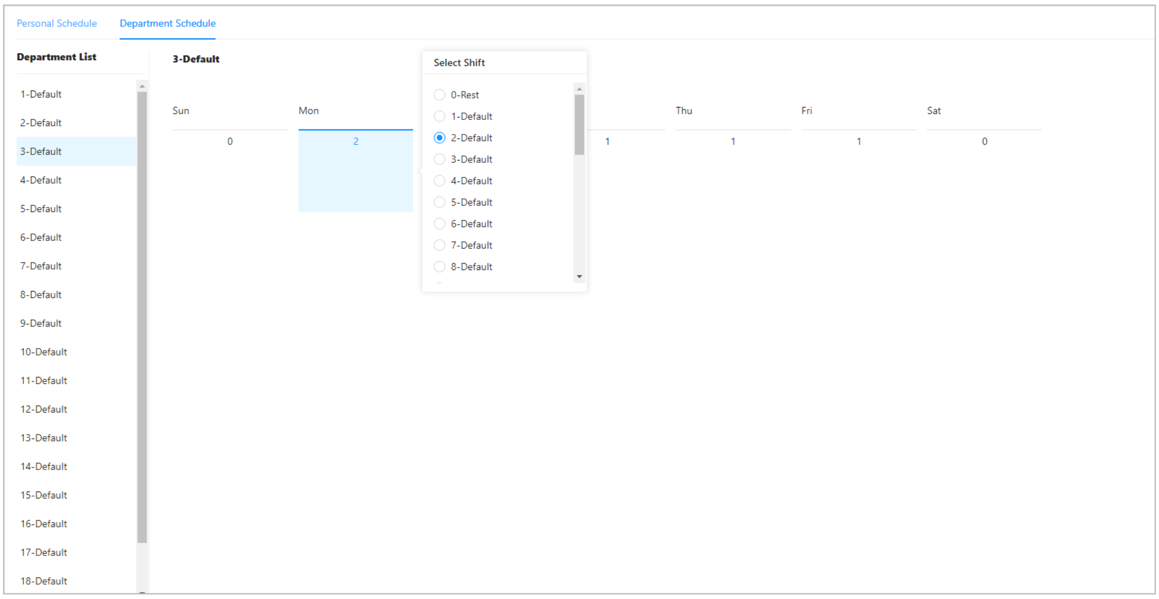
- 0 indicates break.
- 1 to 24 indicates the number of the per-defined shifts.
- 25 indicates business trip.
- 26 indicates leave of absence.

Step 3 Set works schedules for departments.

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

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

Figure 3-26 Schedule shifts to a department



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

3.6.5 Configuring Attendance Modes

Procedure

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

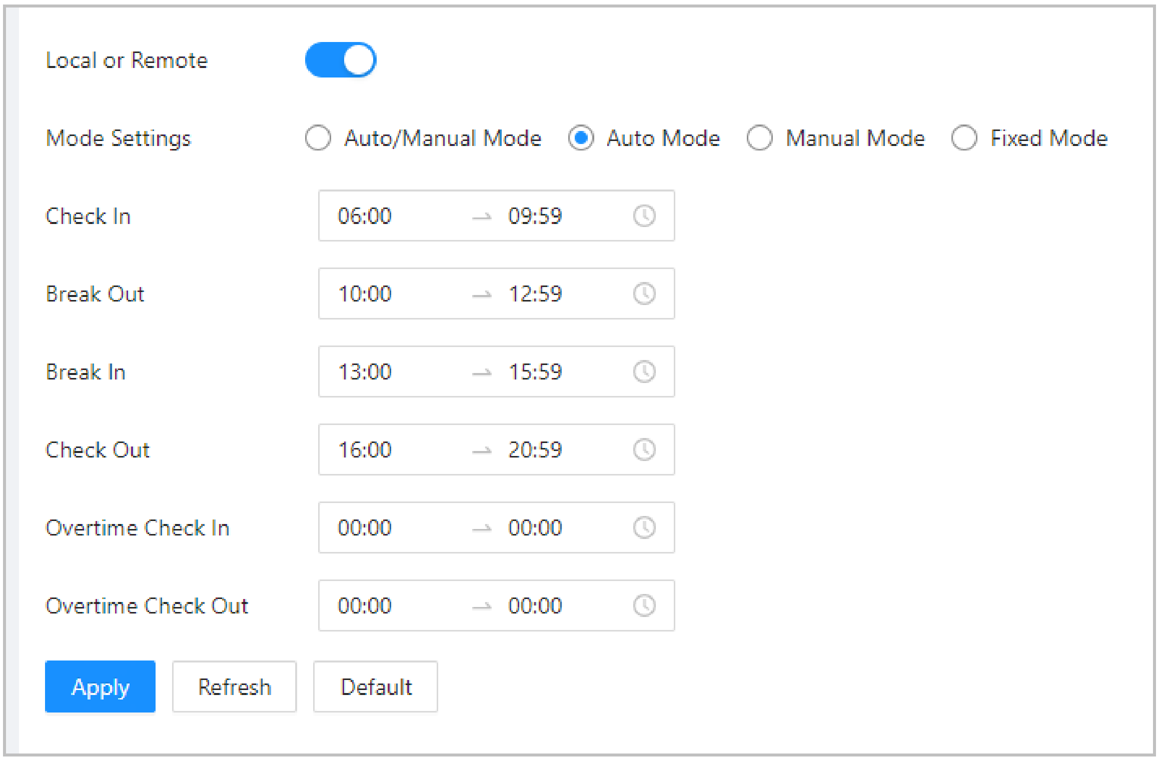
Step 2 Enter the verification interval.

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

Step 3 Enable **Local or Remote**, and then set the attendance mode.

Step 4 Configure attendance modes.

Figure 3-27 Attendance modes



Local or Remote

Mode Settings ○ Auto/Manual Mode ● Auto Mode ○ Manual Mode ○ Fixed Mode

Check In 06:00 → 09:59

Break Out 10:00 → 12:59

Break In 13:00 → 15:59

Check Out 16:00 → 20:59

Overtime Check In 00:00 → 00:00

Overtime Check Out 00:00 → 00:00

Table 3-13 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 starts. ● 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 starts. ● 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 per-defined attendance status all the time.

Step 5 Click **Apply**.

Related Operations

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

3.7 Configuring Audio and Video

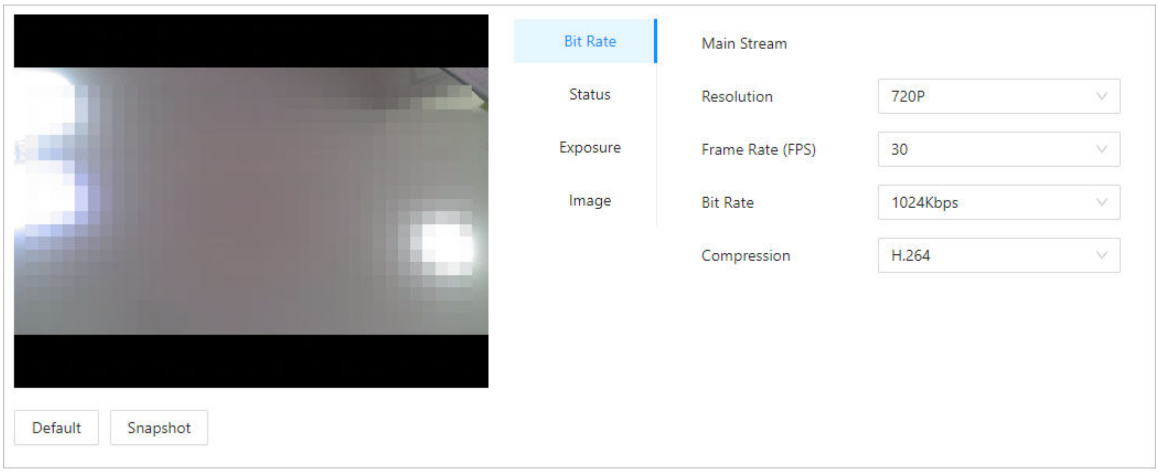
3.7.1 Configuring Video

Log in to the webpage, select **Audio and Video Config** > **Video**

- Default: Restore to defaults settings.
- Capture: Take a snapshot of the current image.

Bit Rate

Figure 3-28 Bit rate



Main Stream

Resolution: 720P

Frame Rate (FPS): 30

Bit Rate: 1024Kbps

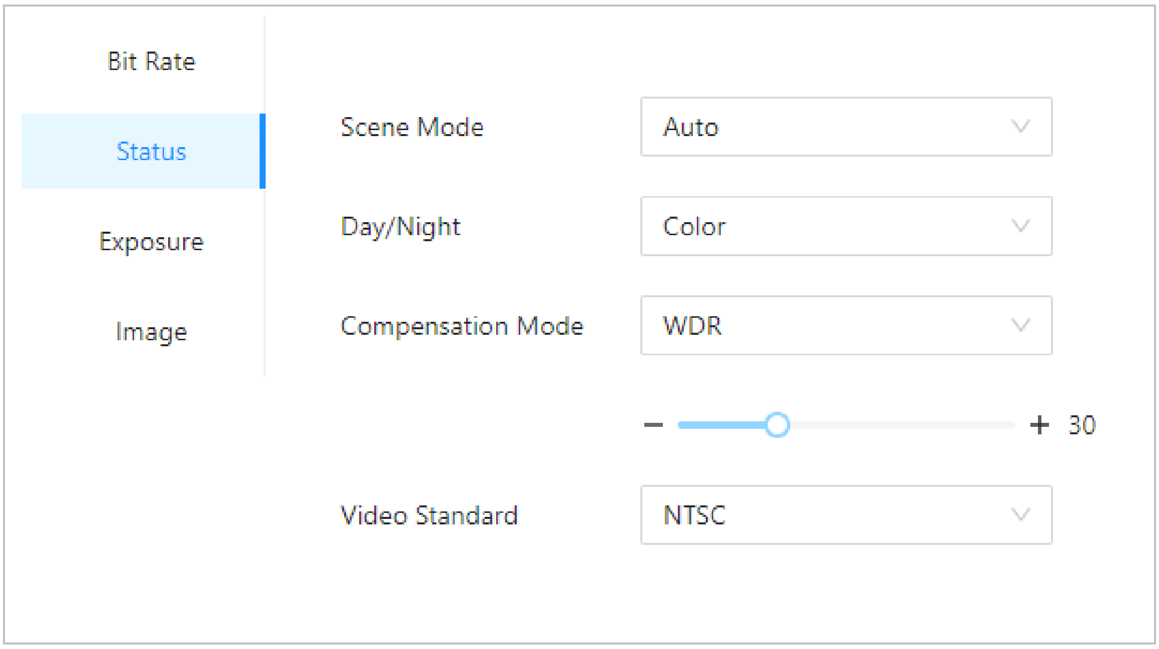
Compression: H.264

Table 3-14 Description of bit rate parameters

Parameter	Description
Resolution	📖 When the Device functions as the a VTO and connects the VTH, the acquired stream limit of VTH is 720p.When resolution is changed to 1080p, the call and monitor function might be affected.
Frame Rate (FPS)	The number of frames (or images) per second.
Bit Rate	The amount of data transmitted over an internet connection in a given amount of time. Select a proper bandwidth based on your network speed.
Compression	Video compression standard to deliver good video quality at lower bit rates.

Status

Figure 3-29 Status



Scene Mode: Auto

Day/Night: Color

Compensation Mode: WDR

30

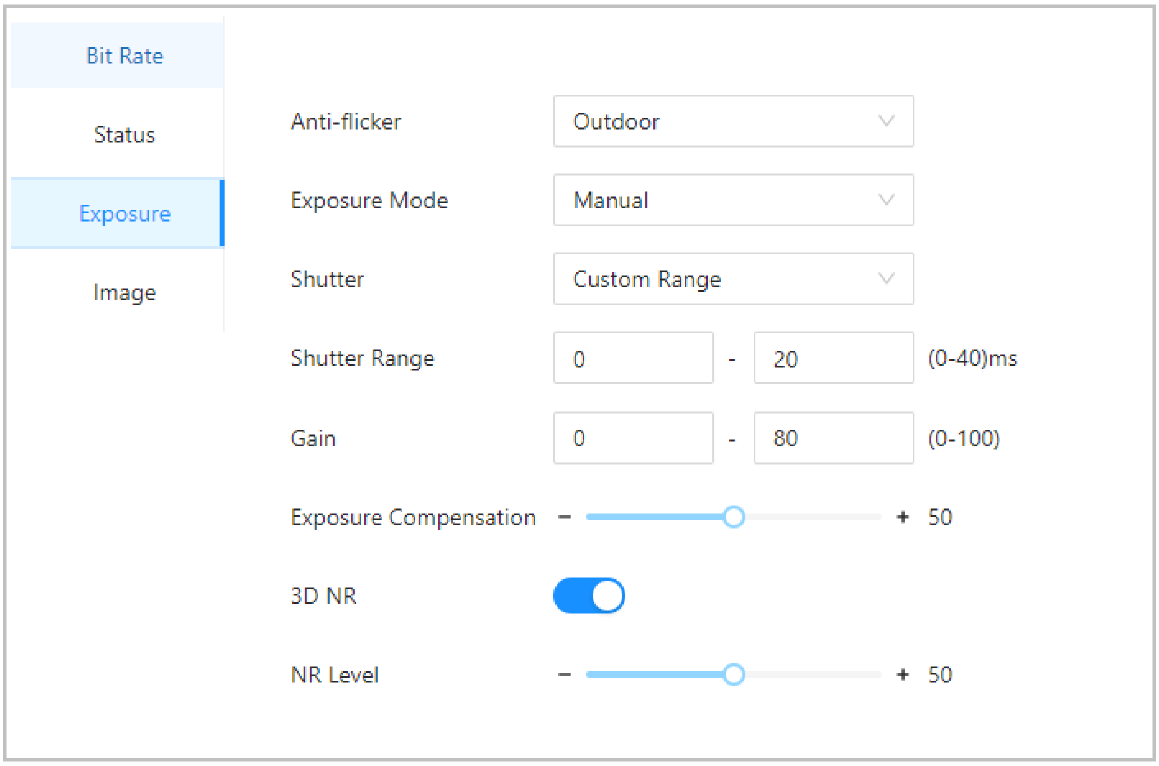
Video Standard: NTSC

Table 3-15 Parameters description of status

Parameter	Description
Scene Mode	The image hue is different in different scene mode. ● **Close** : Scene mode function is turned off. ● **Auto** : The system automatically adjusts the scene mode based on the photographic sensitivity. ● **Sunny** : In this mode, image hue will be reduced. ● **Night** : In this mode, image hue will be increased.
Day/Night	Day/Night mode affects light compensation in different situations. ● **Auto** : The system automatically adjusts the day/night mode based on the photographic sensitivity. ● **Colorful** : In this mode, images are colorful. ● **Black and white** : In this mode, images are in black and white.
Compensation Mode	● **Disable** : Compensation is turned off. ● **BLC** : Backlight compensation automatically brings more light to darker areas of an image when bright light shining from behind obscures it. ● **WDR** : The system dims bright areas and compensates for dark areas to create a balance to improve the overall image quality. ● **HLC** : Highlight compensation (HLC) is a technology used in CCTV/IP security cameras to deal with images that are exposed to lights like headlights or spotlights. The image sensor of the camera detects strong lights in the video and reduces exposure in these spots to enhance the overall quality of the image.
Video Standard	Select from **PAL** and **NTSC**.

Exposure

Figure 3-30 Exposure



Anti-flicker: Outdoor

Exposure Mode: Manual

Shutter: Custom Range

Shutter Range: 0 - 20 (0-40)ms

Gain: 0 - 80 (0-100)

Exposure Compensation: 50

3D NR: ●

NR Level: 50

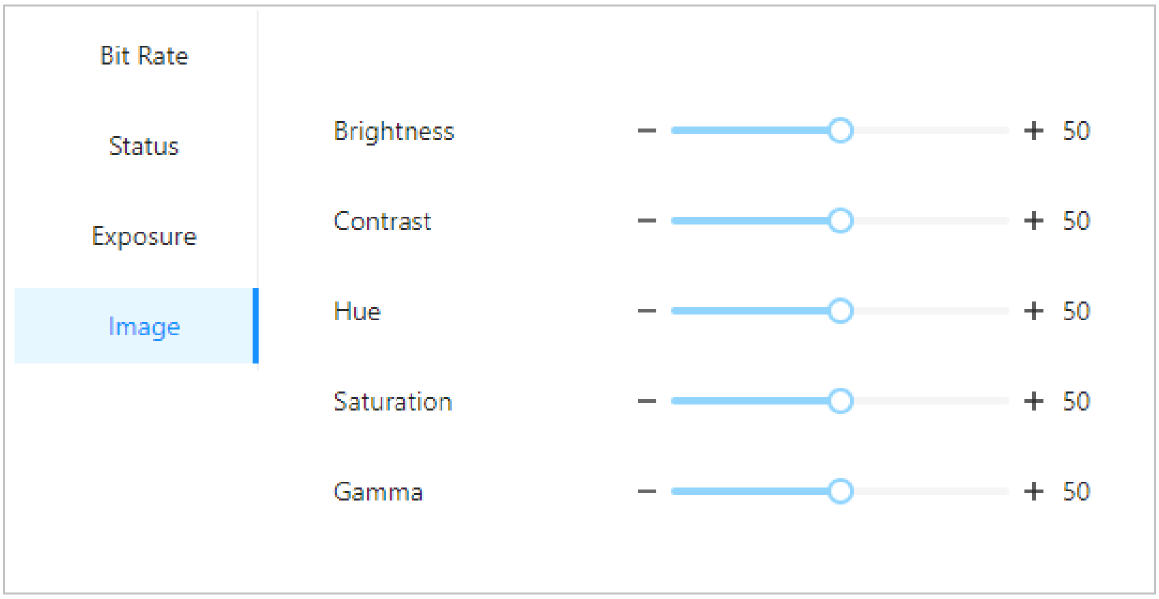
Table 3-16 Exposure parameter description

Parameter	Description
Anti-flicker	Set anti-flicker to reduce flicker and decrease or reduce uneven colors or exposure. ● **50Hz** : When the mains electricity is 50 Hz, the exposure is automatically adjusted based on brightness of the surroundings to prevent the appearance of horizontal lines. ● **60Hz** : When the mains electricity is 60 Hz, the exposure is automatically adjusted based on brightness of the surroundings to reduce the appearance of horizontal lines. ● **Outdoor** : When **Outdoor** is selected, the exposure mode can be switched.

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

Image

Figure 3-31 Image



Brightness 50

Contrast 50

Hue 50

Saturation 50

Gamma 50

Table 3-17 Image description

Parameter	Description
Brightness	The brightness of the image. Higher value means brighter images.
Contrast	Contrast is the difference in the luminance or color that makes an object distinguishable. The larger the contrast value is, the greater the color contrast will be.
Hue	Refers to the strength or saturation of a color. It describes the color intensity, or how pure it is.
Saturation	Color saturation indicates the intensity of color in an image. As the saturation increases, the appear stronger, for example being more red or more blue. 📖 The saturation value does not change image brightness.
Gamma	Change the image brightness and contrast in a non-linear way. The higher the value, the brighter the image.

3.7.2 Configuring Audio

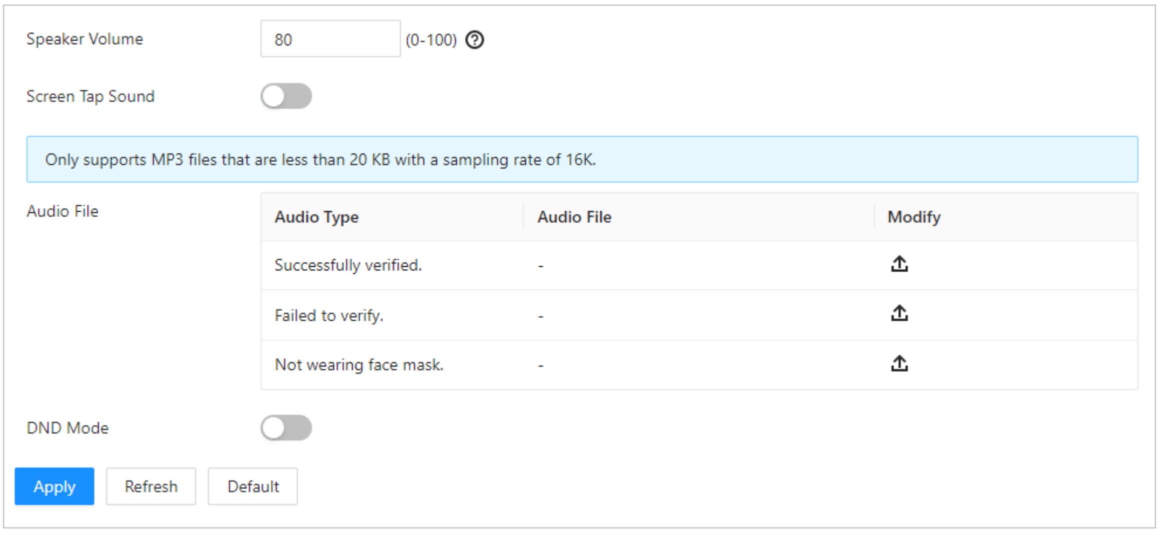
Set the speaker volume and audio prompts during identity verification.

Procedure

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

Step 2 Configure the audio parameters.

Figure 3-32 Configure audio parameters



Speaker Volume: 80 (0-100)

Screen Tap Sound: off

Only supports MP3 files that are less than 20 KB with a sampling rate of 16K.

Audio File

Audio Type	Audio File	Modify
Successfully verified.	-	⇧
Failed to verify.	-	⇧
Not wearing face mask.	-	⇧

DND Mode: off

Table 3-18 Parameters description

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

Parameters	Description
Audio File	Click Upload audio files to the platform.
DND Mode	No voice prompts during the set time when you verify your identity on the Device. You can set up to 4 periods.

Step 3 Click ⇧ to upload audio files to platform for each audio type.

Only supports MP3 files that are less than 20 KB with a sampling rate of 16K.

Step 4 Click **Apply**.

3.8 Communication Settings

3.8.1 Network Settings

3.8.1.1 Configuring TCP/IP

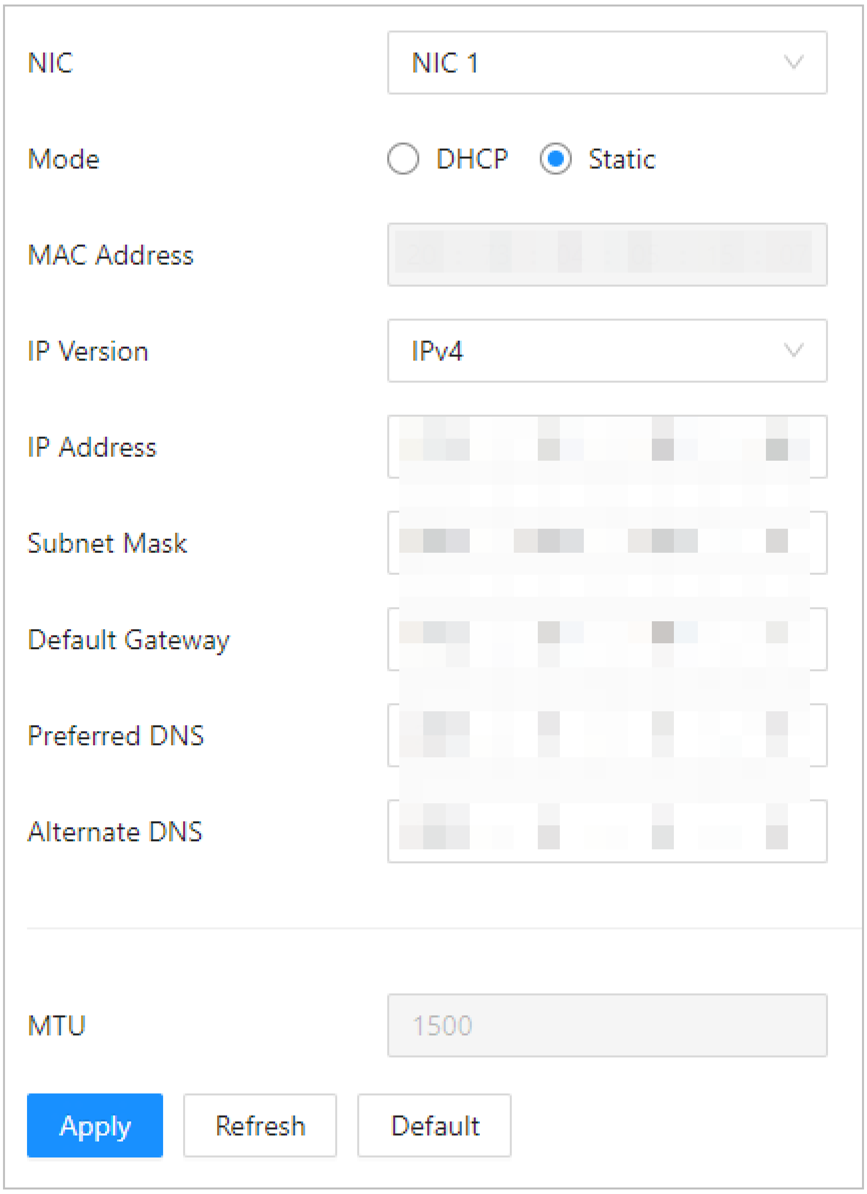
You need to configure IP address of Device to make sure that it can communicate with other devices.

Procedure

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

Step 2 Configure the parameters.

Figure 3-33 TCP/IP



NIC: NIC 1

Mode: ○ DHCP ● Static

MAC Address

IP Version: IPv4

IP Address

Subnet Mask

Default Gateway

Preferred DNS

Alternate DNS

MTU: 1500

Table 3-19 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.

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

Step 3 Click **OK**.

3.8.1.2 Configuring Wi-Fi

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

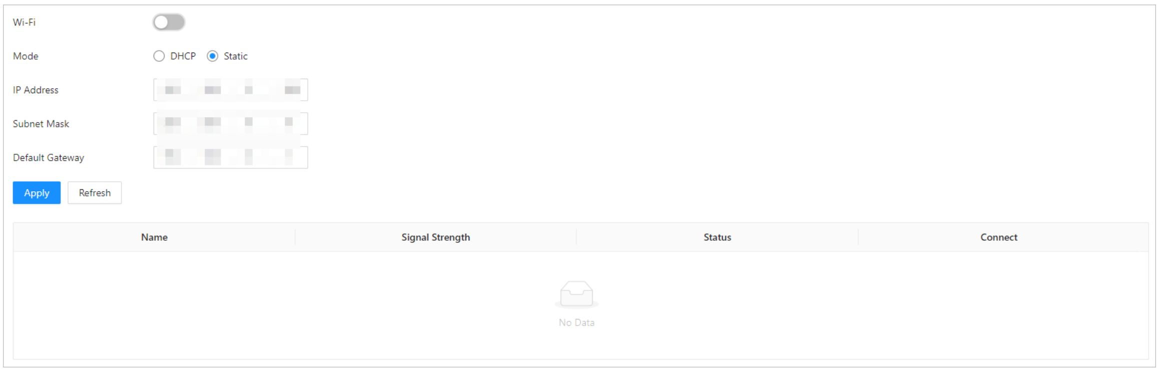
Procedure

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

Step 2 Turn on Wi-Fi.

All available Wi-Fi are displayed.

Figure 3-34 Wi-Fi



Wi-Fi ○

Mode ○ DHCP ● Static

IP Address [redacted]

Subnet Mask [redacted]

Default Gateway [redacted]

Name	Signal Strength	Status	Connect

No Data

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

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

The Wi-Fi is connected.

Related Operations

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

3.8.1.3 Configuring Wi-Fi AP

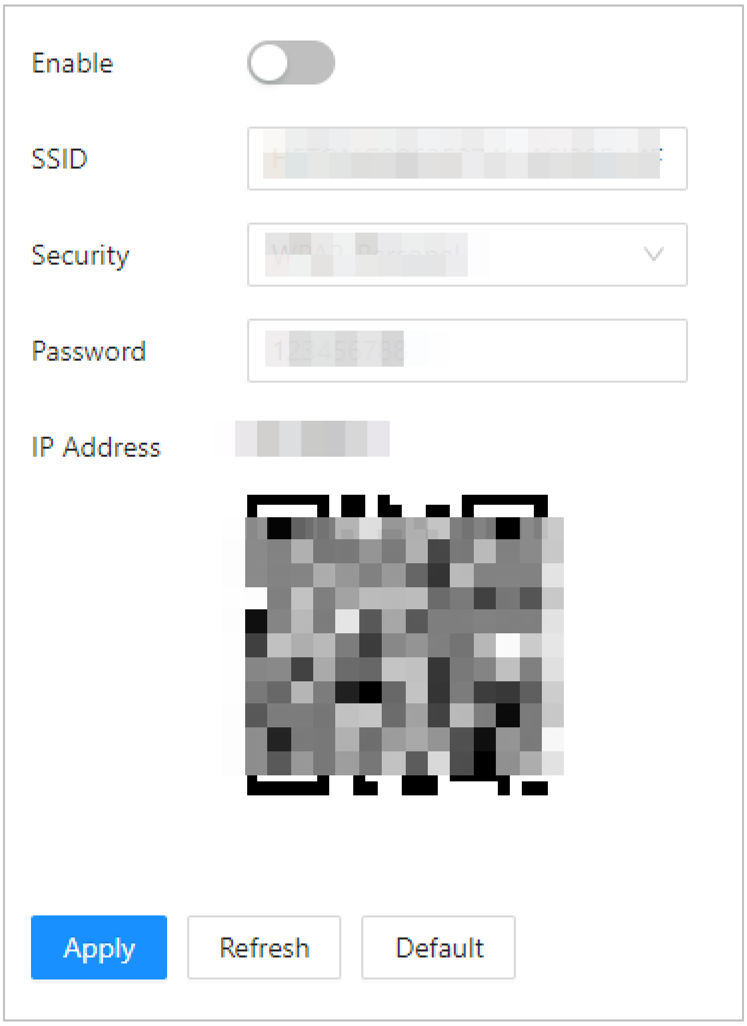
- The Wi-Fi function is available on select models.
- The Wi-Fi and Wi-Fi AP cannot be enabled at the same time.

Procedure

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

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

Figure 3-35 Wi-Fi AP



Enable

SSID

Security

Password

IP Address

Results

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

3.8.1.4 Configuring Port

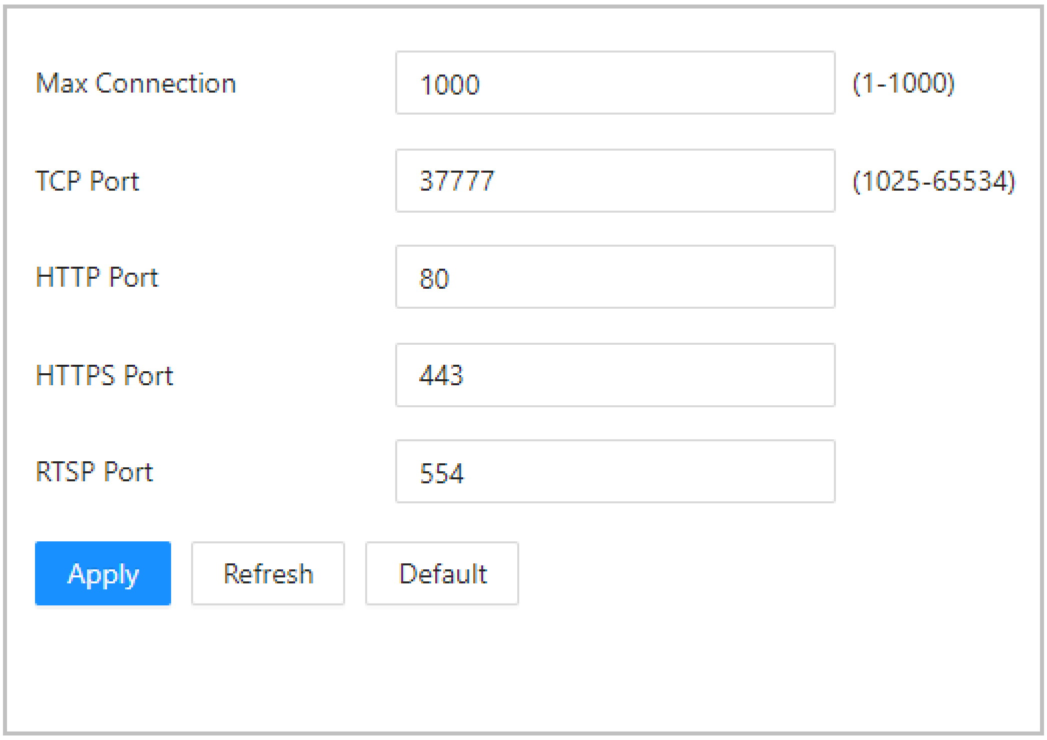
You can limit access to the Device at the same time through webpage, desktop client and mobile client.

Procedure

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

Step 2 Configure the ports.

Figure 3-36 Configure ports



Max Connection 1000 (1-1000)

TCP Port 37777 (1025-65534)

HTTP Port 80

HTTPS Port 443

RTSP Port 554

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

Table 3-20 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**.

3.8.1.5 Configuring Basic Service

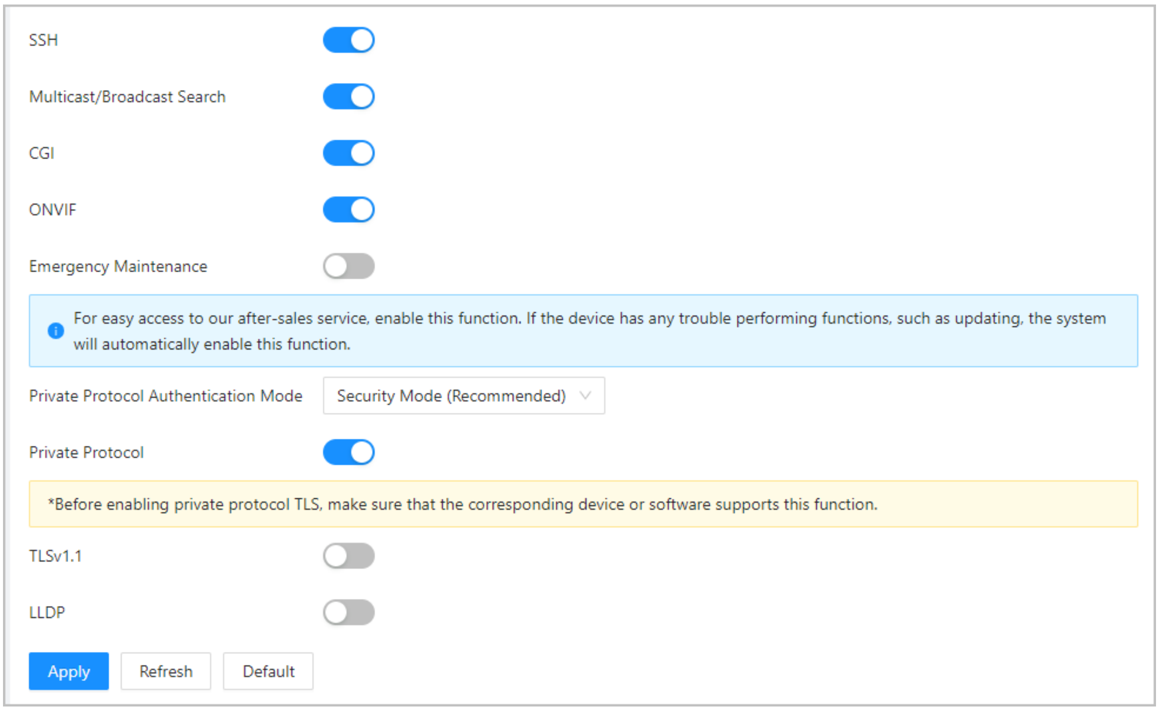
When you want to connect the Device to a third-party platform, turn on the CGI and ONVIF functions.

Procedure

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

Step 2 Configure the basic service.

Figure 3-37 Basic service


SSH ●
Multicast/Broadcast Search ●
CGI ●
ONVIF ●
Emergency Maintenance ○

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 ○

Table 3-21 Basic service parameter description

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

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

Step 3 Click **Apply**.

3.8.1.6 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.

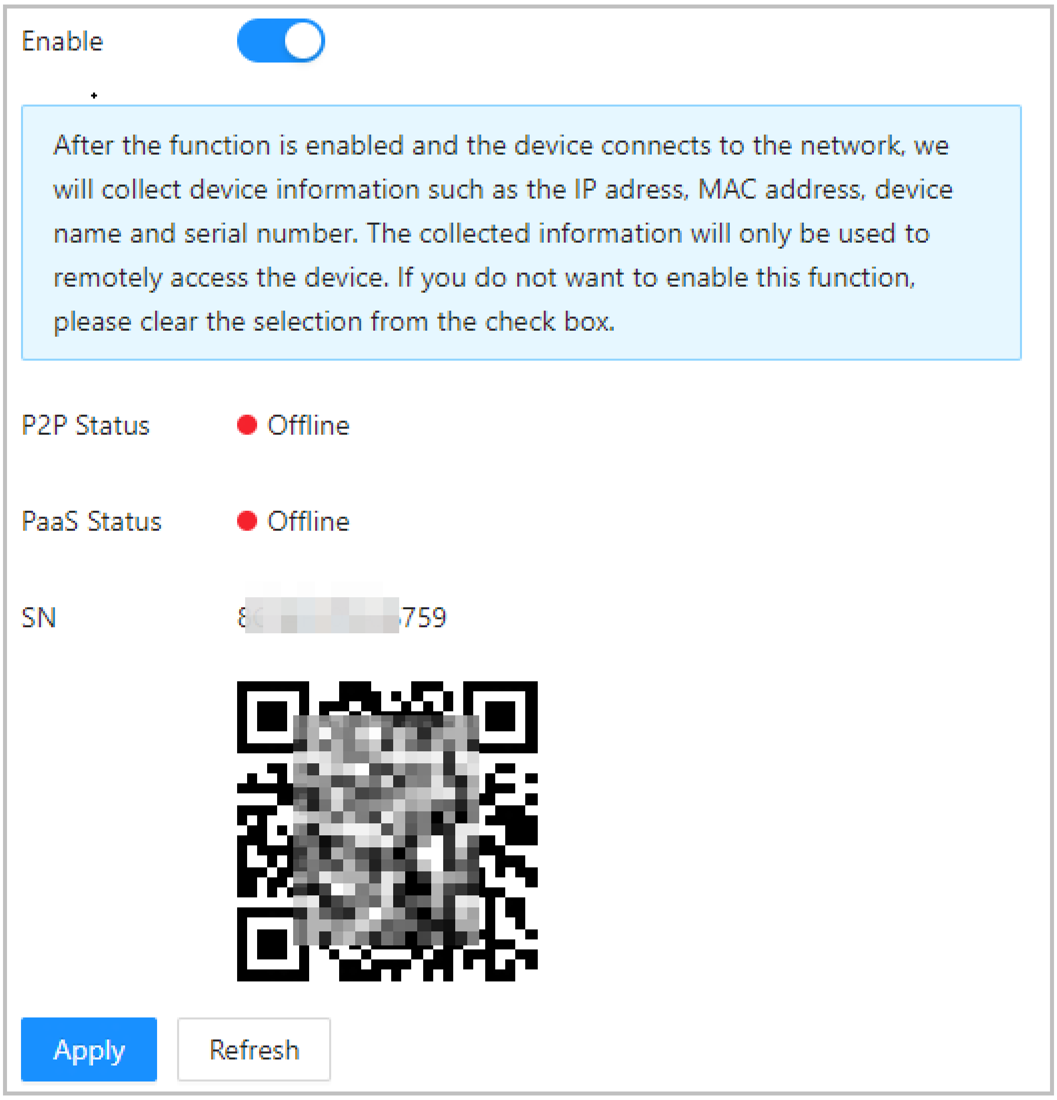
Procedure

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 3-38 Cloud service



Enable

After the function is enabled and the device connects to the network, we will collect device information such as the IP adress, 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

Step 3 Click **Apply**.

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

3.8.1.7 Configuring Auto Registration

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

Background Information

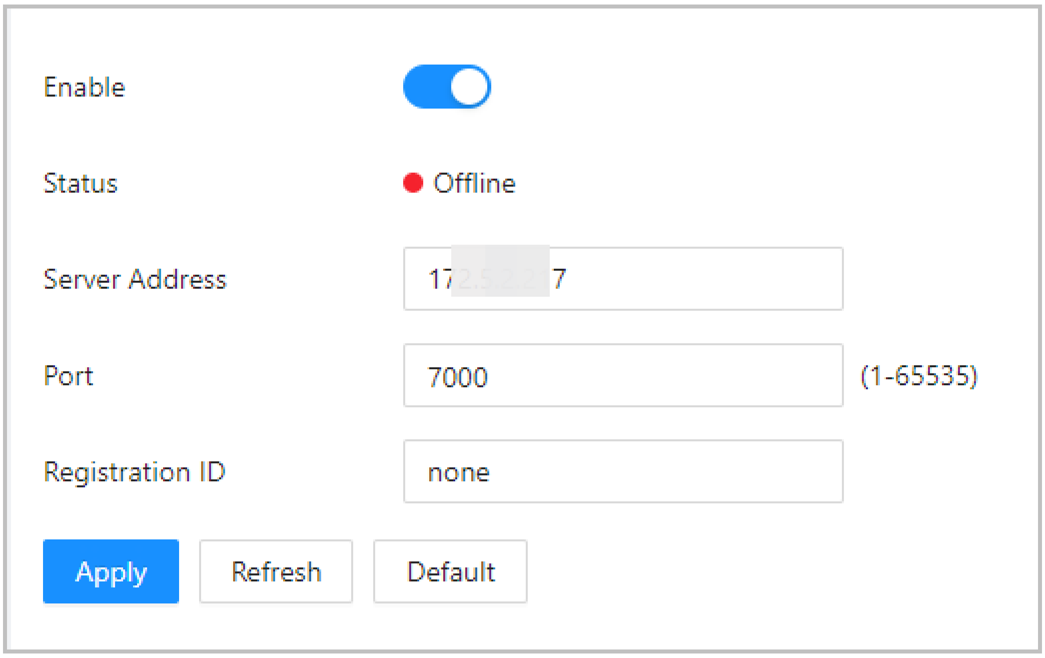
The auto registration only supports SDK.

Procedure

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

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

Figure 3-39 Auto Registration



Enable: on

Status: ● Offline

Server Address: 17[redacted]7

Port: 7000 (1-65535)

Registration ID: none

Table 3-22 Automatic registration description

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

Step 3 Click **Apply**.

3.8.1.8 Configuring CGI Auto Registration

Connect to a third-party platform through CGI protocol.

Background Information

Only supports IPv4.

Procedure

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

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

Table 3-23 Automatic registration description

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

Step 3 Click **OK**.

3.8.1.9 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**.

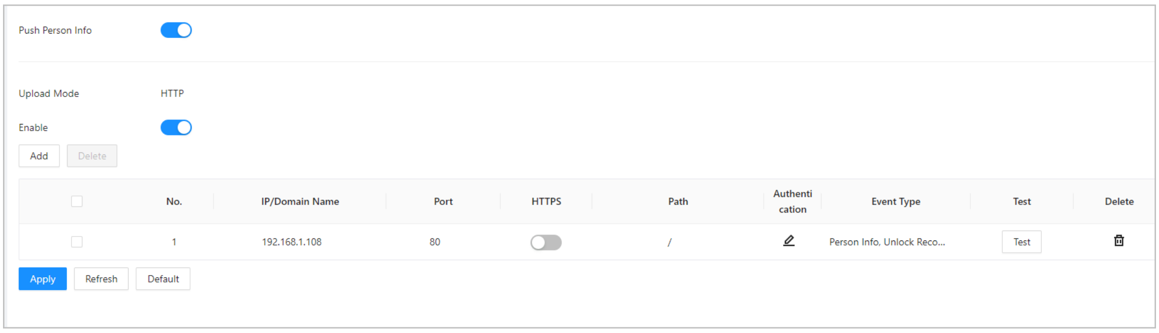
Step 2 (Optional) Enable **Push Person Info**.

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 3-40 Automatic upload



Push Person Info ●

Upload Mode HTTP

Enable ●

□	No.	IP/Domain Name	Port	HTTPS	Path	Authentication	Event Type	Test	Delete
□	1	192.168.1.108	80	○	/	✎	Person Info, Unlock Reco...	Test	🗑

Table 3-24 Parameters description

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

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

Step 5 Click **Apply**.

3.8.2 Configuring RS-485

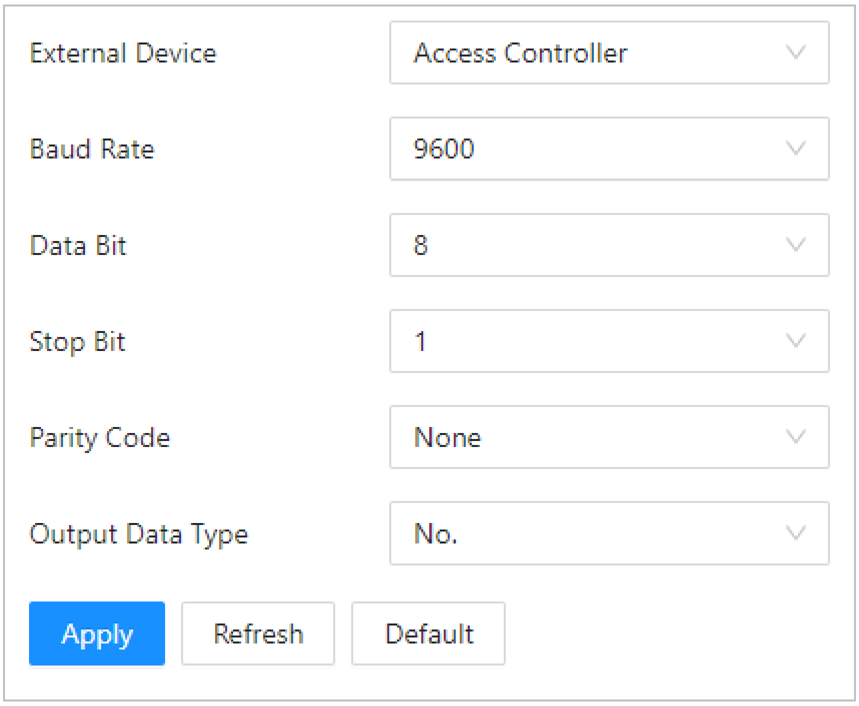
Configure the RS-485 parameters if you connect an external device to the RS-485 port.

Procedure

Step 1 Select **Communication Settings** > **RS-485 Settings**.

Step 2 Configure the parameters.

Figure 3-41 Configure parameters



External Device: Access Controller

Baud Rate: 9600

Data Bit: 8

Stop Bit: 1

Parity Code: None

Output Data Type: No.

Table 3-25 Description of RS-485 parameters

Parameter	Description
External Device	● Access Controller Select **Access Controller** when the Device functions as a card reader, and sends data to other external access controllers to control access. ● Card Reader: The Device functions as an access controller, and connects to an external card reader. ● Reader (OSDP): The Device is connected to a card reader based on OSDP protocol. ● Door Control Security: The door exit button, lock and fire linkage is not effective after the security module is enabled.
Baud Rate	Select the baud rate. It is 9600 by default.
Data Bit	The number of bits used to transmit the actual data in a serial communication. It represents the binary digits that carry the information being transmitted.
Stop Bit	A bit sent after the data and optional parity bits to indicate the end of a data transmission. It allows the receiver to prepare for the next byte of data and provides synchronization in the communication protocol.
Parity Code	An additional bit sent after the data bits to detect transmission errors. It helps verify the integrity of the transmitted data by ensuring a specific number of logical high or low bits.
Output Data Type	When you configure the external device as **Access Controller**. ● 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. ● No.: Outputs data based on the user ID.

Step 3 Click **Apply**.

3.8.3 Configuring Wiegand

Supports access Wiegand devices. Configure the mode and the transmission mode according to your actual devices.

Procedure

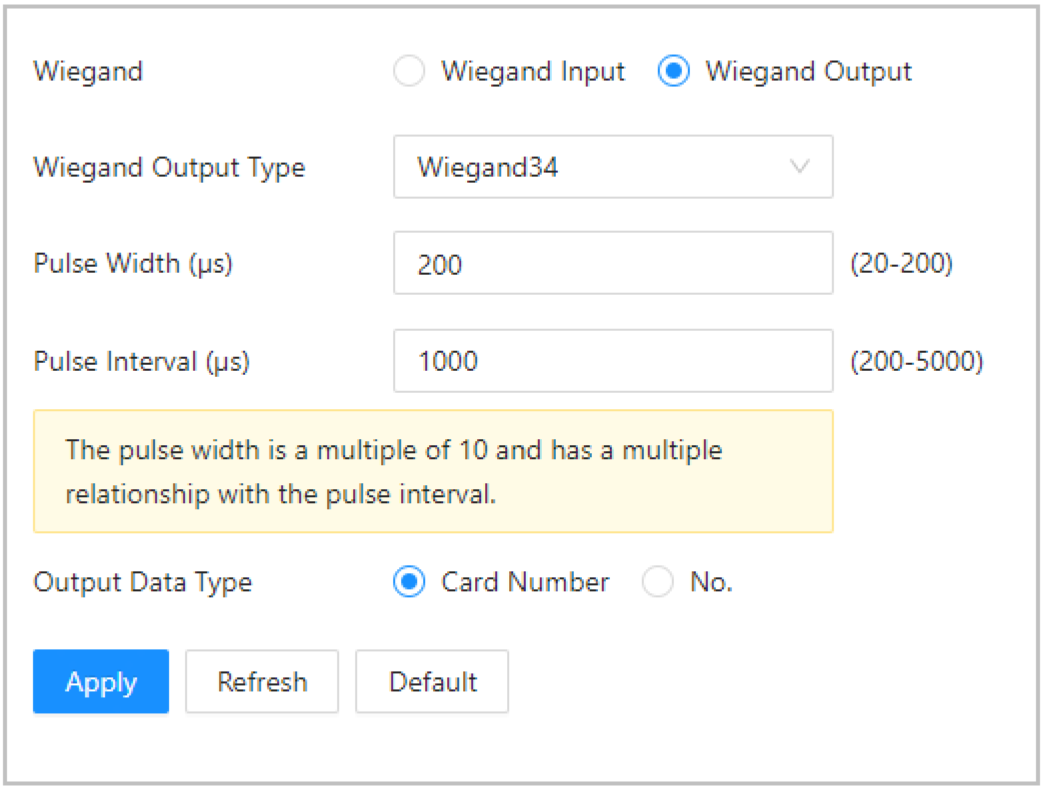
Step 1 Select **Communication Settings** > **Wiegand**.

Step 2 Select a Wiegand type, and then configure parameters.

- Select **Wiegand Input** when you connect an external card reader to the Device.

  When the Device connects to a third-party device through the Wiegand input port, and the card number read by the Device is in the reverse order from the actual card number. In this case, you can turn on **Card No. Inversion** function.
- Select **Wiegand Output** when the Device functions as a card reader, and you need to connect it to another access controller.

Figure 3-42 Wiegand output



Wiegand ○ Wiegand Input ● Wiegand Output

Wiegand Output Type: Wiegand34

Pulse Width (μs): 200 (20-200)

Pulse Interval (μs): 1000 (200-5000)

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

Output Data Type ● Card Number ○ No.

Table 3-26 Description of Wiegand output

Parameter	Description
Wiegand Output Type	Select a Wiegand format to read card numbers or ID numbers. ● **Wiegand26** : Reads 3 bytes or 6 digits. ● **Wiegand34** : Reads 4 bytes or 8 digits. ● **Wiegand66** : Reads 8 bytes or 16 digits.
Pulse Width	Enter the pulse width and pulse interval of Wiegand output.
Pulse Interval	
Output Data Type	Select the type of output data. ● **No.** : Outputs data based on user ID. The data format is hexadecimal or decimal. ● **Card Number** : Outputs data based on user's first card number.

Step 3 Click **Apply**.

3.9 Configuring the System

3.9.1 User Management

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

3.9.1.1 Adding Administrators

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

Procedure

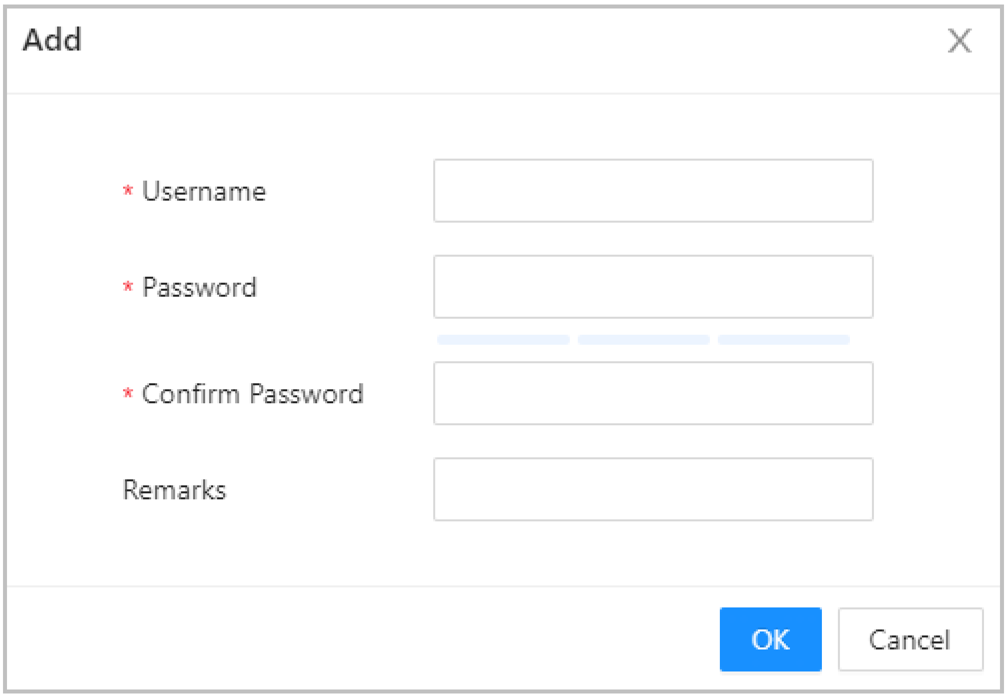
Step 1 On the home page, select **System** > **Account**.

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 3-43 Add administrators



Add

* Username

* Password

* Confirm Password

Remarks

Step 3 Click **OK**.

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

3.9.1.2 Adding ONVIF Users

Background Information

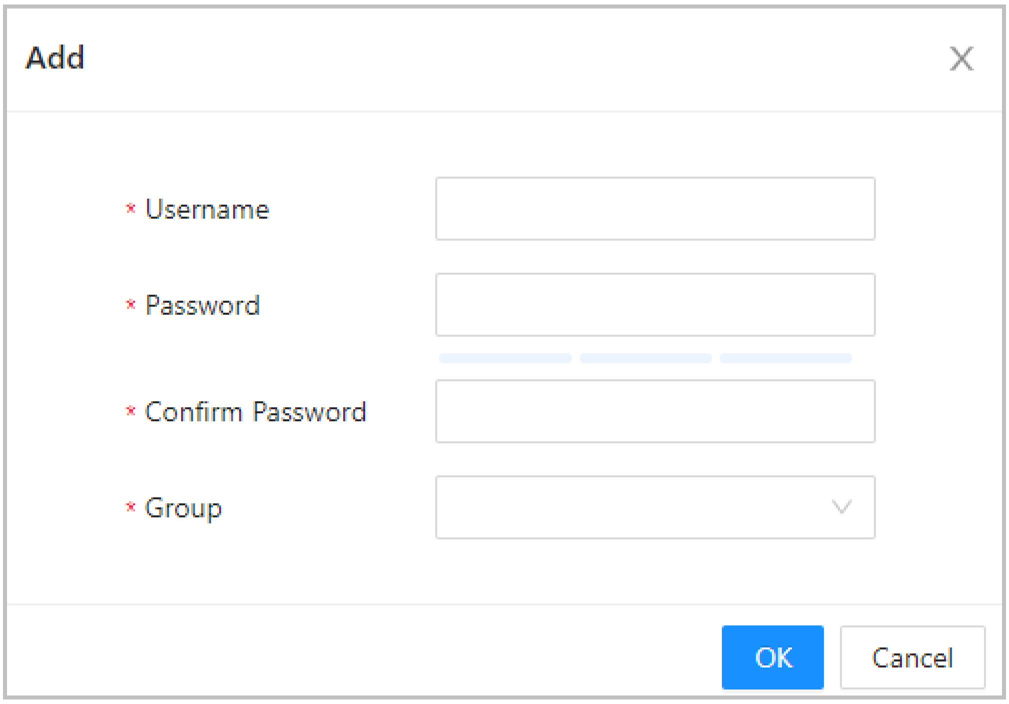
Open Network Video Interface Forum (ONVIF), a global and open industry forum that is established for the development of a global open standard for the interface of physical IP-based security products, which allows the compatibility from different manufactures. ONVIF users have their identities verified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

Procedure

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

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

Figure 3-44 Add ONVIF user



Add

* Username

* Password

* Confirm Password

* Group

Table 3-27 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 ' " ; : &).

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

Step 3 Click **OK**.

3.9.1.3 Resetting the Password

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

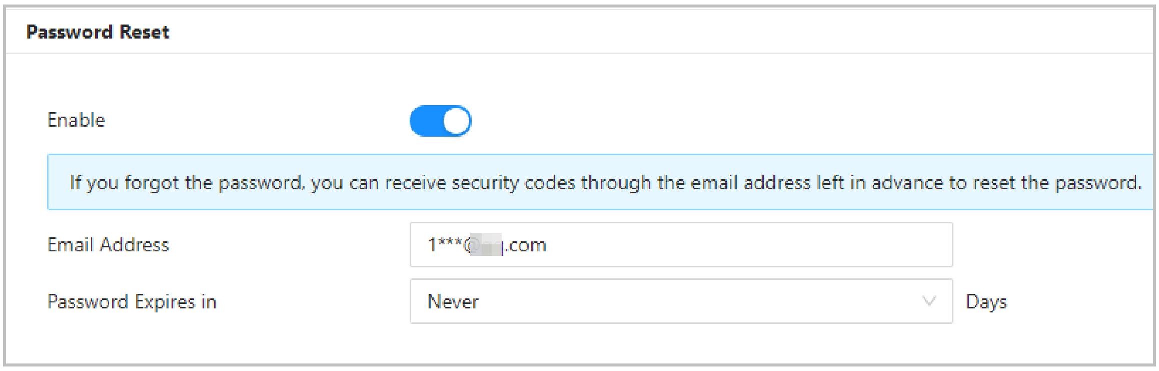
Procedure

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 3-45 Reset Password



Password Reset

Enable: ON

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

Email Address: 1***@[redacted].com

Password Expires in: Never Days

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

Step 4 Click **Apply**.

3.9.1.4 Viewing Online Users

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

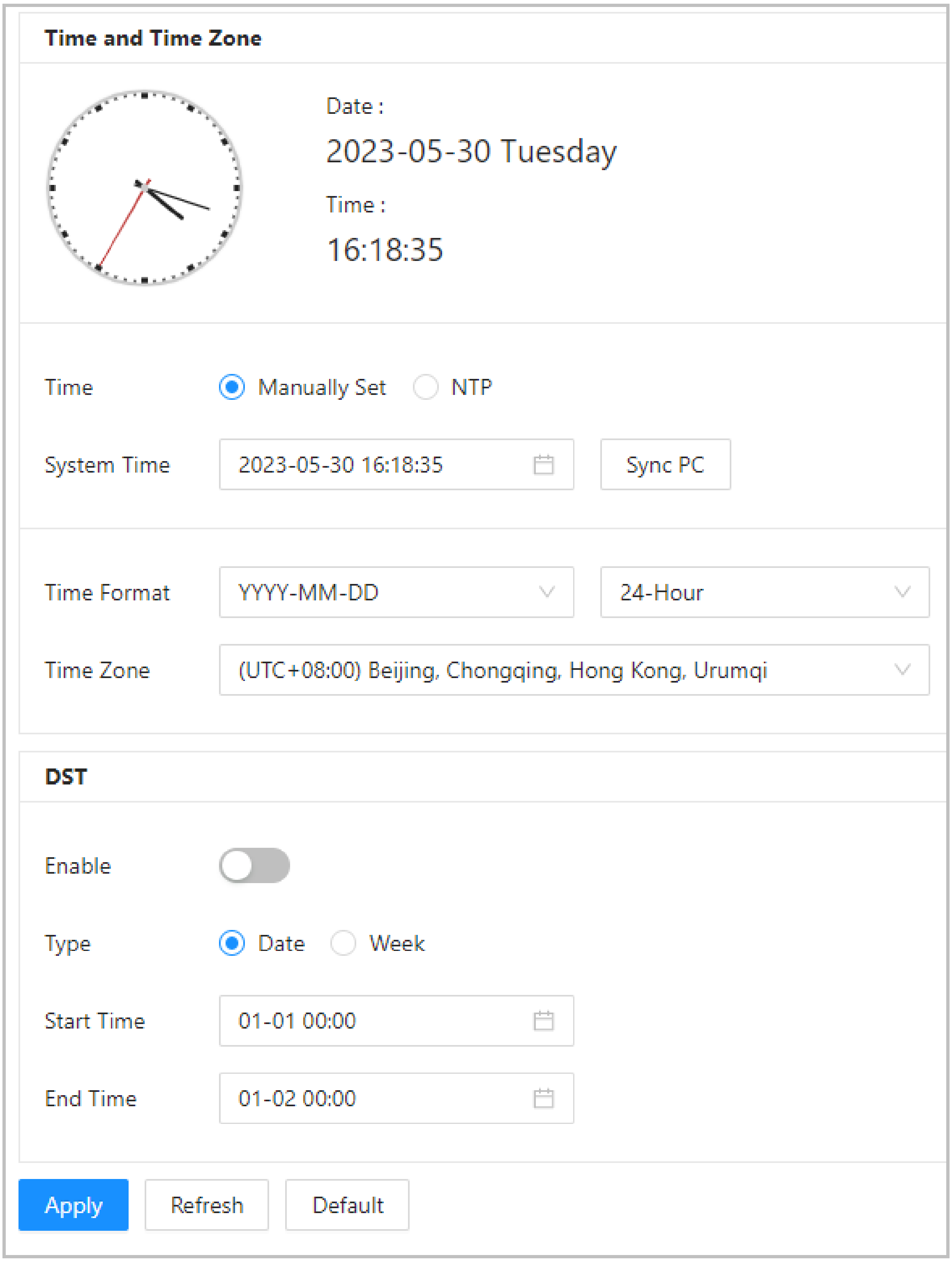
3.9.2 Configuring Time

Procedure

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

Step 2 Configure the time of the Platform.

Figure 3-46 Date settings



Time and Time Zone

Date : 2023-05-30 Tuesday

Time : 16:18:35

Time ● Manually Set ○ NTP

System Time 2023-05-30 16:18:35

Time Format YYYY-MM-DD 24-Hour

Time Zone (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi

DST

Enable

Type ● Date ○ Week

Start Time 01-01 00:00

End Time 01-02 00:00

Table 3-28 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.
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**.

3.10 Maintenance Center

3.10.1 One-click Diagnosis

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

Procedure

Step 1 On the home page, select **Maintenance Center** > **One-click Diagnosis**.

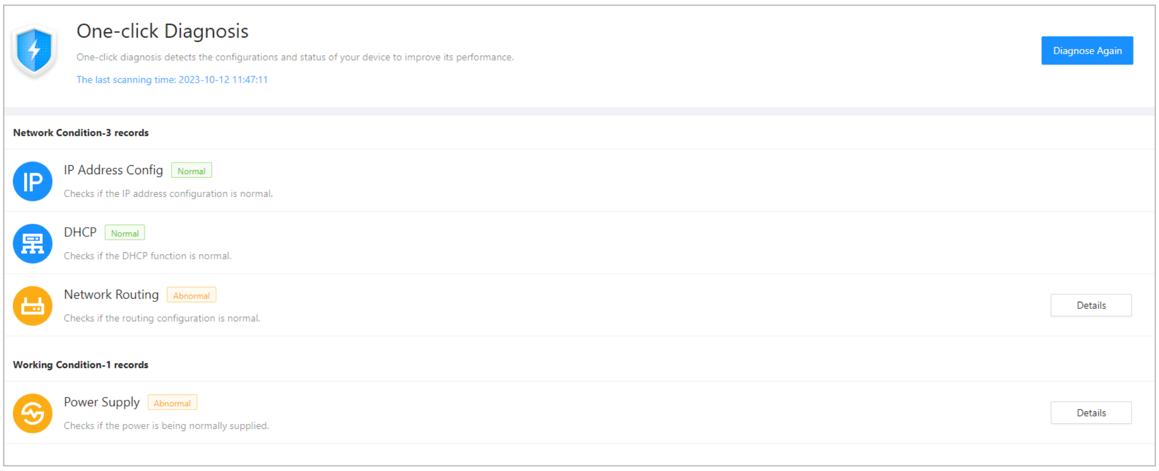
Step 2 Click **Diagnose**.

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

Step 3 (Optional) Click **Details** to view details of abnormal items.

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

Figure 3-47 One-click diagnosis



One-click Diagnosis

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

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

Network Condition-3 records

IP Address Config Normal

Checks if the IP address configuration is normal.

DHCP Normal

Checks if the DHCP function is normal.

Network Routing Abnormal

Checks if the routing configuration is normal.

Working Condition-1 records

Power Supply Abnormal

Checks if the power is being normally supplied.

3.10.2 System Information

3.10.2.1 Viewing Version Information

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

3.10.2.2 Viewing Legal Information

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

3.10.3 Data Capacity

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

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

3.10.4 Viewing Logs

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

3.10.4.1 System Logs

View and search for system logs.

Procedure

Step 1 Log in to the webpage.

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

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

Related Operations

- click **Export** to export the searched logs to your local computer.

- Click **Encrypt Log Backup**, and then enter a password. The exported file can be opened only after entering the password.
- Click 🕮 to view details of a log.

3.10.4.2 Unlock Records

Search for unlock records and export them.

Procedure

Step 1 Log in to the webpage.

Step 2 Select **Maintenance Center** > **Log** > **Unlock Records**.

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

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

3.10.4.3 Alarm Logs

View alarm logs.

Procedure

Step 1 Log in to the webpage.

Step 2 Select **Maintenance Center** > **Log** > **Alarm Logs**.

Step 3 Select the type and the time range.

Step 4 Enter the admin ID, and then click **Search**.

3.10.4.4 Admin Logs

Search for admin logs by using admin ID.

Procedure

Step 1 Log in to the webpage.

Step 2 Select **Maintenance Center** > **Log** > **Admin Logs**.

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

Click **Export** to export admin logs.

3.10.4.5 USB Management

Export user information from/to USB.

Procedure

Step 1 Log in to the webpage.

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

🕮

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

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

3.10.5 Maintenance Management

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

3.10.5.1 Exporting and Importing Configuration Files

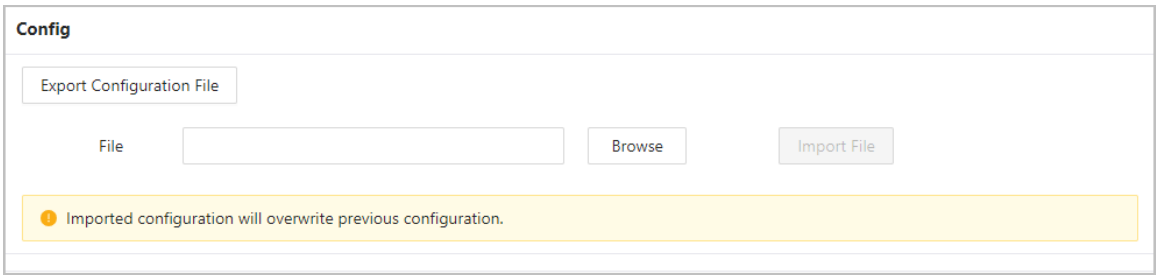
You can import and export the configuration file for the Device. When you want to apply the same configurations to multiple devices, you can import the configuration file to them.

Procedure

Step 1 Log in to the webpage.

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

Figure 3-48 Configuration management



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.

3.10.5.2 Configuring the Fingerprint Similarity Threshold

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

Procedure

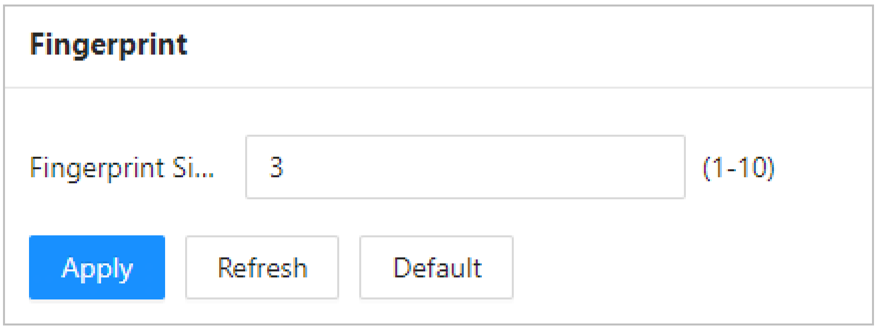
Step 1 Log in to the webpage.

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

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

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

Figure 3-49 Fingerprint similarity threshold



Fingerprint

Fingerprint Si... 3 (1-10)

3.10.5.3 Restoring the Factory Default Settings

Procedure

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

⚠

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

Step 2 Restore to the factory default settings if necessary.

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

3.10.6 Maintenance

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

Procedure

Step 1 Log in to the webpage.

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

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

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

3.10.7 Updating the System

⚠

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

3.10.7.1 File Update

Procedure

Step 1 On the home page, select **Maintenance Center** > **Update**.

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

The update file should be a .bin file.

Step 3 Click **Update**.

The Device will restart after the update finishes.

3.10.7.2 Online Update

Procedure

Step 1 On the home page, select **Maintenance Center** > **Update**.

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

- Select **Auto Check for Updates**, and the Device will automatically check for the latest version update.
- Select **Manual Check**, and you can immediately check whether the latest version is available.

Step 3 (Optional) Click **Update Now** to update the Device immediately.

3.10.8 Advanced Maintenance

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

3.10.8.1 Exporting

Procedure

Step 1 On the home page, select **Maintenance Center** > **Advanced Maintenance** > **Export**.

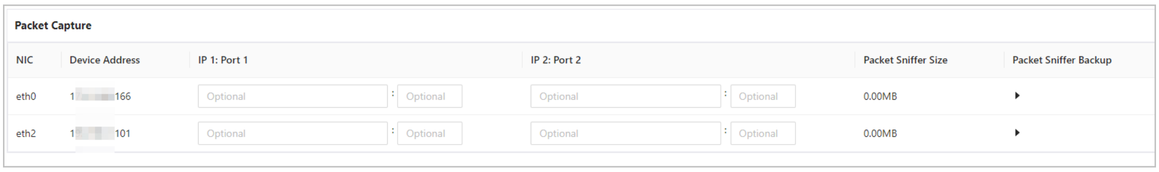
Step 2 Click **Export** to export the serial number, firmware version, device operation logs and configuration information.

3.10.8.2 Packet Capture

Procedure

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

Figure 3-50 Packet Capture



Packet Capture

NIC	Device Address	IP 1: Port 1		IP 2: Port 2		Packet Sniffer Size	Packet Sniffer Backup
eth0	1[redacted]166	Optional	Optional	Optional	Optional	0.00MB	▶
eth2	1[redacted]101	Optional	Optional	Optional	Optional	0.00MB	▶

Step 2 Enter the IP address, click ▶.

▶ changes to ⏸.

Step 3 After you acquired enough data, click ⏸.

Captured packets are automatically downloaded to your local computer.

3.11 Security Settings(Optional)

3.11.1 Security Status

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

Background Information

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

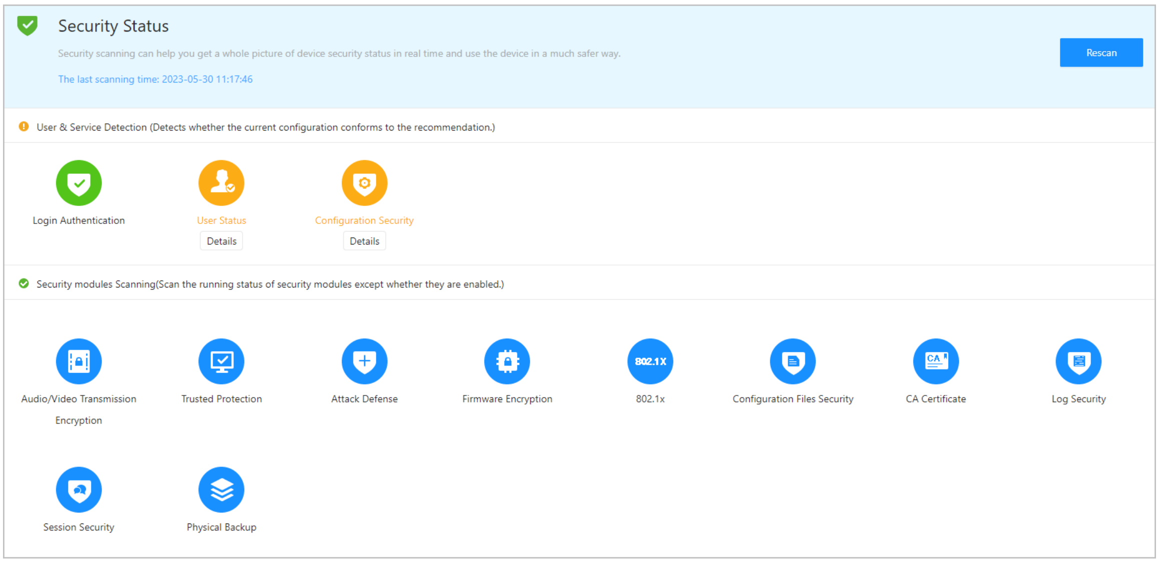
Procedure

Step 1 Select 🛡 > **Security Status**.

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

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

Figure 3-51 Security Status



Security Status

Security scanning can help you get a whole picture of device security status in real time and use the device in a much safer way.

The last scanning time: 2023-05-30 11:17:46

Rescan

User & Service Detection (Detects whether the current configuration conforms to the recommendation.)

Login Authentication

User Status Details

Configuration Security Details

Security modules Scanning(Scan the running status of security modules except whether they are enabled.)

Audio/Video Transmission Encryption

Trusted Protection

Attack Defense

Firmware Encryption

802.1x

Configuration Files Security

CA Certificate

Log Security

Session Security

Physical Backup

Related Operations

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

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

3.11.2 Configuring System Service

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

Procedure

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

Step 2 Turn on the HTTPS service.

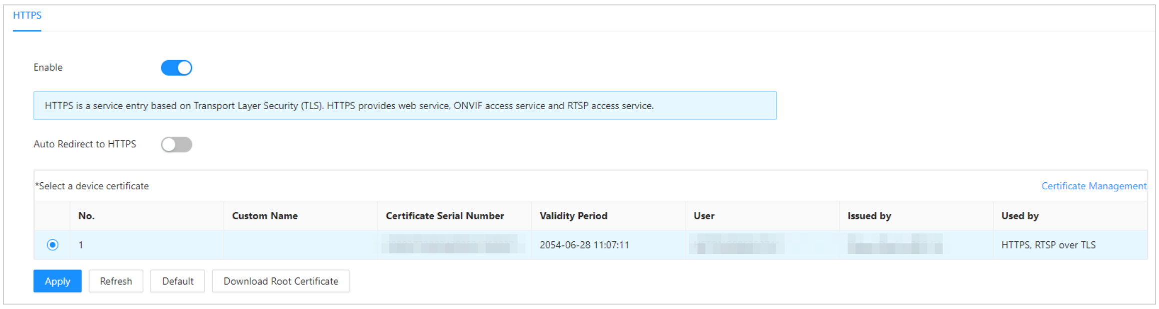
⚠

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

Step 3 Select the certificate.

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

Figure 3-52 System service



HTTPS

Enable ●

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

Auto Redirect to HTTPS ○

*Select a device certificate

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

Step 4 Click **Apply**.

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

3.11.3 Attack Defense

3.11.3.1 Configuring Firewall

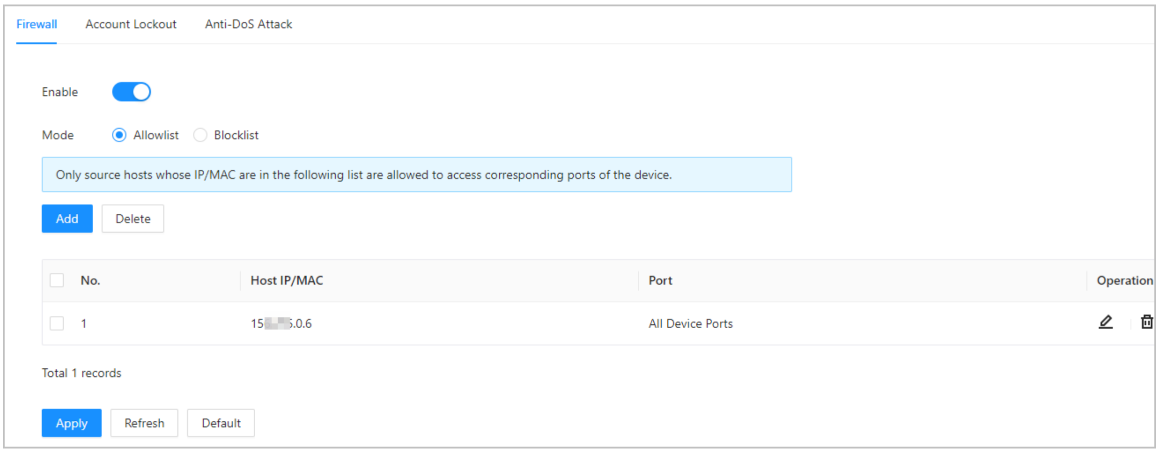
Configure firewall to limit access to the Device.

Procedure

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

Step 2 Click ○ to enable the firewall function.

Figure 3-53 Firewall



Firewall | Account Lockout | Anti-DoS Attack

Enable: on

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[redacted]5.0.6	All Device Ports	✎ 🗑

Total 1 records

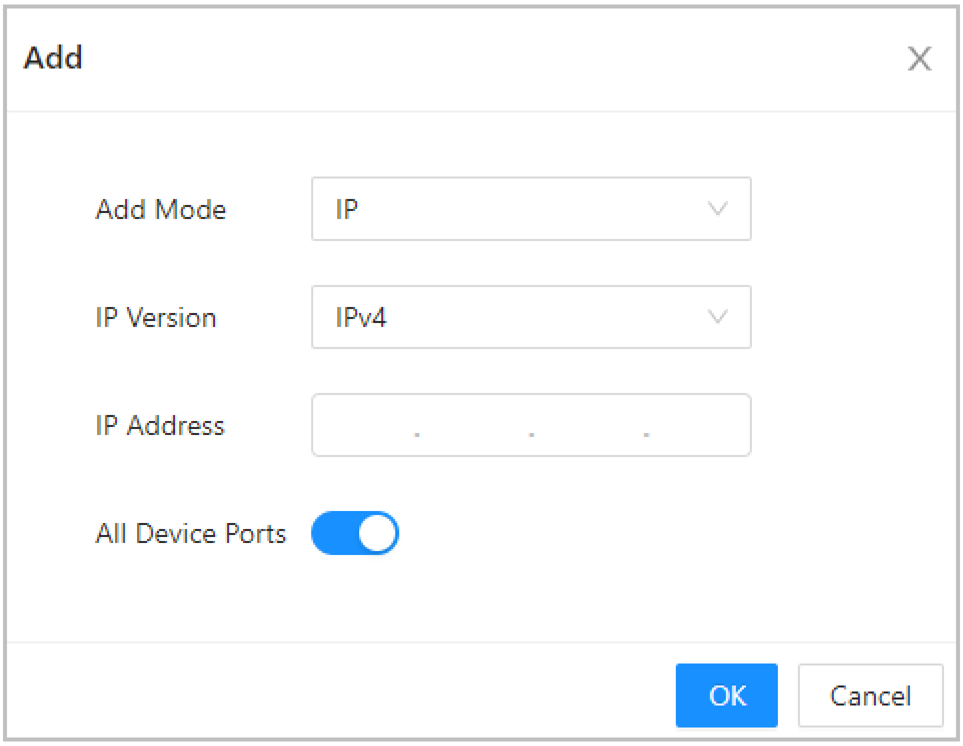
Apply | Refresh | Default

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

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

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

Figure 3-54 Add IP information



Add

Add Mode: IP

IP Version: IPv4

IP Address: . . .

All Device Ports: on

OK | Cancel

Step 5 Click **OK**.

Related Operations

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

3.11.3.2 Configuring Account Lockout

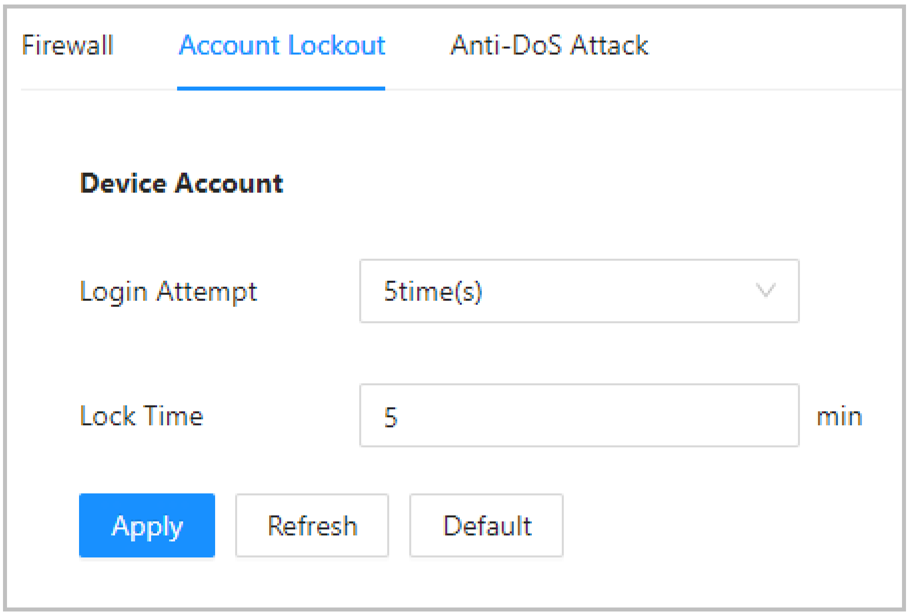
If the incorrect password is entered for a defined number of times, the account will be locked.

Procedure

Step 1 Select 🛡 > **Attack Defense** > **Account Lockout**.

Step 2 Enter the number of login attempts and the time the administrator account and ONVIF user will be locked for.

Figure 3-55 Account lockout



Device Account

Login Attempt: 5time(s)

Lock Time: 5 min

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

Step 3 Click **Apply**.

3.11.3.3 Configuring Anti-DoS Attack

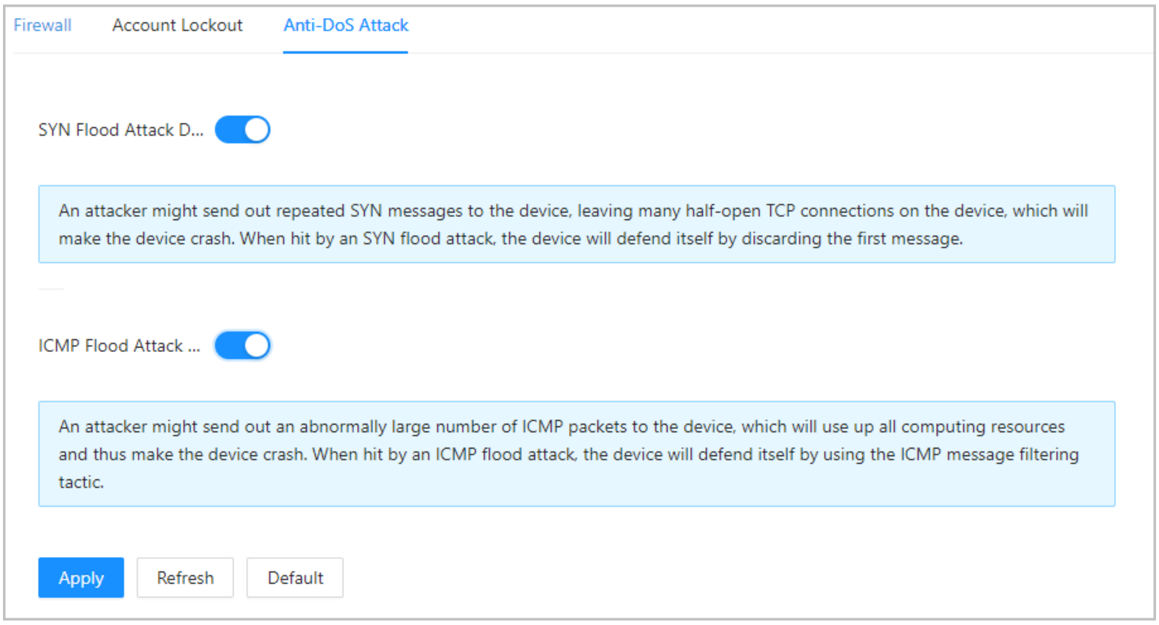
You can enable **SYN Flood Attack Defense** and **ICMP Flood Attack Defense** to defend the Device against Dos attacks.

Procedure

Step 1 Select 🛡 > **Attack Defense** > **Anti-DoS Attack**.

Step 2 Turn on **SYN Flood Attack Defense** or **ICMP Flood Attack Defense** to protect the Device against Dos attack.

Figure 3-56 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.

Step 3 Click **Apply**.

3.11.4 Installing Device Certificate

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

3.11.4.1 Creating Certificate

Create a certificate for the Device.

Procedure

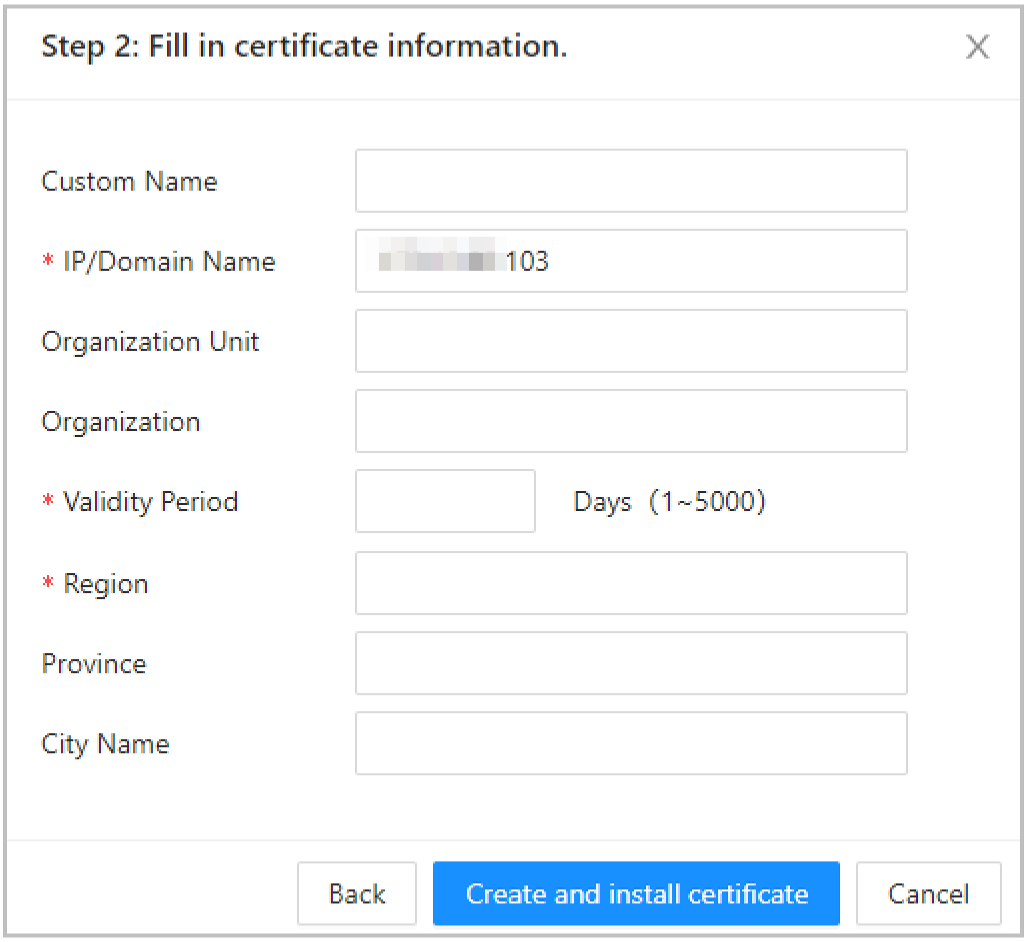
Step 1 Select ⛨ > **CA Certificate** > **Device Certificate**.

Step 2 Select **Install Device Certificate**.

Step 3 Select **Create Certificate** , and click **Next**.

Step 4 Enter the certificate information.

Figure 3-57 Certificate information



Step 2: Fill in certificate information.

Custom Name	
* IP/Domain Name	[redacted] 103
Organization Unit	
Organization	
* Validity Period	Days (1~5000)
* Region	
Province	
City Name	

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

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

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

Related Operations

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

3.11.4.2 Applying for and Importing CA Certificate

Import the third-party CA certificate to the Device.

Procedure

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

Step 2 Click **Install Device Certificate**.

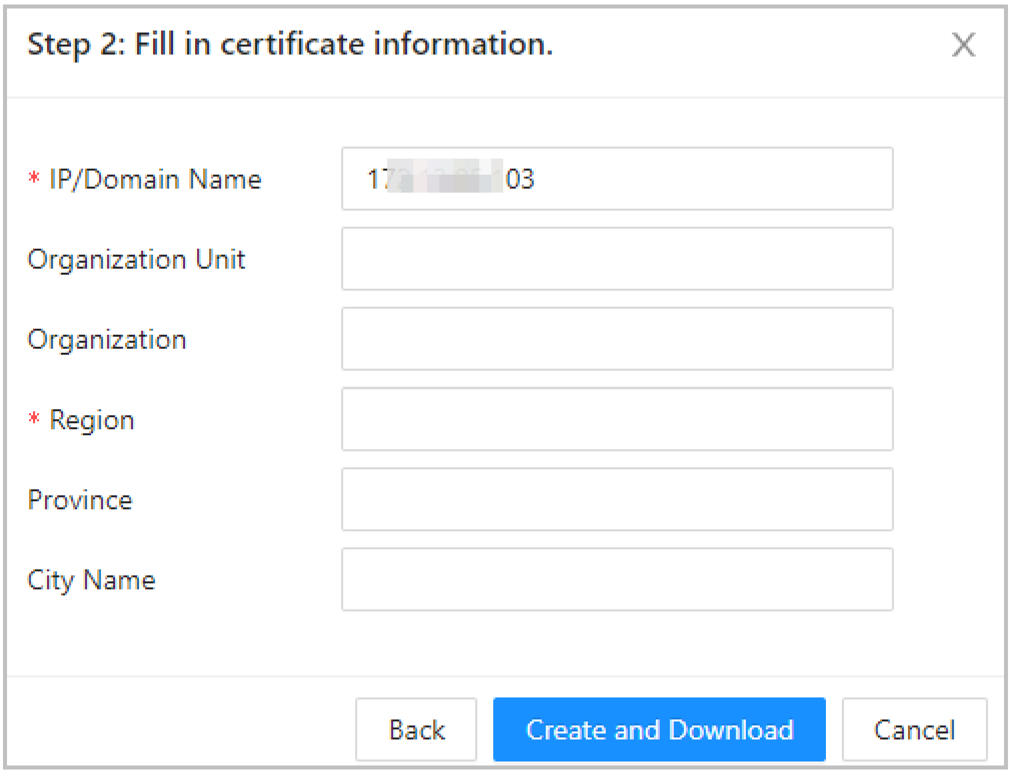
Step 3 Select **Apply for CA Certificate and Import (Recommended)** , and click **Next**.

Step 4 Enter the certificate information.

- IP/Domain name: the IP address or domain name of the Device.

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

Figure 3-58 Certificate information (2)



Step 2: Fill in certificate information.

* IP/Domain Name	17[redacted]03
Organization Unit	
Organization	
* Region	
Province	
City Name	

Step 5 Click **Create and Download**.

Save the request file to your computer.

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

Step 7 Import the signed CA certificate.

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

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

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

Related Operations

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

3.11.4.3 Installing Existing Certificate

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

Procedure

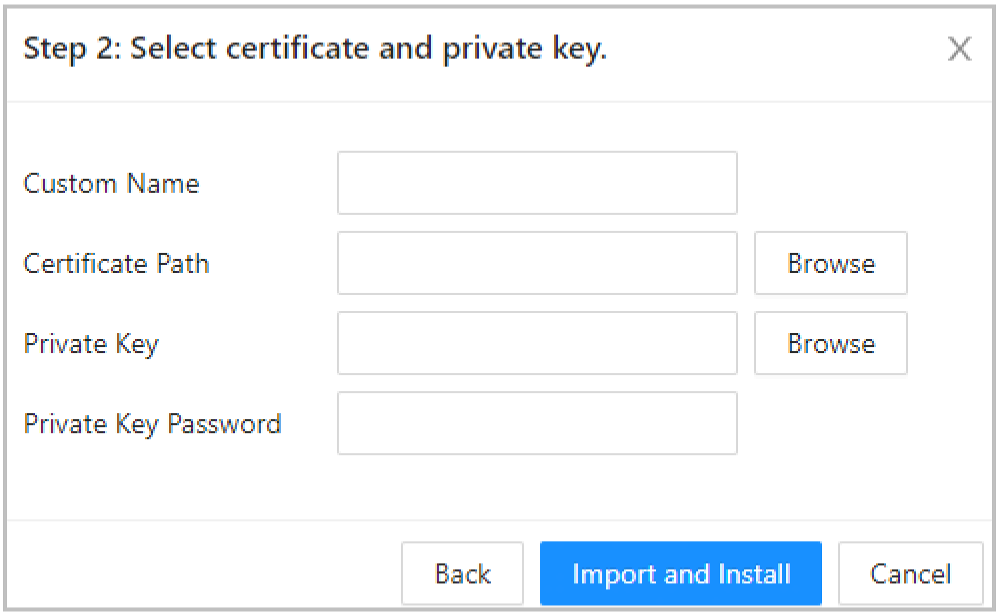
Step 1 Select **Security** > **CA Certificate** > **Device Certificate**.

Step 2 Click **Install Device Certificate**.

Step 3 Select **Install Existing Certificate** , and click **Next**.

Step 4 Click **Browse** to select the certificate and private key file, and enter the private key password.

Figure 3-59 Certificate and private key



Step 2: Select certificate and private key.

Custom Name		
Certificate Path		Browse
Private Key		Browse
Private Key Password		

Step 5 Click **Import and Install**.

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

Related Operations

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

3.11.5 Installing the Trusted CA Certificate

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

Background Information

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

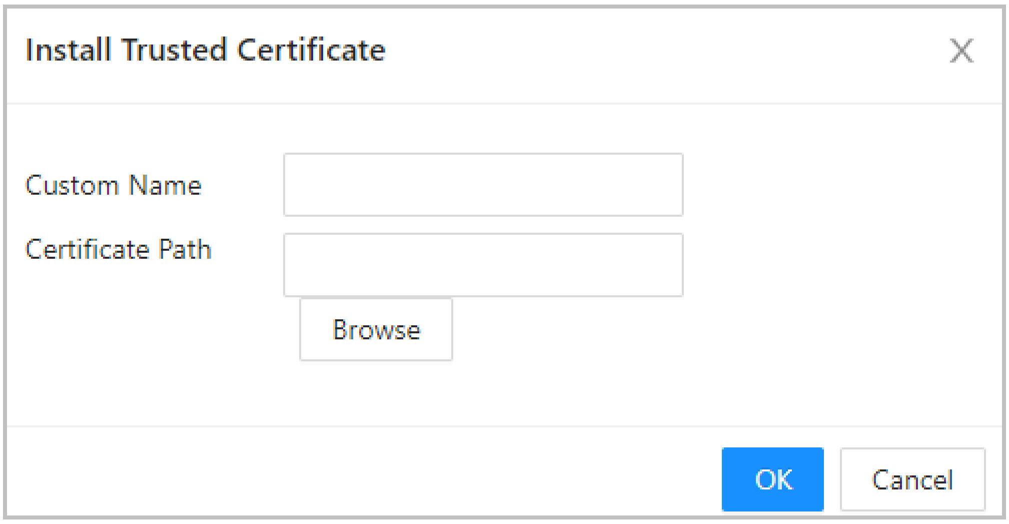
Procedure

Step 1 Select ⛉ > **CA Certificate** > **Trusted CA Certificates**.

Step 2 Select **Install Trusted Certificate**.

Step 3 Click **Browse** to select the trusted certificate.

Figure 3-60 Install the trusted certificate


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.

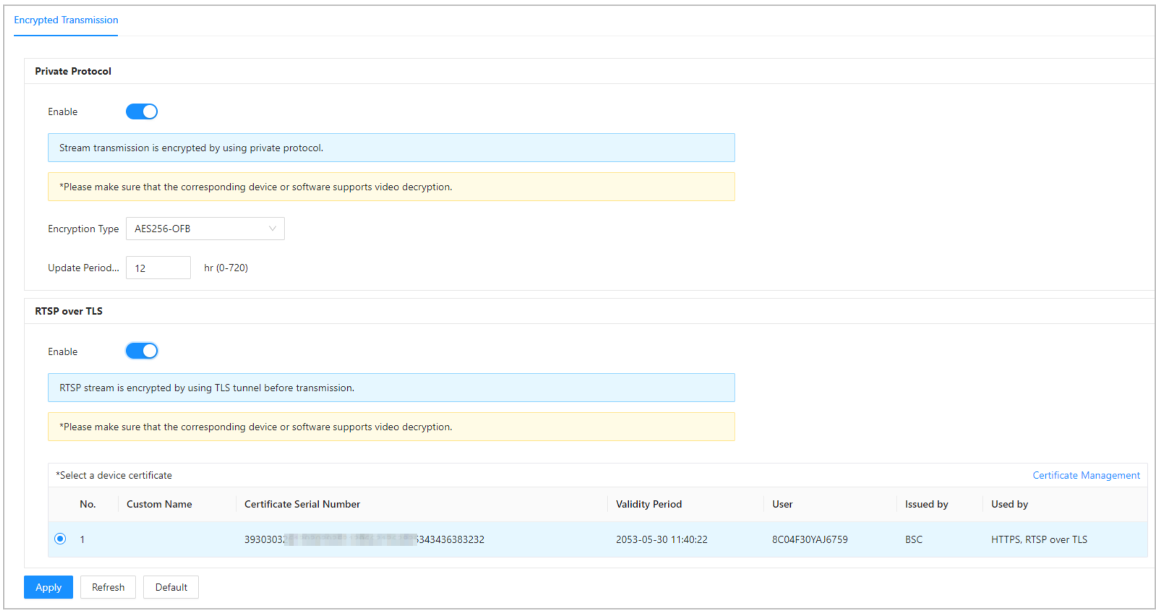
3.11.6 Data Encryption

Procedure

Step 1 Select 🛡 > **Data Encryption**.

Step 2 Configure the parameters.

Figure 3-61 Data encryption



Private Protocol

Enable: On

Stream transmission is encrypted by using private protocol.

*Please make sure that the corresponding device or software supports video decryption.

Encryption Type: AES256-OFB

Update Period...: 12 hr (0-720)

RTSP over TLS

Enable: On

RTSP stream is encrypted by using TLS tunnel before transmission.

*Please make sure that the corresponding device or software supports video decryption.

*Select a device certificate

	No.	Custom Name	Certificate Serial Number	Validity Period	User	Issued by	Used by
●	1		3930303[redacted]343436383232	2053-05-30 11:40:22	8C04F30YAJ6759	BSC	HTTPS, RTSP over TLS

Table 3-29 Data encryption description

	Parameter	Description
Private Protocol	Enable	Streams are encrypted during transmission through private protocol.
	Encryption Type	Keep it as default.
	Update Period of Secret Key	Ranges from 0 h -720 h. 0 means never update the secret key.
RTSP over TLS	Enable	RTSP stream is encrypted during transmission through TLS tunnel.
	Certificate Management	Create or import certificate. For details, see "3.11.4 Installing Device Certificate". The installed certificates are displayed in the list.

3.11.7 Security Warning

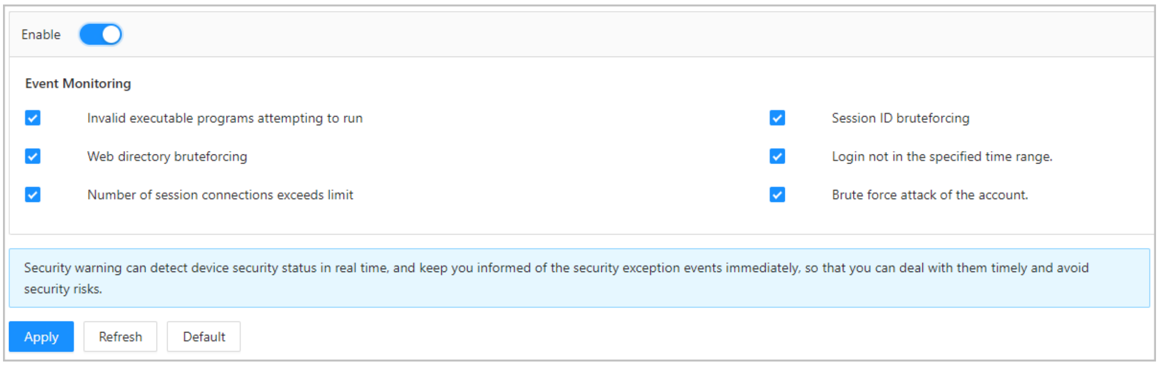
Procedure

Step 1 Select 🛡 > **Security Warning**.

Step 2 Enable the security warning function.

Step 3 Select the monitoring items.

Figure 3-62 Security warning



Enable ●

Event Monitoring

☑ 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.

☑ 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**.

3.11.8 Security Authentication

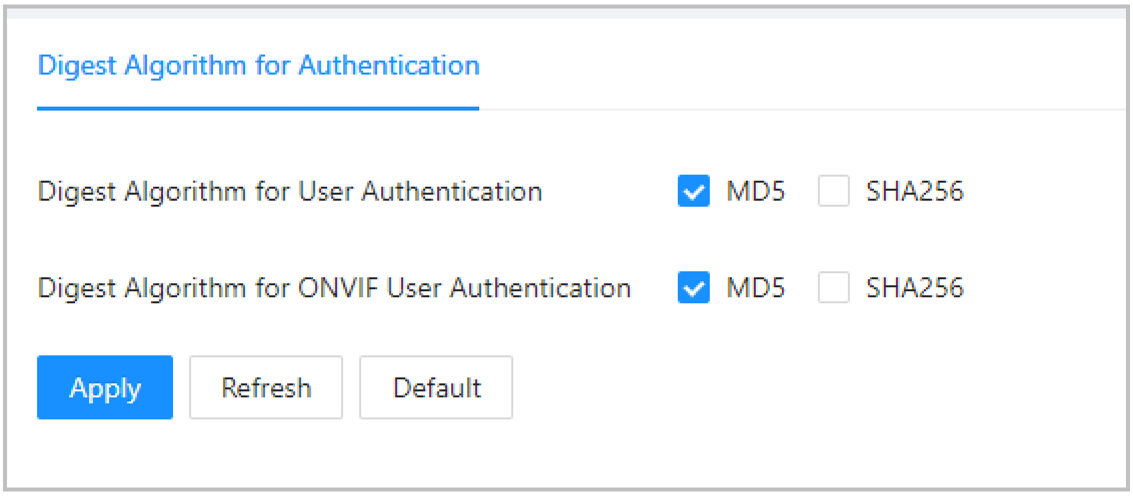
Procedure

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

Step 2 Select a message digest algorithm.

Step 3 Click **Apply**.

Figure 3-63 Security Authentication



Digest Algorithm for Authentication

Digest Algorithm for User Authentication ☑ MD5 □ SHA256

Digest Algorithm for ONVIF User Authentication ☑ MD5 □ SHA256

4 Phone Operations

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

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

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

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

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

4.1 Logging in to the Webpage

Prerequisites

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

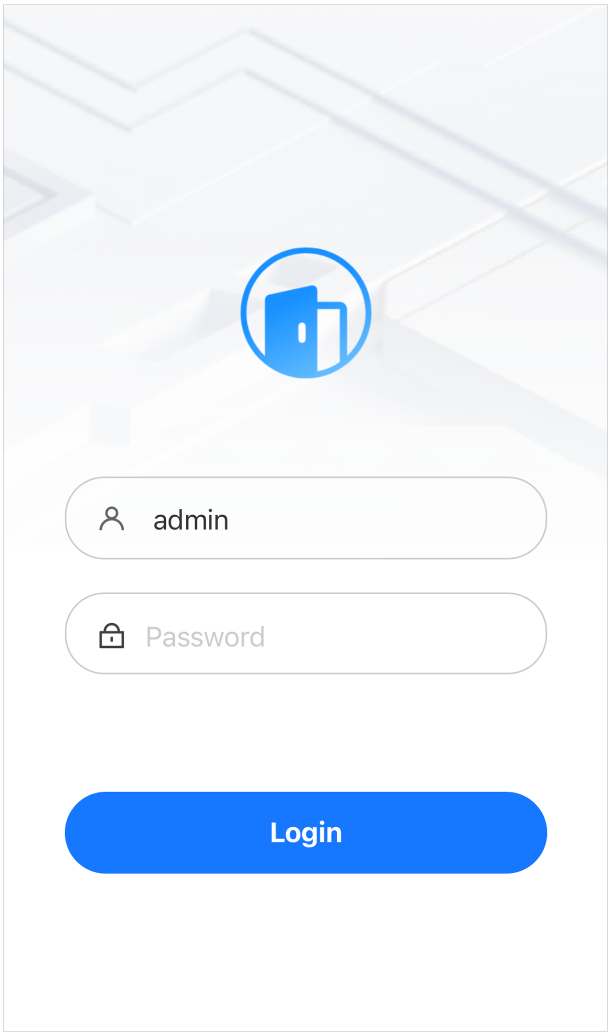
Procedure

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

Step 2 Enter the user name and password.

- The default administrator name is admin, and the password is the one you set up during initialization. We recommend you change the administrator password regularly to increase security.
- If you forget the administrator login password, you can reset the password through the webpage on the computer. For details, see "3.2 Resetting the Password".

Figure 4-1 Login page



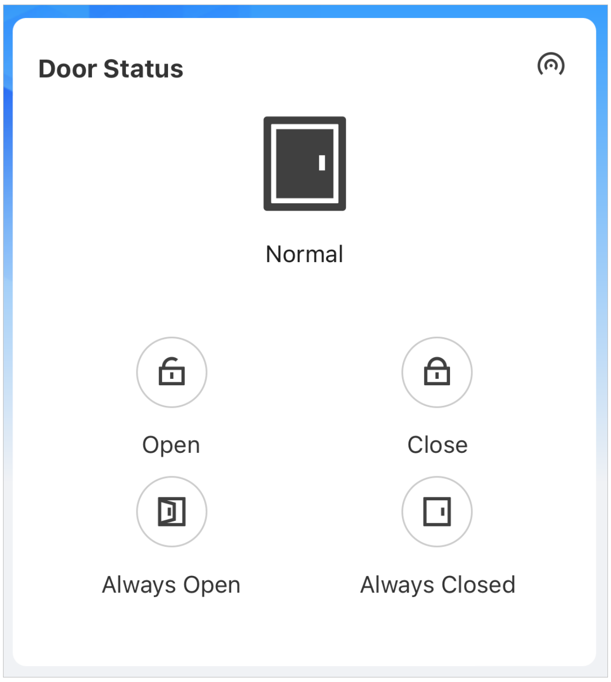
Step 3 Click **Login**.

4.2 Home Page

The home page is displayed after you successfully log in.

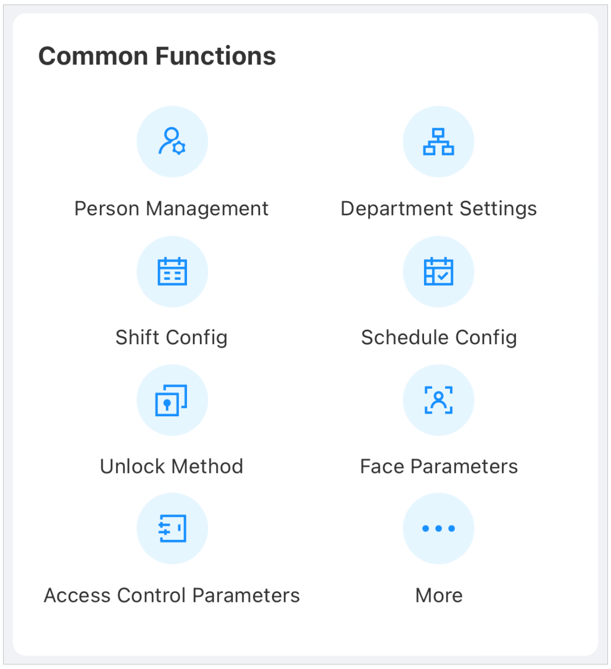
- The **Door Status** area displays the status of the door. You can remotely open or close the door. You can also configure the door status as **Always Open** or **Always Closed**.

Figure 4-2 Door status



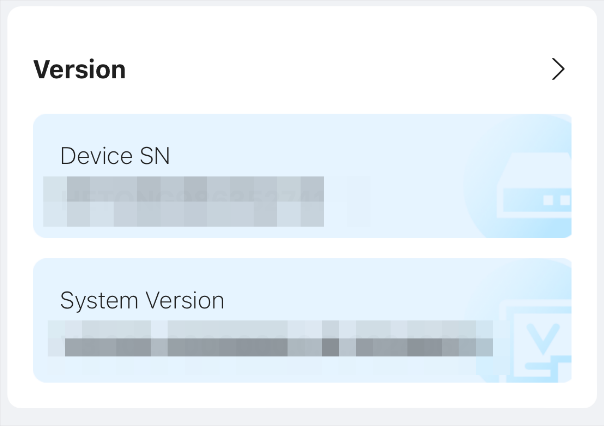
- The **Common Function** area displays the configuration menu of the Device. Click **More** to view all the configuration menus.

Figure 4-3 Common functions



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

Figure 4-4 Version



Version

Device SN

System Version

4.3 Person Management

Add the person and configure the permissions.

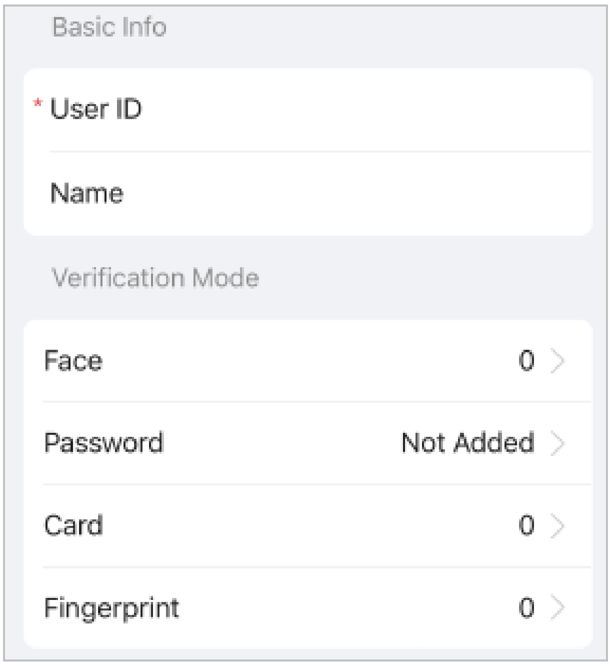
Procedure

Step 1 Log in to the webpage.

Step 2 Click **Person Management** , and then click **+**.

Step 3 Configure user information.

Figure 4-5 Add the person (1)



Basic Info

* User ID

Name

Verification Mode

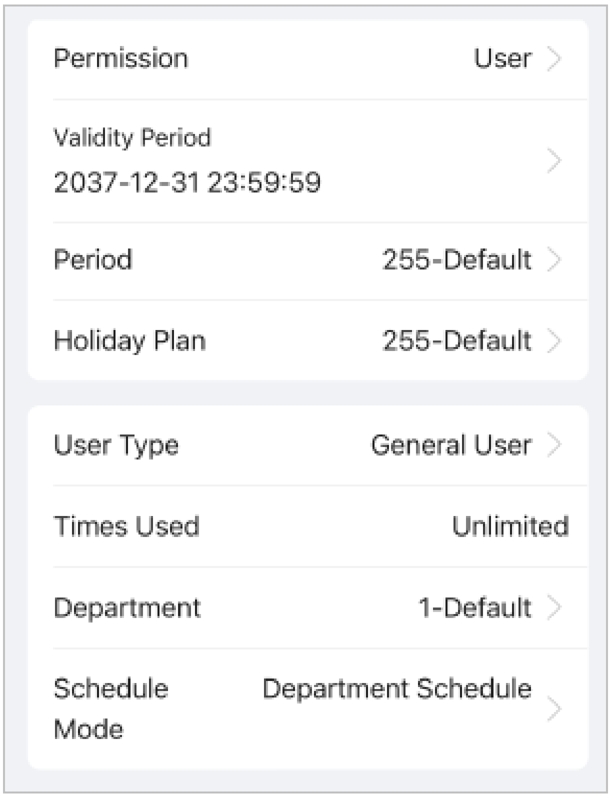
Face 0

Password Not Added

Card 0

Fingerprint 0

Figure 4-6 Add the person (2)



Permission User

Validity Period 2037-12-31 23:59:59

Period 255-Default

Holiday Plan 255-Default

User Type General User

Times Used Unlimited

Department 1-Default

Schedule Mode Department Schedule

Table 4-1 Parameters description

Parameter	Description
User ID	The User ID is like employee ID, which can be numbers, letters, and their combinations, and the maximum length of the number is 30 characters.
Name	The name can have up to 32 characters (including numbers, symbols, and letters).
Face	Upload a face image. Each person can only add up to 2 face images. You can view or delete the face image after you upload it. 📖 The face image is in jpg, jpeg, png format and must be less than 100 KB.
Password	Configure the user password. The maximum length of the password is 8 digits. The duress password is the unlock password + 1. For example, if the user password is 12345, the duress password will be 12346. A duress alarm will be triggered when a duress password is used to unlock the door.

Parameter	Description
Card	- Enter the card number manually. 1. Click **Add**. 2. Enter the card number, and then click **Add**. - Read the number automatically through the Device. 1. Click **Add**. 2. Swipe cards on the card reader. A 60-second countdown is displayed to remind you to swipe cards, and the system will read the card number automatically. If the 60-second countdown expires, click **Read Card** again to start a new countdown. 3. Click **OK**. A user can register up to 5 cards at most. Enter your card number or swipe your card, and then the card information will be read by the Device. You can enable the **Duress Card** function. An alarm will be triggered if a duress card is used to unlock the door. - **Duress Card** : Click to set duress card. - **Change Card No.** : Click to change the card number. One user can only set one duress card.
Fingerprint	Register fingerprints. A user can register up to 3 fingerprints, and you can set a fingerprint to the duress fingerprint. An alarm will be triggered when the duress fingerprint is used to unlock the door. Enroll fingerprints through an enrollment reader or the Device. 1. Click **Add**. 2. Press finger on the scanner according to the on-screen instructions. 3. Click **OK**. - Fingerprint function is only available on select models. - We do not recommend you set the first fingerprint as the duress fingerprint. - One user can only sets one duress fingerprint.
Permission	- **User** : Users only have door access or time attendance permissions. - **Admin** : Administrators can configure the Device besides door access and attendance permissions.
Validity Period	Set a date on which the door access and attendance permissions of the person will be expired.

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

Step 4 Click **Add**.

4.4 Configuring the System

4.4.1 Viewing Version Information

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

4.4.2 Maintenance

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

Procedure

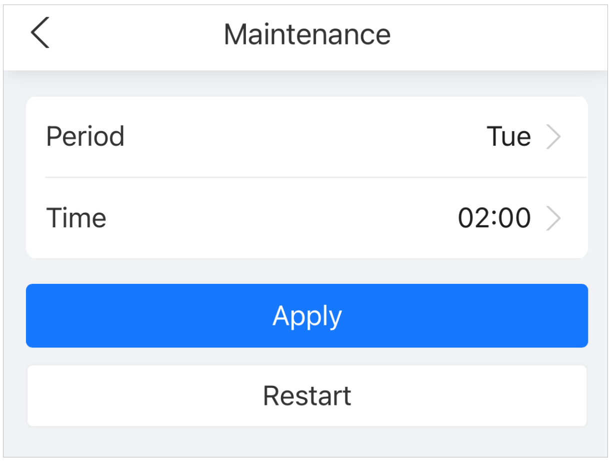
Step 1 Log in to the webpage.

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

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

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

Figure 4-7 Maintenance



Maintenance

Period Tue

Time 02:00

4.4.3 Configuring Time

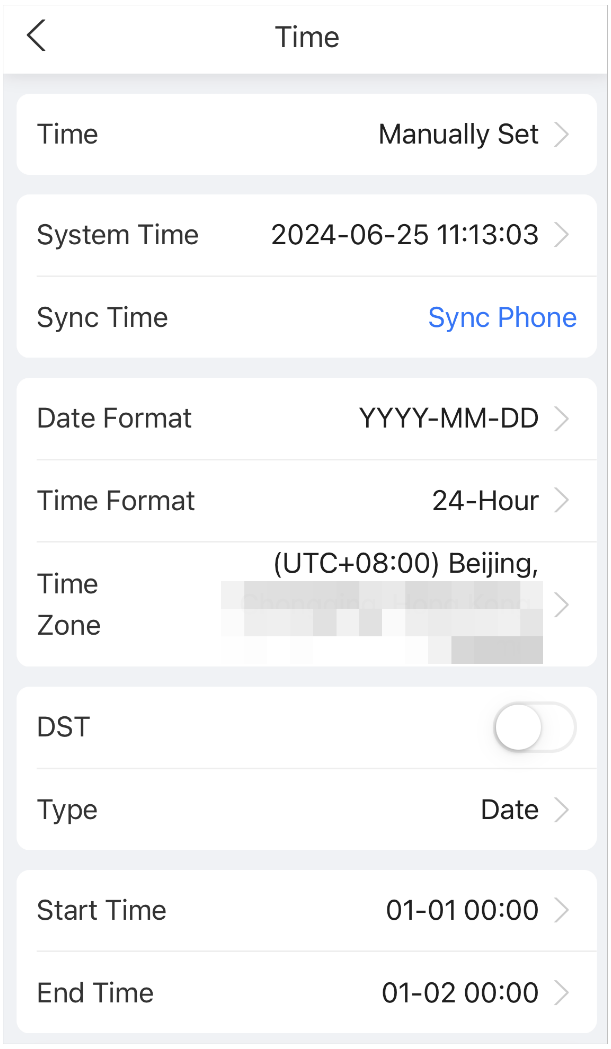
Procedure

Step 1 Log in to the webpage.

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

Step 3 Configure the time.

Figure 4-8 Configure the time parameters



Time

Time: Manually Set

System Time: 2024-06-25 11:13:03

Sync Time: Sync Phone

Date Format: YYYY-MM-DD

Time Format: 24-Hour

Time Zone: (UTC+08:00) Beijing, [redacted]

DST: ○

Type: Date

Start Time: 01-01 00:00

End Time: 01-02 00:00

Table 4-2 Time settings description

Parameter	Description
Time	● Manual Set: Manually enter the time or you can click **Sync Phone** to sync time with the phone. ● NTP: The Device will automatically sync the time with the NTP server. ◇ **Server** : Enter the domain of the NTP server. ◇ **Port** : Enter the port of the NTP server. ◇ **Interval** : Enter its time with the synchronization interval.
Date Format	Select the date format and the time format.
Time Format	
Time Zone	Select the time zone.
DST	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 Click **Apply**.

4.4.4 Data Capacity

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

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

4.5 Configuring Attendance

This function is only available on select models.

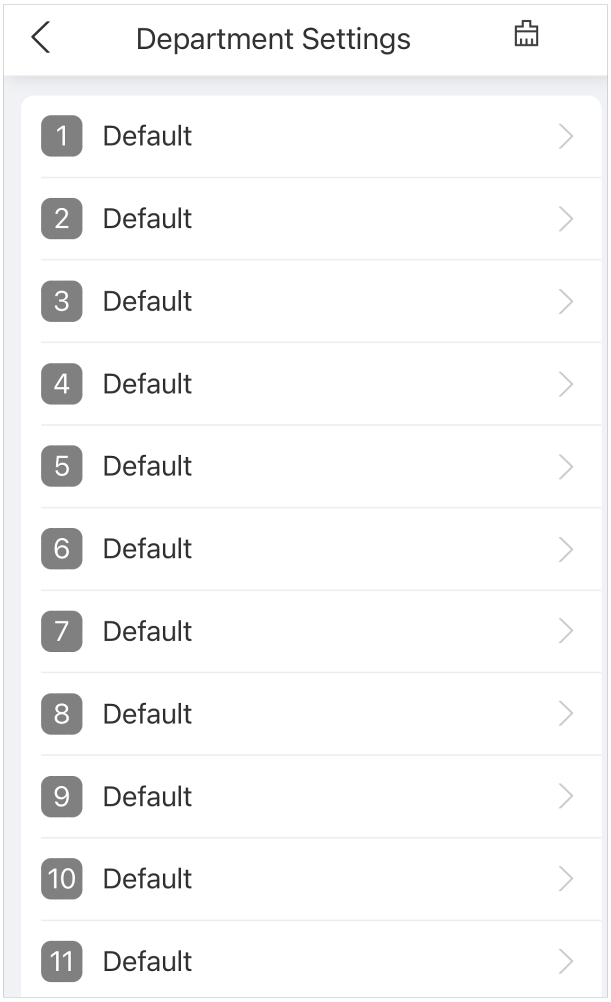
4.5.1 Configuring Departments

Procedure

Step 1 Log in to the webpage.

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

Figure 4-9 Department settings



Department Settings

1 Default

2 Default

3 Default

4 Default

5 Default

6 Default

7 Default

8 Default

9 Default

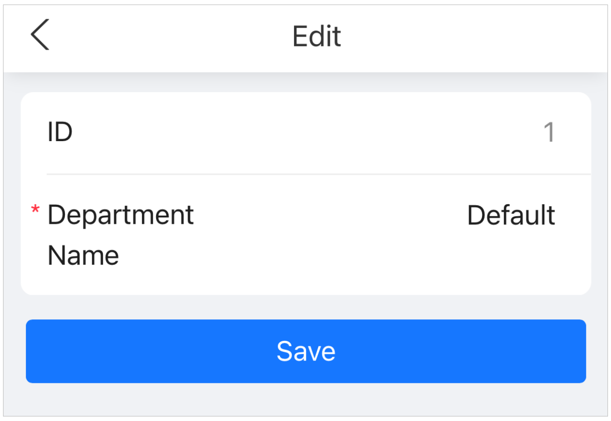
10 Default

11 Default

Step 3 Click the department to rename the department, and then click **Save**.

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

Figure 4-10 Rename the department



Edit

ID 1

* Department Name Default

Related Operations

You can click 🖫 to restore departments to default settings.

4.5.2 Configuring Shifts

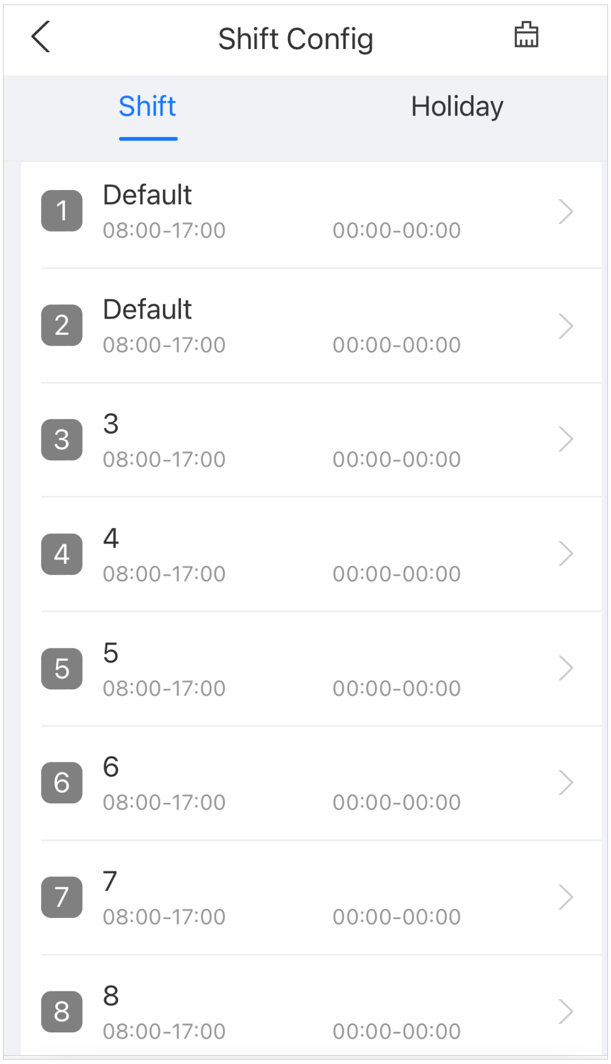
Configure shifts to define time attendance rules. Employees need to work at the time scheduled for their shift to start, and leave at the end time, except when they choose to work overtime.

Procedure

Step 1 Log in to the webpage.

Step 2 Select **More** > **Attendance Config** > **Shift Config** > **Shift**.

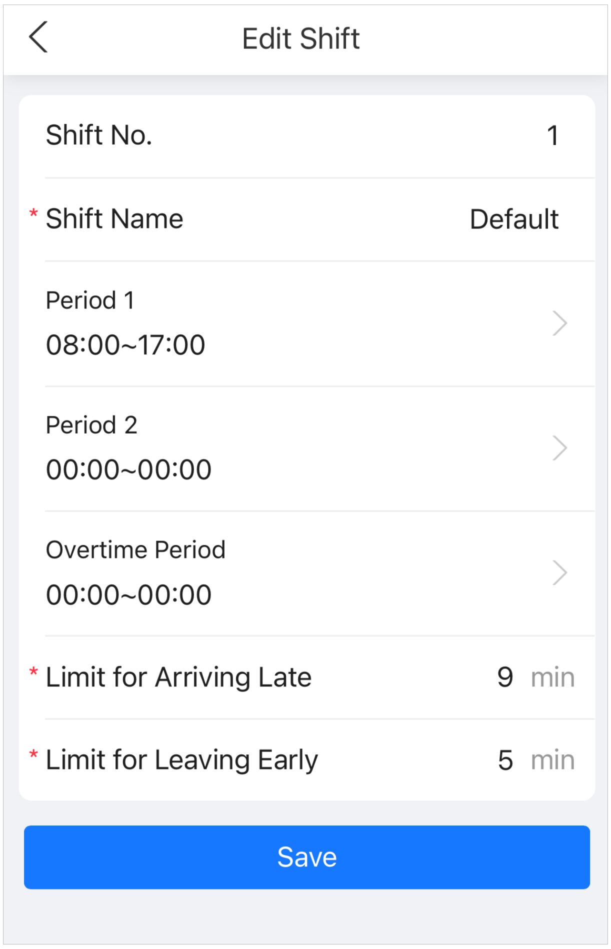
Figure 4-11 Shift list



1	Default	08:00-17:00	00:00-00:00
2	Default	08:00-17:00	00:00-00:00
3	3	08:00-17:00	00:00-00:00
4	4	08:00-17:00	00:00-00:00
5	5	08:00-17:00	00:00-00:00
6	6	08:00-17:00	00:00-00:00
7	7	08:00-17:00	00:00-00:00
8	8	08:00-17:00	00:00-00:00

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

Figure 4-12 Configure the shift



Edit Shift

Shift No. 1

* Shift Name Default

Period 1
08:00~17:00

Period 2
00:00~00:00

Overtime Period
00:00~00:00

* Limit for Arriving Late 9 min

* Limit for Leaving Early 5 min

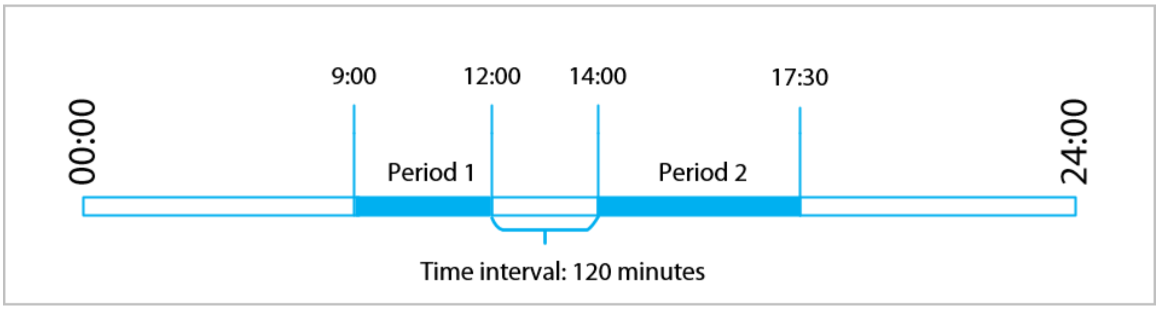
Save

Table 4-3 Shift parameters description

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

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

Figure 4-13 Time interval (even number)



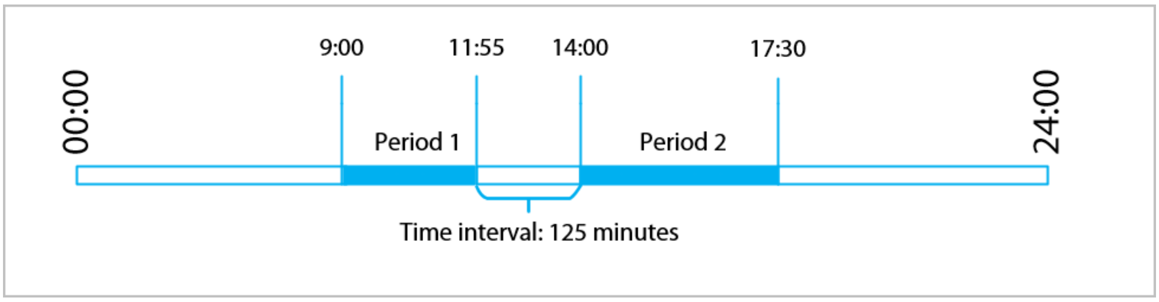
For example: If the interval is 120 minutes, then the clock-out time for period 1 is from 12:00 to 12:59, and the clock-in time for period 2 is from 13:00 to 14:00.

📖

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 4-14 Time interval (even number)



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

📖

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

📖

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

Related Operations

You can click 🗄 to restore shifts to factory defaults.

4.5.3 Configuring Holiday

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

Procedure

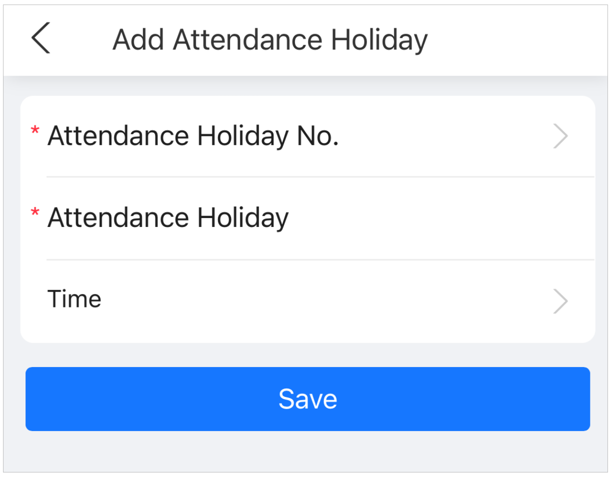
Step 1 Log in to the webpage.

Step 2 Select **More** > **Attendance Config** > **Shift Config** > **Holiday**.

Step 3 Click **+** to add holiday plans.

Step 4 Configure the parameters, and then click **Save**.

Figure 4-15 Add the holiday



Add Attendance Holiday

* Attendance Holiday No.

* Attendance Holiday

Time

Save

Table 4-4 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 Click **OK**.

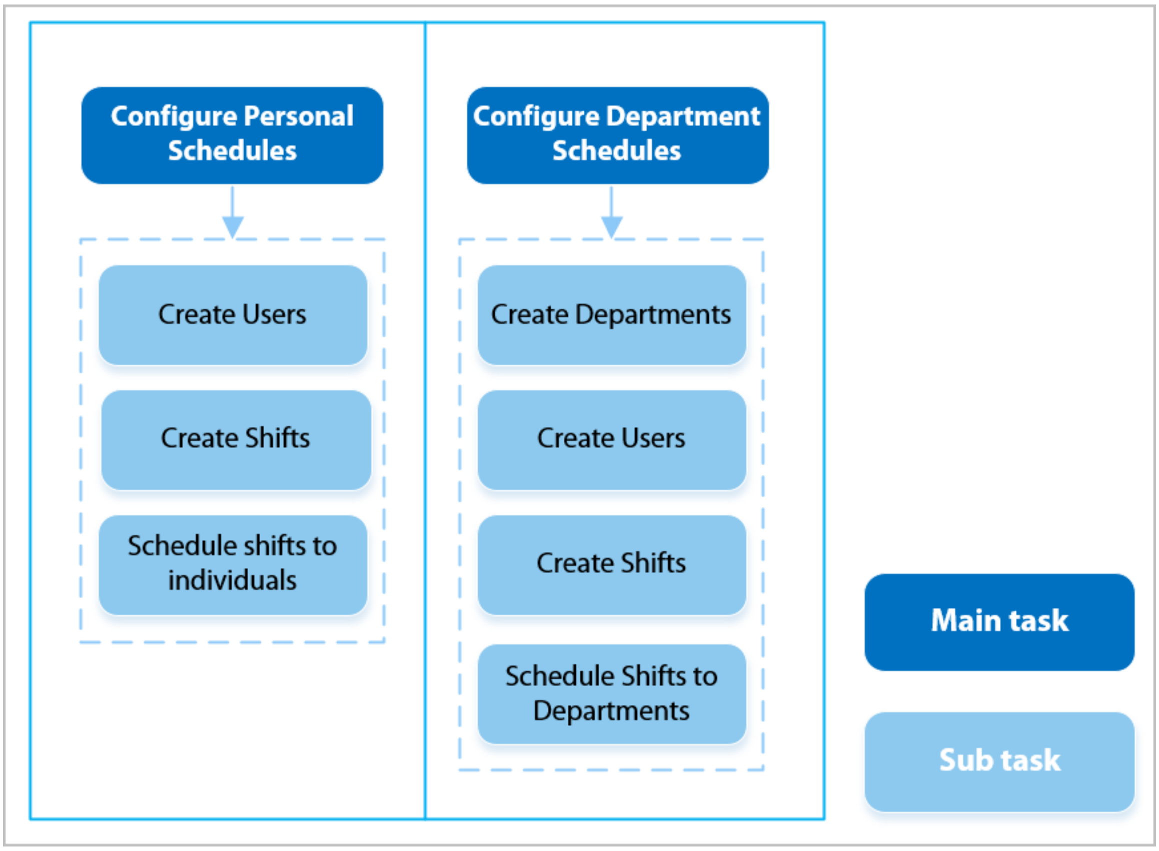
4.5.4 Configuring Work Schedules

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

Background Information

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

Figure 4-16 Configuring work schedules


Configure Personal Schedules
Create Users
Create Shifts
Schedule shifts to individuals
Configure Department Schedules
Create Departments
Create Users
Create Shifts
Schedule Shifts to Departments
Main task
Sub task

Procedure

Step 1 Log in to the webpage.

Step 2 Select **More** > **Attendance Config** > **Schedule Config**.

Step 3 Set work schedules for individuals.

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

   After you configure the **Schedule Mode** as the **Personal Schedule** when you add the person, the person is displayed in the person list.
3. On the calendar, select a day, and then select a shift.

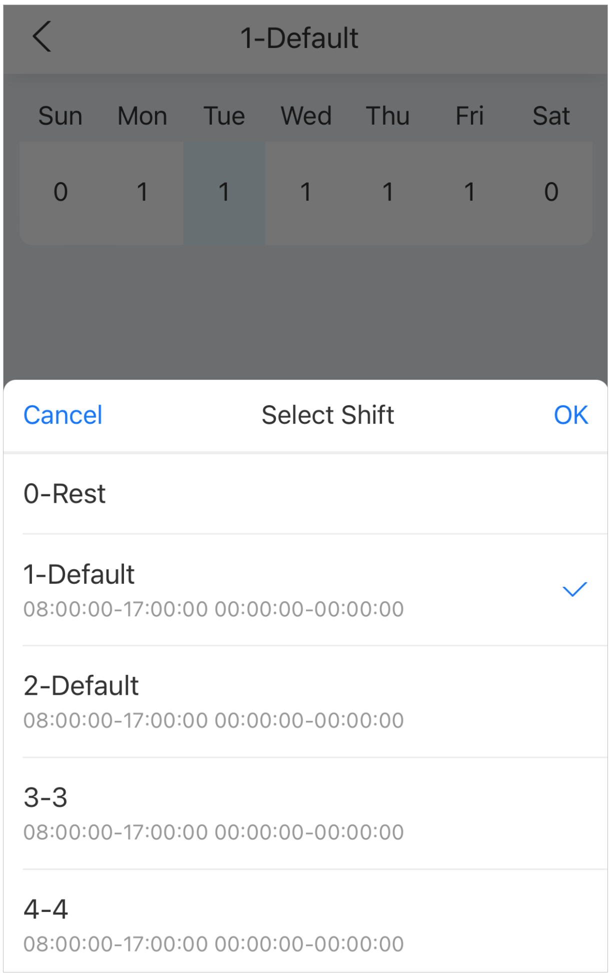
You can only set work schedules for the current month and the next month.

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

Step 4 Set works schedules for departments.

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

Figure 4-17 Department schedule



1-Default

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

Cancel Select Shift OK

0-Rest

1-Default ✓
08:00:00-17:00:00 00:00:00-00:00:00

2-Default
08:00:00-17:00:00 00:00:00-00:00:00

3-3
08:00:00-17:00:00 00:00:00-00:00:00

4-4
08:00:00-17:00:00 00:00:00-00:00:00

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

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

4.5.5 Configuring Attendance Modes

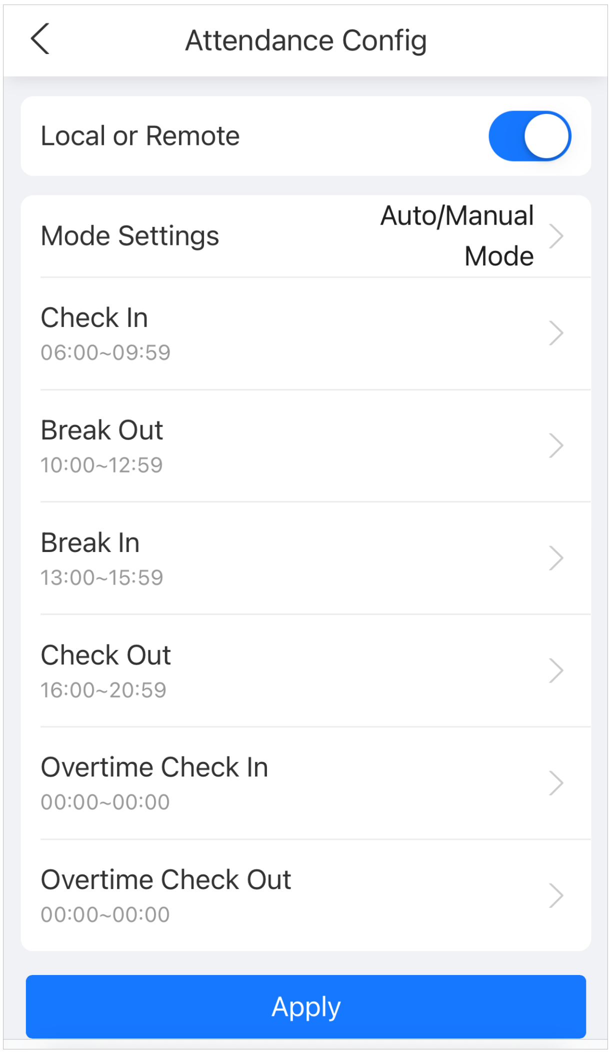
Procedure

Step 1 Log in to the webpage.

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

Step 3 Enable **Local or Remote**, and then configure the attendance mode.

Figure 4-18 Attendance configuration



Attendance Config

Local or Remote

Mode Settings: Auto/Manual Mode

Check In
06:00~09:59

Break Out
10:00~12:59

Break In
13:00~15:59

Check Out
16:00~20:59

Overtime Check In
00:00~00:00

Overtime Check Out
00:00~00:00

Table 4-5 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 starts. ● 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 starts. ● 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 per-defined attendance status all the time.

Step 4 Click **Apply**.

4.6 Configuring Access Control

4.6.1 Configuring Unlock Methods

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

Procedure

Step 1 Log in to the webpage.

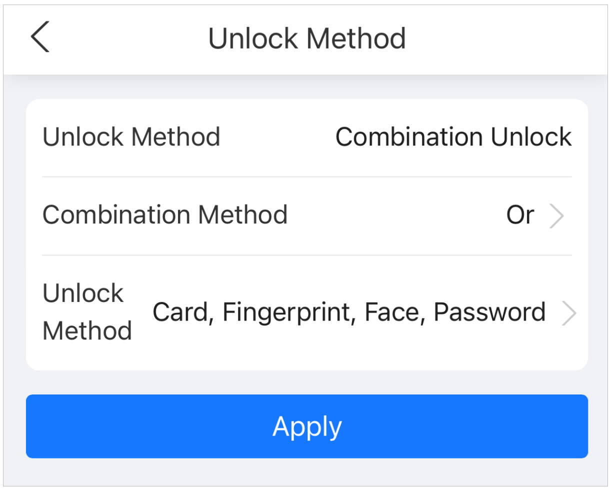
Step 2 Click **Unlock Method** on the main menu, or select **More** > **Access Control** > **Unlock Method**.

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

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

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

Figure 4-19 Unlock method



Unlock Method

Unlock Method	Combination Unlock
Combination Method	Or
Unlock Method	Card, Fingerprint, Face, Password

4.6.2 Configuring Face Parameters

Configure face detection parameters. Face parameters might differ depending on models of the product.

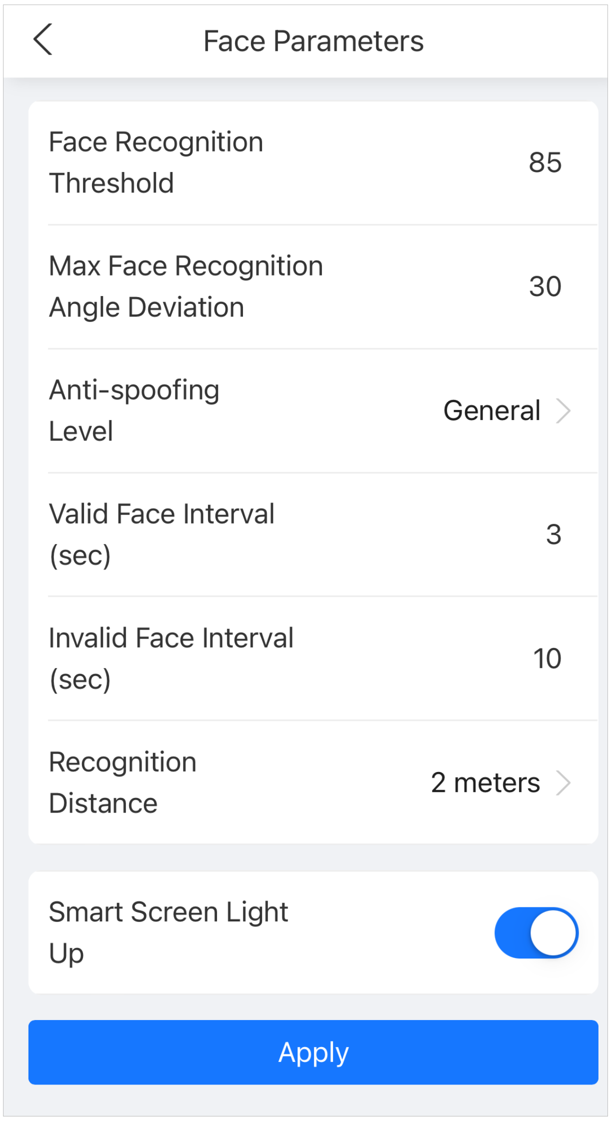
Procedure

Step 1 Log in to the webpage.

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

Step 3 Configure the parameters, and then click **Apply**.

Figure 4-20 Configure the face parameters



Face Parameters

Face Recognition Threshold	85
Max Face Recognition Angle Deviation	30
Anti-spoofing Level	General
Valid Face Interval (sec)	3
Invalid Face Interval (sec)	10
Recognition Distance	2 meters
Smart Screen Light Up	●

Table 4-6 Description of face parameters

Name	Description
Face Recognition Threshold	Adjust the accuracy level of face recognition. Higher threshold means higher accuracy and lower false recognition rate. 📖 When the threshold is too low such as 0, the false recognition rate will be extremely high. Please be advised.
Max Face Recognition Angle Deviation	Set the largest angle that a face can be posed in for face detection. The larger the value, the larger the range for the face angle. If the angle a face is positioned in is not within the defined range, it might not be detected properly.
Anti-spoofing Level	This prevents people from being able to use photos, videos, mask and other substitutes to gain unauthorized access.

Name	Description
Valid Face Interval (sec)	When the same face remains in front of the lens after the first successful recognition, the Device will perform recognition again for the face after a defined interval.
Invalid Face Interval (sec)	When the same face remains in front of the lens after the first failed recognition, the Device will perform recognition again for the face after a defined interval.
Recognition Distance	The distance between the face and the lens.
Smart Screen Light Up	When enabled, in the screen-off status, the screen will light up when a face is detected.

4.6.3 Configuring Access Control Parameters

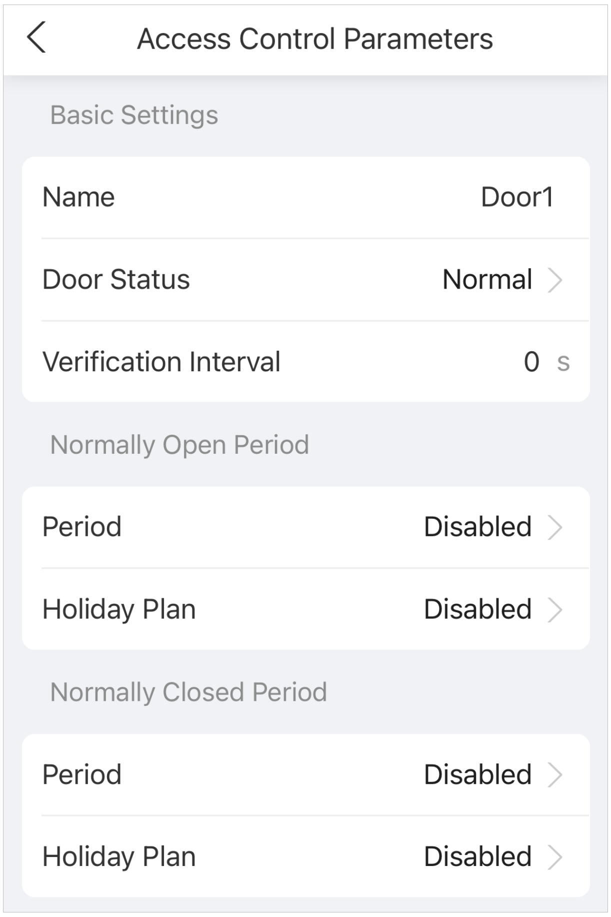
Procedure

Step 1 Log in to the webpage.

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

Step 3 Configure basic parameters for the access control, and then click **Apply**.

Figure 4-21 Access control parameters (1)



Access Control Parameters

Basic Settings

Name Door1

Door Status Normal

Verification Interval 0 s

Normally Open Period

Period Disabled

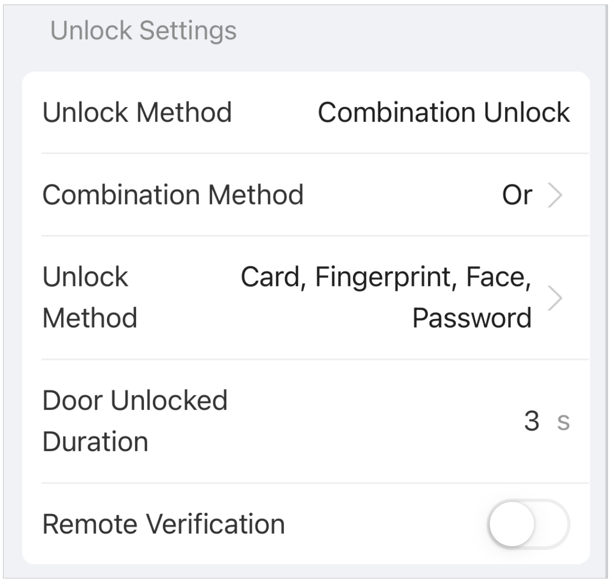
Holiday Plan Disabled

Normally Closed Period

Period Disabled

Holiday Plan Disabled

Figure 4-22 Access control parameters (2)



Unlock Settings

Unlock Method: Combination Unlock

Combination Method: Or

Unlock Method: Card, Fingerprint, Face, Password

Door Unlocked Duration: 3 s

Remote Verification: ○

Table 4-7 Description of access control parameters

Parameter		Description
Basic Settings	Name	The name of the door.
	Door Status	Set the door status. ● Normal: The door will be unlocked and locked according to your settings. ● Always Open: The door remains unlocked all the time. ● Always Closed: The door remains locked all the time.
	Verification Interval	If you verify your identity multiple times within a set period, only the earliest verification will be considered valid, and the door will not open after the second or later verifications. From the moment the door fails to open, you must wait for the configured verification time interval before attempting to verify your identity again.
Normally Open Period	Period/Holiday Plan	When you select **Normal**, you can select a time template from the drop-down list. The door remains open or closed during the defined time. ● When normally open period conflicts with normally closed period, normally open period takes priority over normally closed period. ● When period conflict with holiday plan, holiday plans takes priority over periods.
Normally Closed Period	Period/Holiday Plan	
Unlock Settings	Unlock Method	**Combination Unlock** by default.

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

Step 4 Click **Apply**.

4.6.4 Configuring Alarms

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

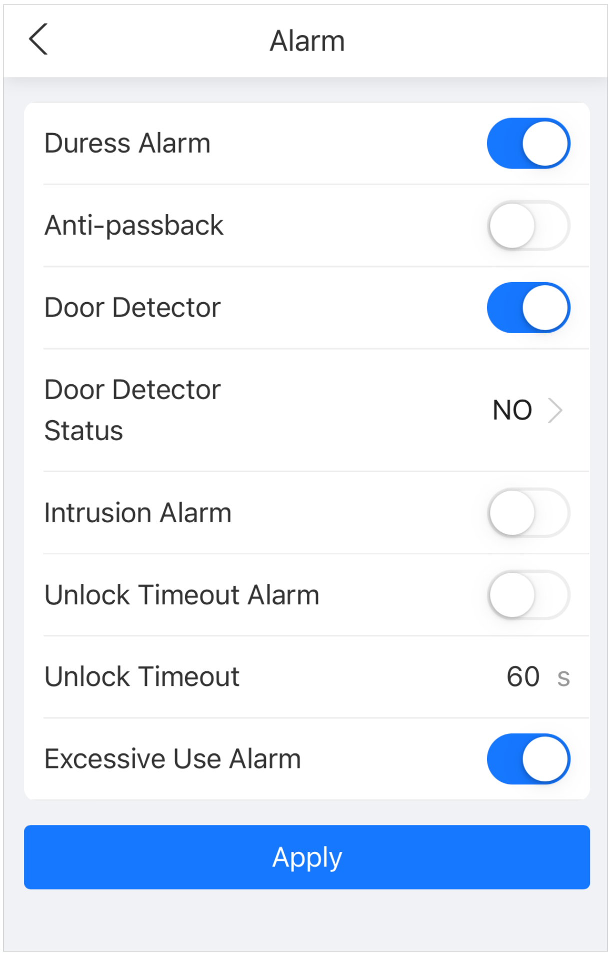
Procedure

Step 1 Log in to the webpage.

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

Step 3 Configure alarm parameters, and then click **Apply**.

Figure 4-23 Alarm settings



Alarm

Duress Alarm: on

Anti-passback: off

Door Detector: on

Door Detector Status: NO

Intrusion Alarm: off

Unlock Timeout Alarm: off

Unlock Timeout: 60 s

Excessive Use Alarm: on

Table 4-8 Description of alarm parameters

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

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. ● Normally Closed: The sensor is in a shorted position when the door or window is closed. ● Normally Open: 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. 📖 The door detector and door timed out function need to be enabled at the same time.
Unlock Timeout	
Excessive Use Alarm	If the wrong password or card is used 5 times in a row within 60 seconds, the alarm for excessive use of illegal card will be triggered and lasts for a defined time.

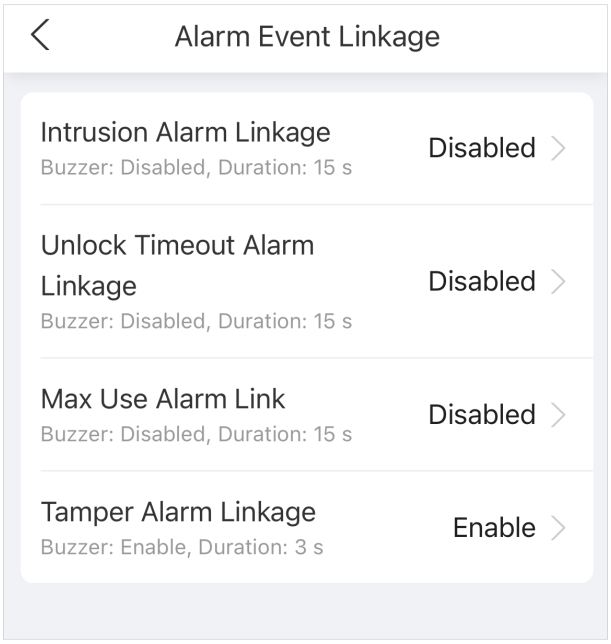
4.6.5 Configuring Alarm Event Linkage

Procedure

Step 1 Log in to the webpage.

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

Figure 4-24 Alarm event linkage



Alarm Event Linkage

Intrusion Alarm Linkage: Disabled
Buzzer: Disabled, Duration: 15 s

Unlock Timeout Alarm Linkage: Disabled
Buzzer: Disabled, Duration: 15 s

Max Use Alarm Link: Disabled
Buzzer: Disabled, Duration: 15 s

Tamper Alarm Linkage: Enable
Buzzer: Enable, Duration: 3 s

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

Table 4-9 Alarm event linkage

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

Parameter	Description
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.

4.6.6 Configuring Card Settings

Background Information

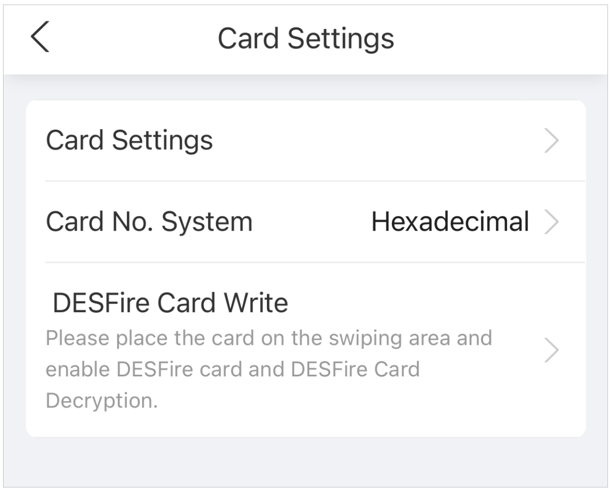
Procedure

Step 1 Log in to the webpage.

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

Step 3 Configure the card parameters, and then click **Apply**.

Figure 4-25 Card settings (1)



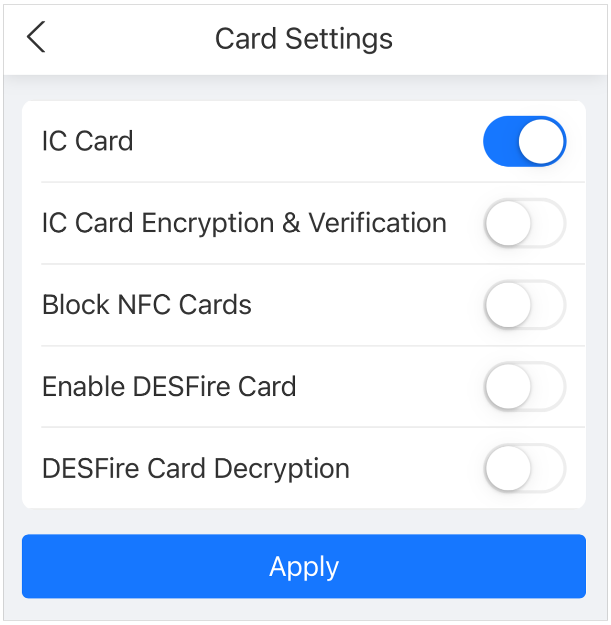
Card Settings

Card No. System Hexadecimal

DESFire Card Write

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

Figure 4-26 Card settings (2)



IC Card ●

IC Card Encryption & Verification ○

Block NFC Cards ○

Enable DESFire Card ○

DESFire Card Decryption ○

Table 4-10 Card parameters description

Item	Parameter	Description
Card Settings	IC Card	The IC card can be read when this function is enabled. 🕮 This function is only available on select models.
	IC Card Encryption & Verification	The encrypted card can be read when this function is enabled. 🕮 Make sure **IC Card** is enabled.
	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 **IC Card** is enabled. ● NFC function is only available on select models of phones.
	Enable 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.

Item	Parameter	Description
DESFire Card Write	Card Number	Place the card on the reader, enter the card number, and then click **Write** to write card number to the card. 📖 ● Desfire card function must be enabled. ● Only supports hexadecimal format. ● Supports up to 8 characters.

Step 4 Click **Apply**.

4.6.7 Privacy Setting

Procedure

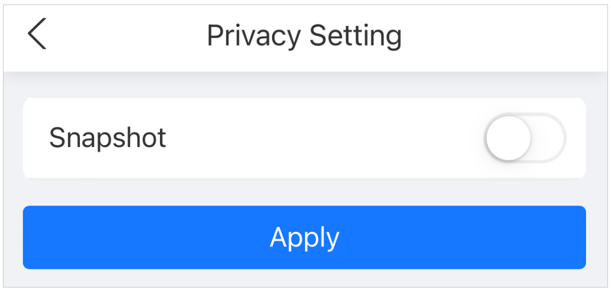
Step 1 Log in to the webpage.

Step 2 Select **More** > **Access Control** > **Privacy Setting**.

Step 3 Enable snapshot function.

Face images will be captured automatically when people unlock the door.

Figure 4-27 Enable snapshot



Step 4 Click **Apply**.

4.7 Communication Settings

4.7.1 Configuring TCP/IP

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

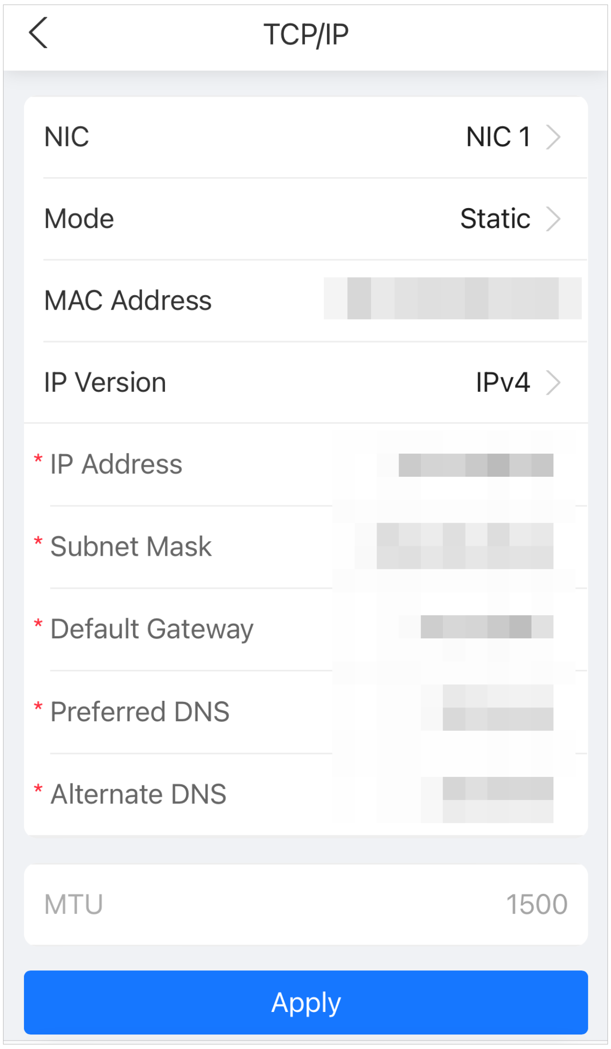
Procedure

Step 1 Log in to the webpage.

Step 2 Select **More** > **Communication Settings** > **Network Setting** > **TCP/IP**.

Step 3 Configure the parameters, and then click **Apply**.

Figure 4-28 TCP/IP



TCP/IP

NIC: NIC 1

Mode: Static

MAC Address: [redacted]

IP Version: IPv4

* IP Address: [redacted]

* Subnet Mask: [redacted]

* Default Gateway: [redacted]

* Preferred DNS: [redacted]

* Alternate DNS: [redacted]

MTU: 1500

Table 4-11 Description of TCP/IP

Parameter	Description
Mode	● Static: Manually enter IP address, subnet mask, and gateway. ● DHCP: It stands for Dynamic Host Configuration Protocol. When DHCP is turned on, the Device will automatically be assigned with IP address, subnet mask, and gateway.
MAC Address	MAC address of the Device.
IP Version	IPv4 or IPv6.
IP Address	If you set the mode to **Static**, configure the IP address, subnet mask and gateway. 📖 ● 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.
Subnet Mask	
Default Gateway	

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

4.7.2 Configuring Wi-Fi

Procedure

Step 1 Log in to the webpage.

Step 2 Select **More** > **Communication Settings** > **Wi-Fi**.

Step 3 Turn on Wi-Fi.

All available Wi-Fi are displayed.

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

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

The Wi-Fi is connected.

Related Operations

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

4.7.3 Configuring Wi-Fi AP

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

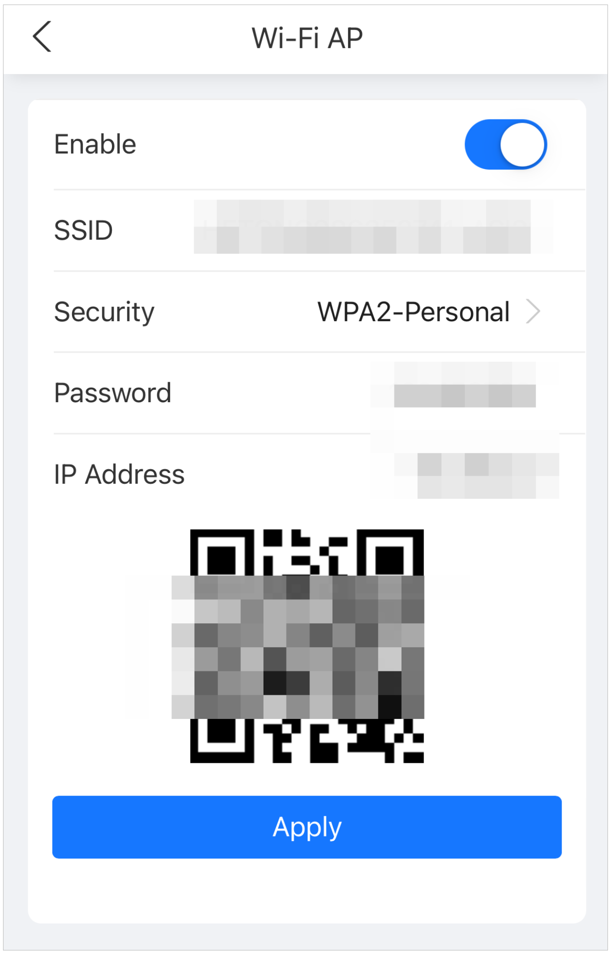
Procedure

Step 1 Log in to the webpage.

Step 2 Select **More** > **Communication Settings** > **Wi-Fi AP**.

Step 3 Enable the function, and then click **Apply**.

Figure 4-29 Wi-Fi AP



Wi-Fi AP

Enable: on

SSID

Security: WPA2-Personal

Password

IP Address

4.7.4 Configuring Cloud Service

Procedure

Step 1 Log in to the webpage.

Step 2 Select **More** > **Communication Settings** > **Cloud Service**.

Step 3 Turn on the cloud service function.

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

Step 4 Click **Apply**.

4.7.5 Configuring Auto Registration

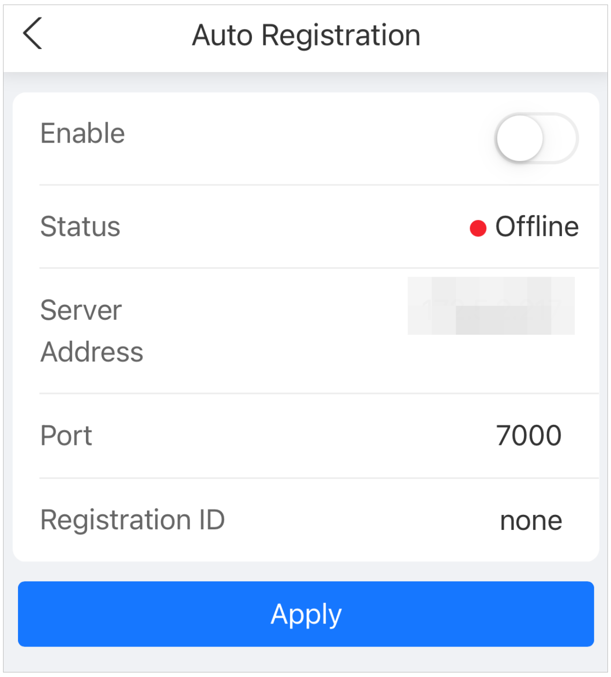
Procedure

Step 1 Log in to the webpage.

Step 2 Select **More** > **Network Setting** > **Auto Registration**.

Step 3 Enable the auto registration function, configure the parameters, and then click **Apply**.

Figure 4-30 Auto registration



Auto Registration

Enable

Status ● Offline

Server Address [redacted]

Port 7000

Registration ID none

Table 4-12 Automatic registration description

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

4.7.6 Configuring Wiegand

Procedure

Step 1 Log in to the webpage.

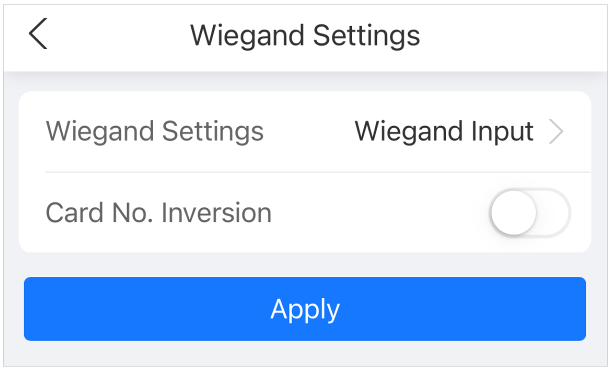
Step 2 Select **More** > **Communication Settings** > **Wiegand**.

Step 3 Select a Wiegand type, configure the parameters, and then click **Apply**.

- Select **Wiegand Input** when you connect an external card reader to the Device.

  When the Device connects to a third-party device through the Wiegand input port, and the card number read by the Device is in the reverse order from the actual card number. In this case, you can turn on **Card No. Inversion** function.

Figure 4-31 Wiegand input

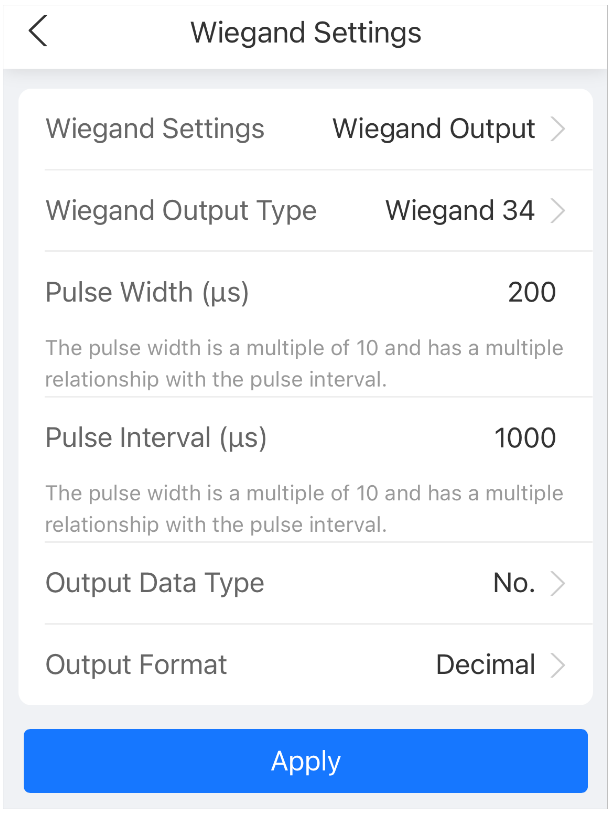


Wiegand Settings: Wiegand Input

Card No. Inversion

- Select **Wiegand Output** when the Device functions as a card reader, and you need to connect it to another access controller.

Figure 4-32 Wiegand output



Wiegand Settings: Wiegand Output

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.

Output Data Type: No.

Output Format: Decimal

Table 4-13 Description of Wiegand output

Parameter	Description
Wiegand Output Type	Select a Wiegand format to read card numbers or ID numbers. ◇ **Wiegand26** : Reads 3 bytes or 6 digits. ◇ **Wiegand34** : Reads 4 bytes or 8 digits. ◇ **Wiegand66** : Reads 8 bytes or 16 digits.
Pulse Width	Enter the pulse width and pulse interval of Wiegand output.
Pulse Interval	

Parameter	Description
Output Data Type	Select the type of output data. ◇ **No.** : Outputs data based on user ID. The data format is hexadecimal or decimal. ◇ **Card Number** : Outputs data based on user's first card number.

4.7.7 Configuring RS-485

Configure the RS-485 parameters if you connect an external device to the RS-485 port.

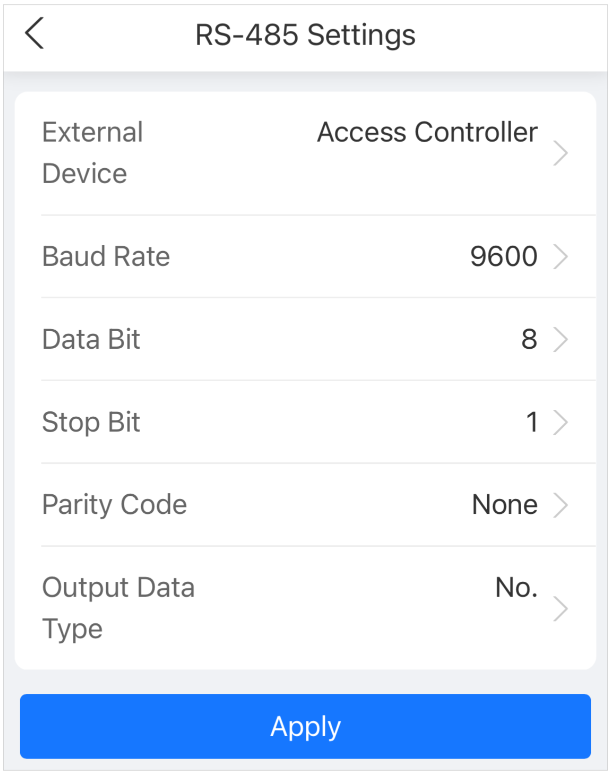
Procedure

Step 1 Log in to the webpage.

Step 2 Select **More** > **Communication Settings** > **RS-485 Settings**.

Step 3 Configure the parameters, and then click **Apply**.

Figure 4-33 RS-485 settings



RS-485 Settings

External Device: Access Controller

Baud Rate: 9600

Data Bit: 8

Stop Bit: 1

Parity Code: None

Output Data Type: No.

Table 4-14 Description of RS-485 parameters

Parameter	Description
External Device	● Access Controller Select **Access Controller** when the Device functions as a card reader, and sends data to other external access controllers to control access. ● Card Reader: The Device functions as an access controller, and connects to an external card reader. ● Reader (OSDP): The Device is connected to a card reader based on OSDP protocol. ● Door Control Security: The door exit button, lock and fire linkage is not effective after the security module is enabled.
Baud Rate	Select the baud rate. It is 9600 by default.
Data Bit	The number of bits used to transmit the actual data in a serial communication. It represents the binary digits that carry the information being transmitted.
Stop Bit	A bit sent after the data and optional parity bits to indicate the end of a data transmission. It allows the receiver to prepare for the next byte of data and provides synchronization in the communication protocol.
Parity Code	An additional bit sent after the data bits to detect transmission errors. It helps verify the integrity of the transmitted data by ensuring a specific number of logical high or low bits.
Output Data Type	When you configure the external device as **Access Controller**. ● 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. ● No.: Outputs data based on the user ID.

4.8 Configuring Audio Prompts

Set audio prompts during identity verification.

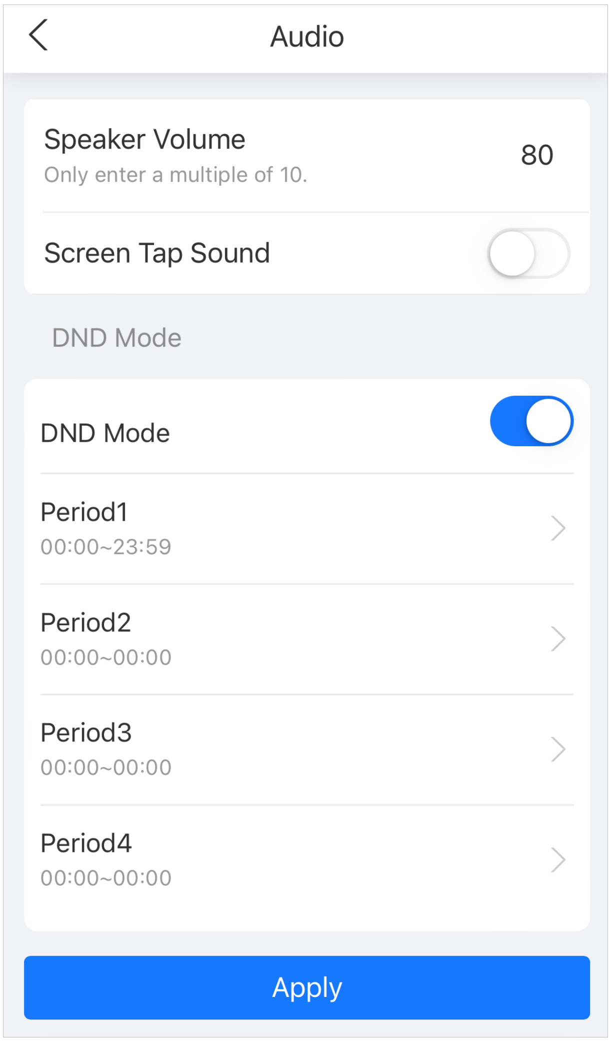
Procedure

Step 1 Log in to the webpage.

Step 2 Select **More** > **Audio and Video Config** > **Audio**.

Step 3 Configure the audio parameters, and then click **Apply**.

Figure 4-34 Configure the audio parameters



Audio

Speaker Volume 80

Only enter a multiple of 10.

Screen Tap Sound ○

DND Mode

DND Mode ●

Period1 00:00~23:59

Period2 00:00~00:00

Period3 00:00~00:00

Period4 00:00~00:00

Table 4-15 Parameters description

Parameters	Description
Speaker Volume	Set the volume of the speaker.
Screen Tap Sound	When this function is enabled, the device will produce sound when pressing the button.
DND Mode	No voice prompts during the set time when you verify your identity on the Device. You can set up to 4 periods.

4.9 Viewing Logs

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

4.9.1 System Logs

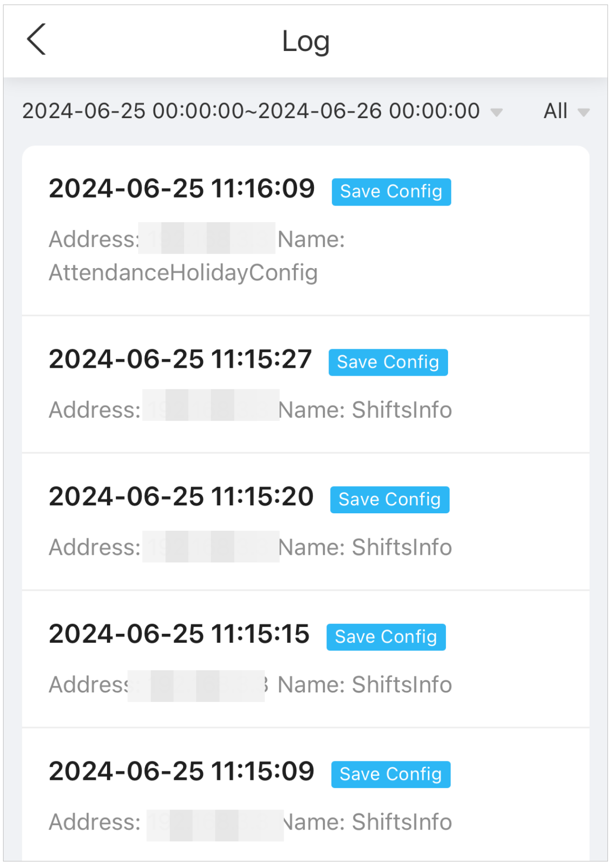
View and search for system logs.

Procedure

Step 1 Log in to the webpage.

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

Figure 4-35 Logs



Log

2024-06-25 00:00:00~2024-06-26 00:00:00 All

2024-06-25 11:16:09 Save Config
Address: [redacted] Name: AttendanceHolidayConfig

2024-06-25 11:15:27 Save Config
Address: [redacted] Name: ShiftsInfo

2024-06-25 11:15:20 Save Config
Address: [redacted] Name: ShiftsInfo

2024-06-25 11:15:15 Save Config
Address: [redacted] Name: ShiftsInfo

2024-06-25 11:15:09 Save Config
Address: [redacted] Name: ShiftsInfo

4.9.2 Unlock Records

Search for unlock records.

Procedure

Step 1 Log in to the webpage.

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

Step 3 Click the record to view the details.

4.9.3 Alarm Logs

View alarm logs.

Procedure

Step 1 Log in to the webpage.

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

5 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.

5.1 Installing and Logging In

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

Procedure

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

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

📖

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

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

5.2 Adding Devices

You need to add the Device to Smart PSS Lite. You can add them in batches or individually.

5.2.1 Adding Device One by One

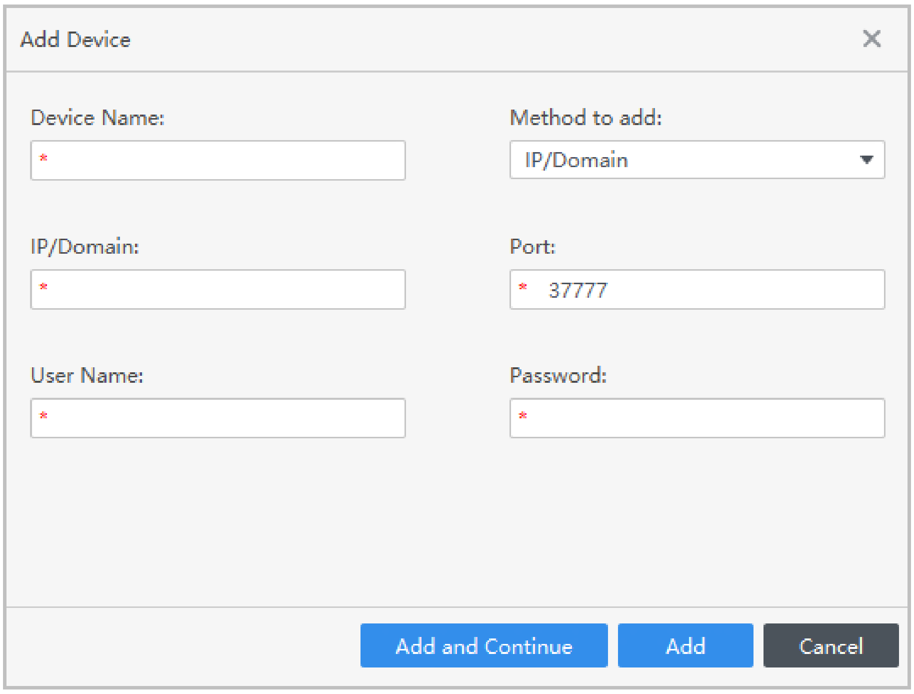
You can add devices one by one through entering their IP addresses or domain names.

Procedure

Step 1 On the **Device Manager** page, click **Add**.

Step 2 Configure the information of the device.

Figure 5-1 Add devices



Add Device

Device Name: *

Method to add: IP/Domain

IP/Domain: *

Port: * 37777

User Name: *

Password: *

Table 5-1 Parameters of IP adding

Parameter	Description
Device Name	We recommend you name devices with the monitoring area for easy identification.
Method to add	Select **IP/Domain**. ● IP/Domain: Enter the IP address or domain name of the device. ● SN: Enter the serial number of the device.
Port	Enter the port number, and the port number is 37777 by default. The actual port number might differ according to different models.
User Name	Enter the username of the device.
Password	Enter the password of the device.

Step 3 Click **Add**.

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

5.2.2 Adding Devices in Batches

Background Information

- We recommend you add devices by automatically search when you need to add devices in batches within the same network segment, or when the network segment is known but the exact IP addresses of devices are not known.
- Close ConfigTool and DSS when you configure devices; otherwise, you may not be able to find all devices.

Procedure

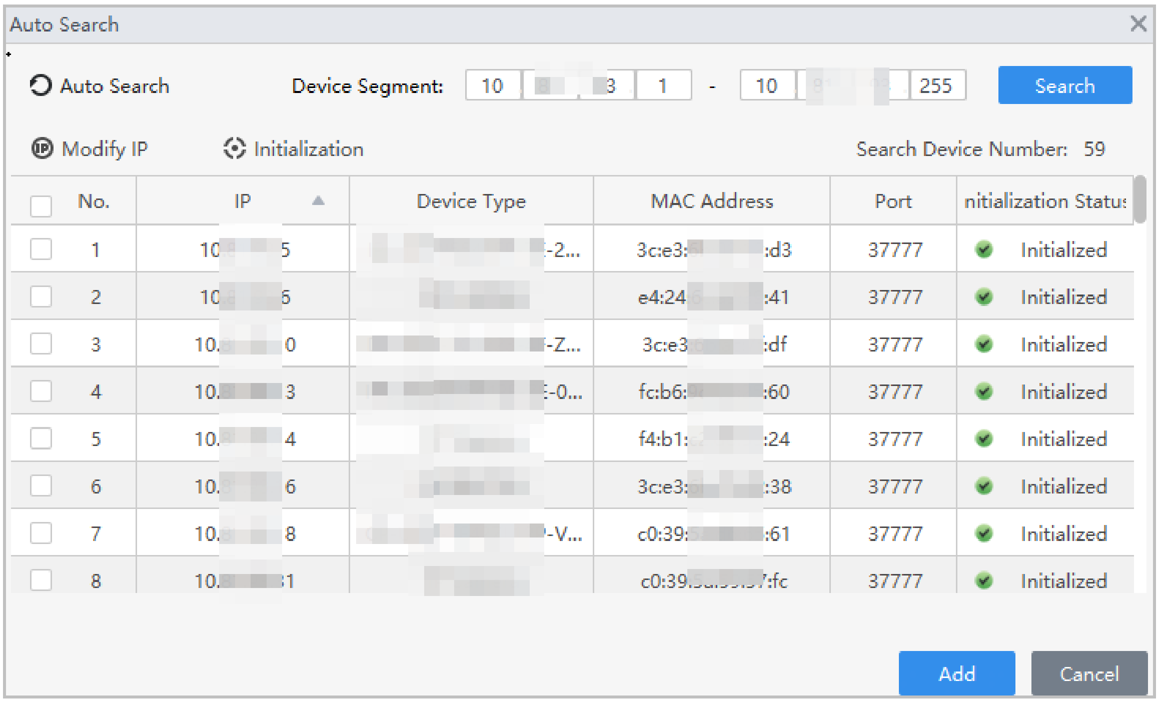
Step 1 On the **Device Manager** page, click **Auto Search**.

Step 2 Select a search method.

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

You can select both methods for the system to automatically search for devices on the network your computer is connected to and other networks.

Figure 5-2 Search for devices



Auto Search ✕

Auto Search   Device Segment: 10 [redacted] 3 1 - 10 [redacted] 255   Search

Modify IP   Initialization   Search Device Number: 59

☐	No.	IP	Device Type	MAC Address	Port	nitialization Statu:
☐	1	10[redacted]5	[redacted]-2...	3c:e3:[redacted]:d3	37777	✓ Initialized
☐	2	10[redacted]5	[redacted]	e4:24[redacted]:41	37777	✓ Initialized
☐	3	10.[redacted]0	[redacted]-Z...	3c:e3[redacted]:df	37777	✓ Initialized
☐	4	10.[redacted]3	[redacted]-0...	fc:b6:[redacted]:60	37777	✓ Initialized
☐	5	10.[redacted]4	[redacted]	f4:b1:[redacted]:24	37777	✓ Initialized
☐	6	10.[redacted]6	[redacted]	3c:e3:[redacted]:38	37777	✓ Initialized
☐	7	10.[redacted]8	[redacted]-V...	c0:39:[redacted]:61	37777	✓ Initialized
☐	8	10.[redacted]1	[redacted]	c0:39[redacted]:fc	37777	✓ Initialized

Add   Cancel

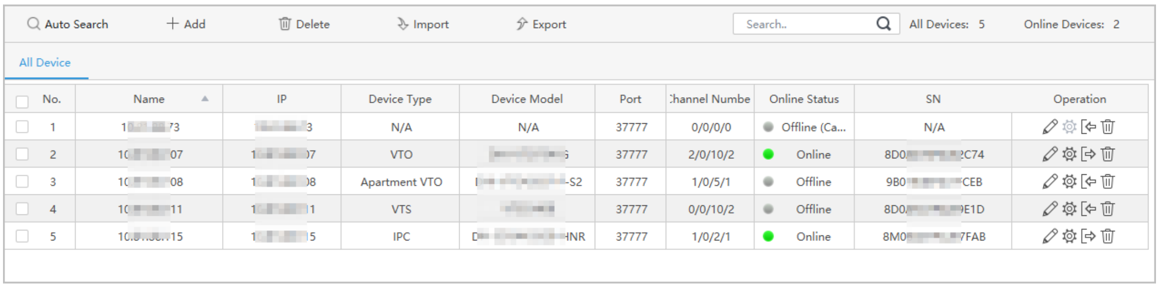
Step 3 Click devices, and then click **Add**.

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

Results

After the devices are successfully added, they are displayed on this page.

Figure 5-3 Added devices



Auto Search   + Add   Delete   Import   Export   Search..   All Devices: 5   Online Devices: 2

All Device

☐	No.	Name	IP	Device Type	Device Model	Port	:hannel Numbe	Online Status	SN	Operation
☐	1	1[redacted]73	[redacted]3	N/A	N/A	37777	0/0/0/0	● Offline (Ca...	N/A	
☐	2	10[redacted]07	1[redacted]07	VTO	[redacted]	37777	2/0/10/2	● Online	8D0[redacted]2C74	
☐	3	10[redacted]08	1[redacted]08	Apartment VTO	[redacted]-S2	37777	1/0/5/1	● Offline	9B0[redacted]CEB	
☐	4	10[redacted]11	1[redacted]1	VTS	[redacted]	37777	0/0/10/2	● Offline	8D0[redacted]9E1D	
☐	5	10[redacted]15	1[redacted]5	IPC	D[redacted]HNR	37777	1/0/2/1	● Online	8M0[redacted]7FAB	

5.3 User Management

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

5.3.1 Configuring Card Type

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

Procedure

Step 1 Log in to Smart PSS Lite.

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

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

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

Step 4 Click **OK**.

5.3.2 Adding Users

5.3.2.1 Adding Users One by One

Procedure

Step 1 Select **Personnel** > **Personnel Manager** > **Add**.

Step 2 Enter basic information of staff.

1. Select **Basic Info**.
2. Add basic information of staff.
3. Take snapshot or upload picture, and then click **Finish**.

> - The card number can be read automatically or filled in manually. To automatically read card number, select the card reader next to **Card No.**, and then place the card on the card reader. The card number will be read automatically.
> - You can select multiple USB cameras to snap pictures.

- Set password

  Click **Add** to add the password.
- Configure card

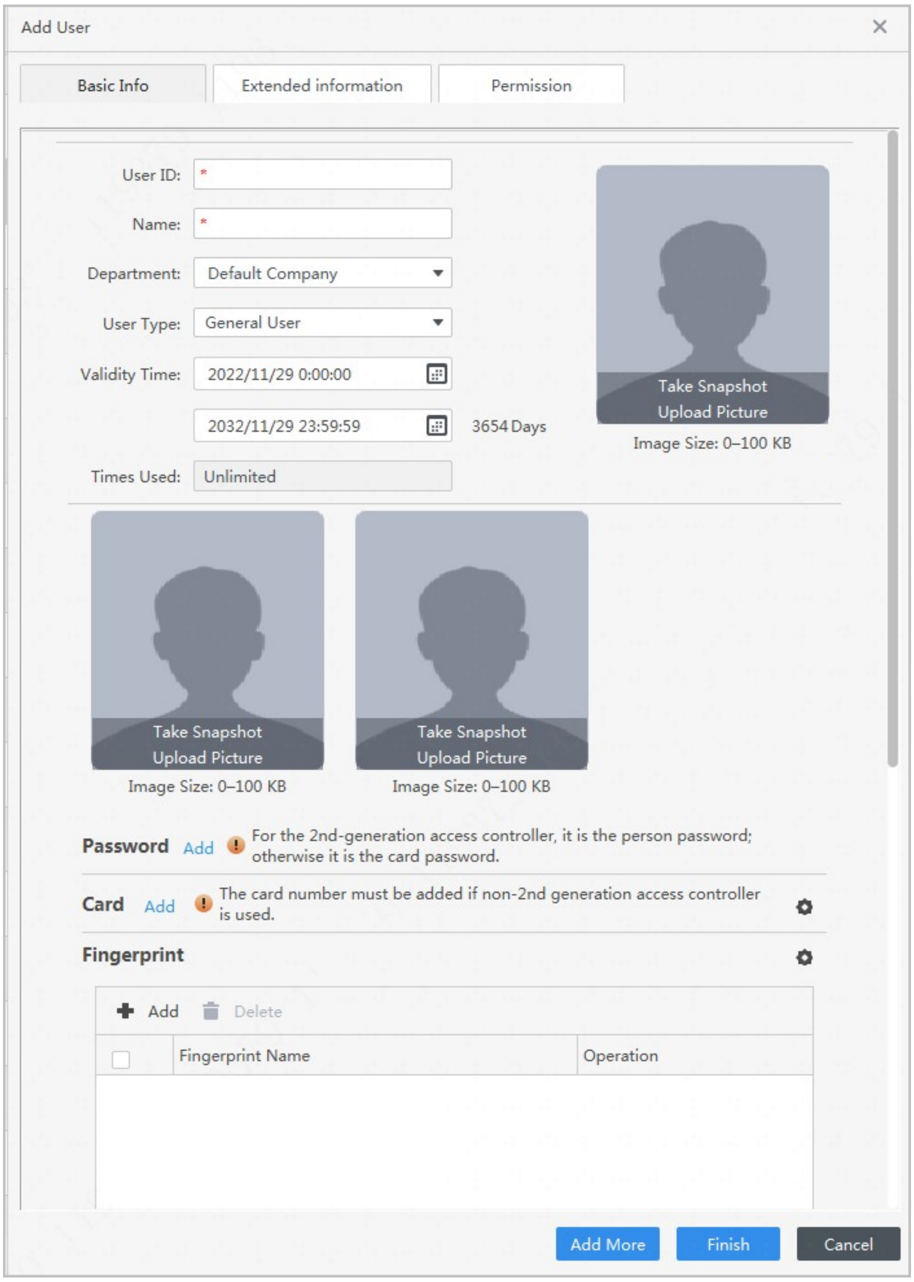
  a. Click ⚙ to select **Device** or **Card issuer** as card reader.
  b. Add cards.
  c. After adding, you can select the card as main card or duress card, or replace the card with a new one, or delete the card.
  d. Click ▦ to display the QR code of the card.

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

a. Click ⚙ to select **Device** or **Fingerprint Scanner** as the fingerprint collector.

b. Add fingerprint. Select **Add** > **Add Fingerprint**, and then press finger on the scanner for three times continuously.

Figure 5-4 Add basic information



Add User

User ID: *

Name: *

Department: Default Company

User Type: General User

Validity Time: 2022/11/29 0:00:00

2032/11/29 23:59:59 3654 Days

Times Used: Unlimited

Image Size: 0–100 KB

Password Add For the 2nd-generation access controller, it is the person password; otherwise it is the card password.

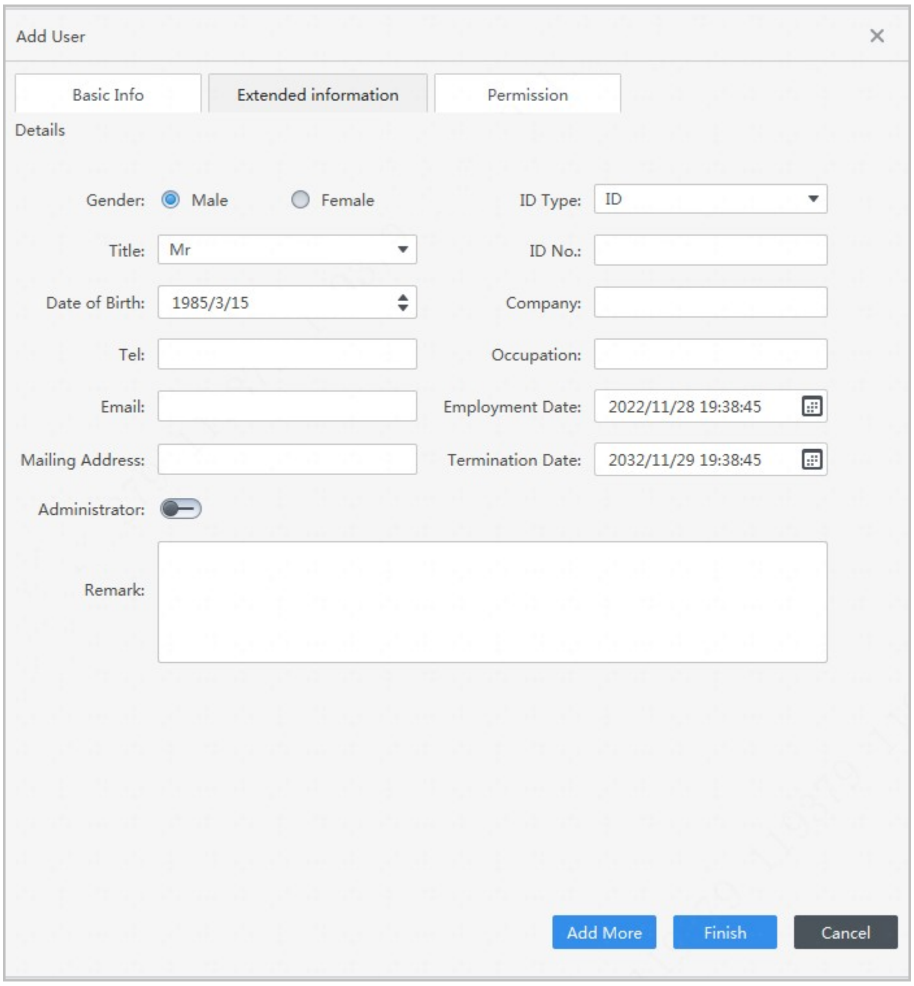
Card Add The card number must be added if non-2nd generation access controller is used.

Fingerprint

□	Fingerprint Name	Operation

Step 3 Click **Extended information** to add extended information of the personnel, and then click **Finish** to save.

Figure 5-5 Add extended information



Gender: ● Male ○ Female

Title: Mr

Date of Birth: 1985/3/15

Tel:

Email:

Mailing Address:

Administrator:

Remark:

ID Type: ID

ID No.:

Company:

Occupation:

Employment Date: 2022/11/28 19:38:45

Termination Date: 2032/11/29 19:38:45

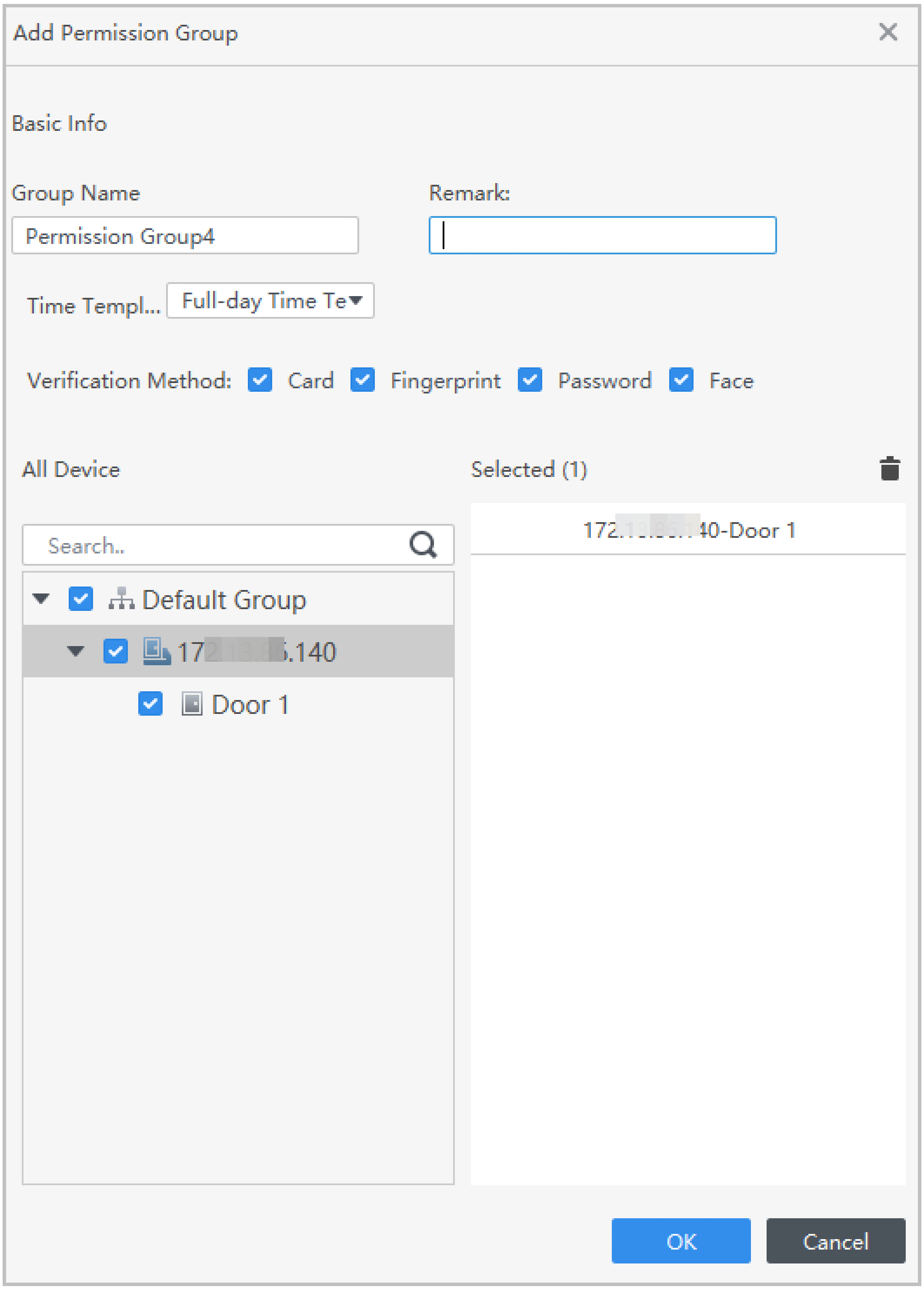
Step 4 Configure permissions.

1. Click + .
2. Enter the group name, remarks (optional), and select a time template.
3. Select verification methods and doors.

Step 5 Configure permissions. For details, see "5.3.3 Assigning Access Permission".

1. Select **Group**.
2. Enter the group name, remarks (optional), and select a time template.
3. Select verification methods and doors.
4. Click **OK**.

Figure 5-6 Configure permission groups



Add Permission Group

Basic Info

Group Name: Permission Group4

Remark:

Time Templ...: Full-day Time Te

Verification Method: ☑ Card ☑ Fingerprint ☑ Password ☑ Face

All Device

Search..

- ☑ Default Group
  - ☑ 17[redacted].140
    - ☑ Door 1

Selected (1)

172.[redacted]40-Door 1

Step 6 Click **Finish**.

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

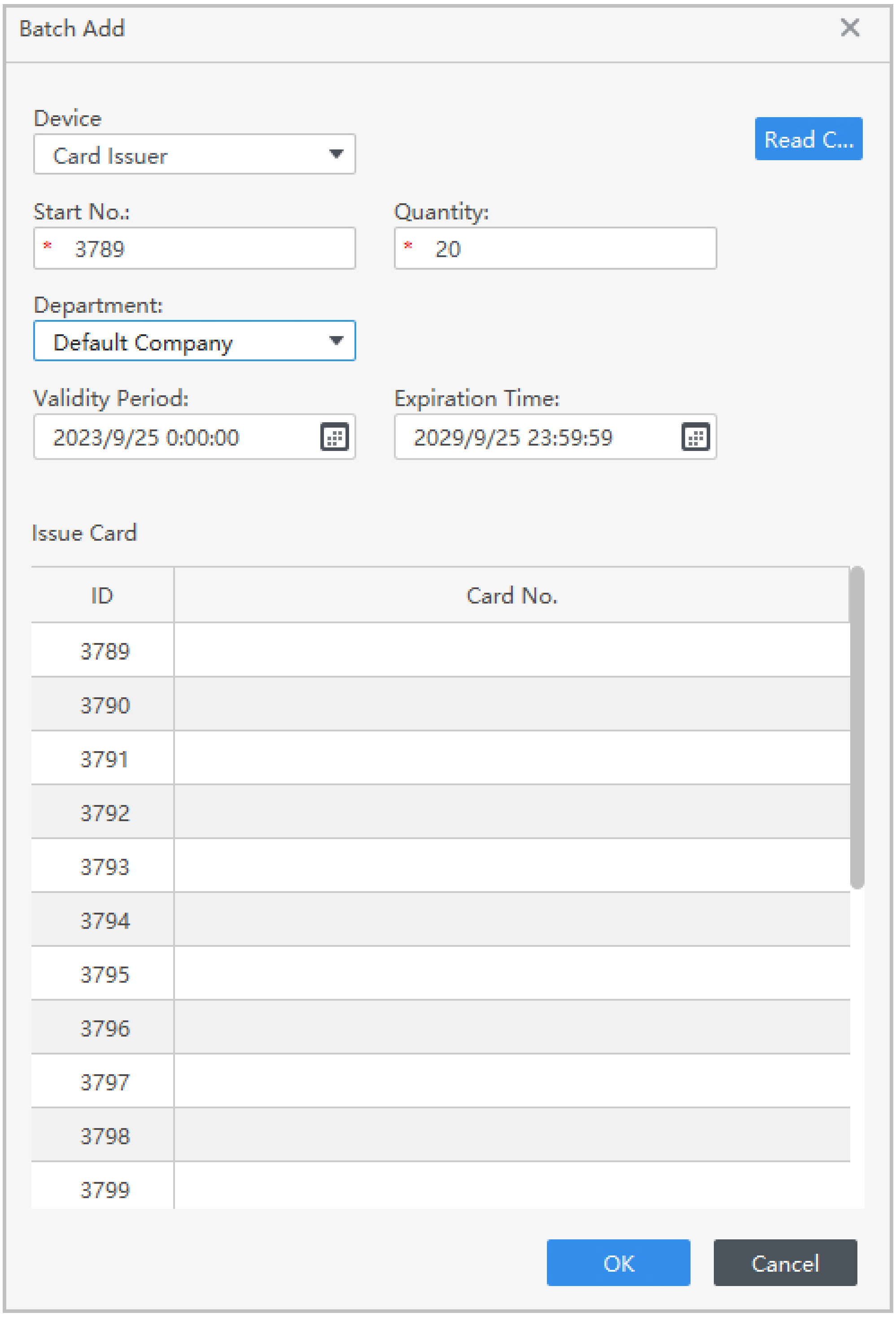
5.3.2.2 Adding Users in Batches

Procedure

Step 1 Click **Personnel Manger** > **Batch Update** > **Batch Add**.

Step 2 Select **Card issuer** or **Device** from the **Device** list, and then configure the parameters.

Figure 5-7 Add users in batches



Batch Add

Device: Card Issuer

Start No.: * 3789

Quantity: * 20

Department: Default Company

Validity Period: 2023/9/25 0:00:00

Expiration Time: 2029/9/25 23:59:59

Issue Card

ID	Card No.
3789	
3790	
3791	
3792	
3793	
3794	
3795	
3796	
3797	
3798	
3799	

Table 5-2 Add users in batches parameters

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

Step 3 Click **Read Card No.**, and swipe cards on the card reader.

The card number will be read automatically.

Step 4 Click **OK**.

5.3.3 Assigning Access Permission

Create a permission group that is a collection of door access permissions, and then link users with the group so that users can unlock doors associated with the permission group.

Procedure

Step 1 Click **Access Solution** > **Personnel Manger** > **Permission**.

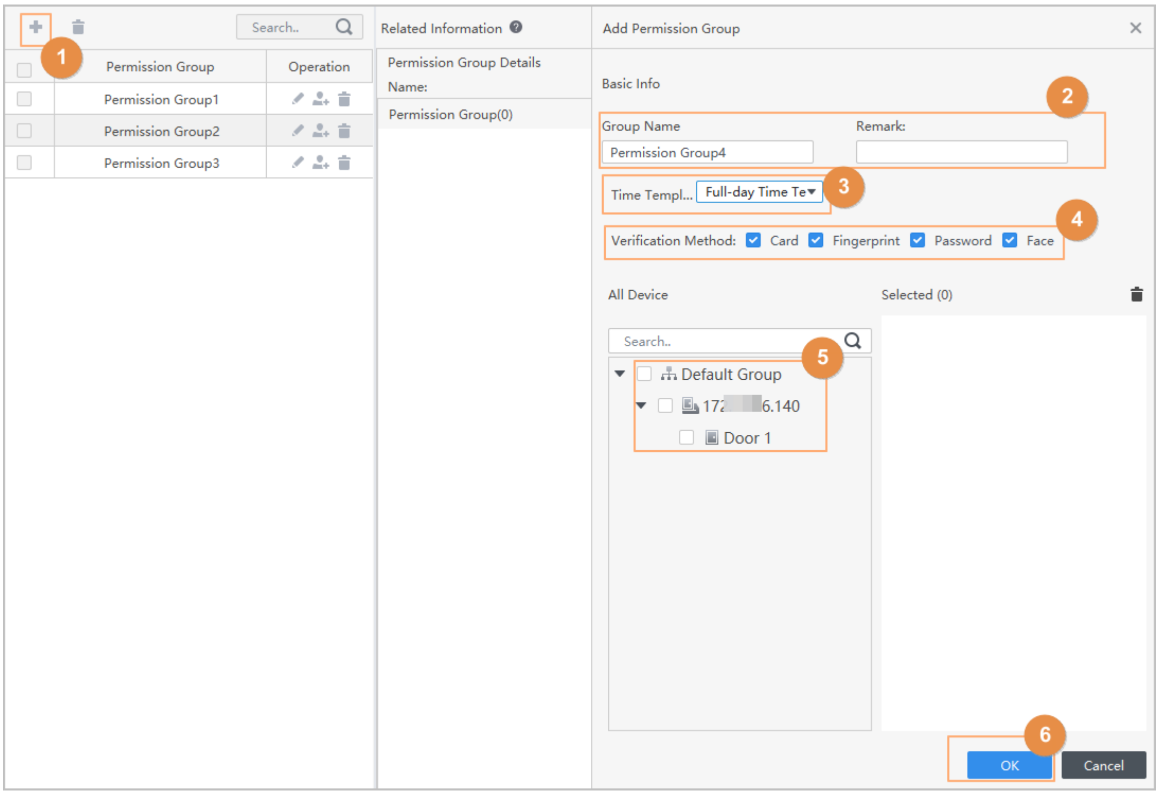
Step 2 Click + .

Step 3 Enter the group name, remarks (optional), and select a time template.

Step 4 Select verification methods and doors.

Step 5 Click **OK**.

Figure 5-8 Create a permission group



Permission Group	Operation
Permission Group1	
Permission Group2	
Permission Group3	

Related Information

Permission Group Details

Name:

Permission Group(0)

Add Permission Group

Basic Info

Group Name: Permission Group4

Remark:

Time Templ...: Full-day Time Te

Verification Method: ☑ Card ☑ Fingerprint ☑ Password ☑ Face

All Device

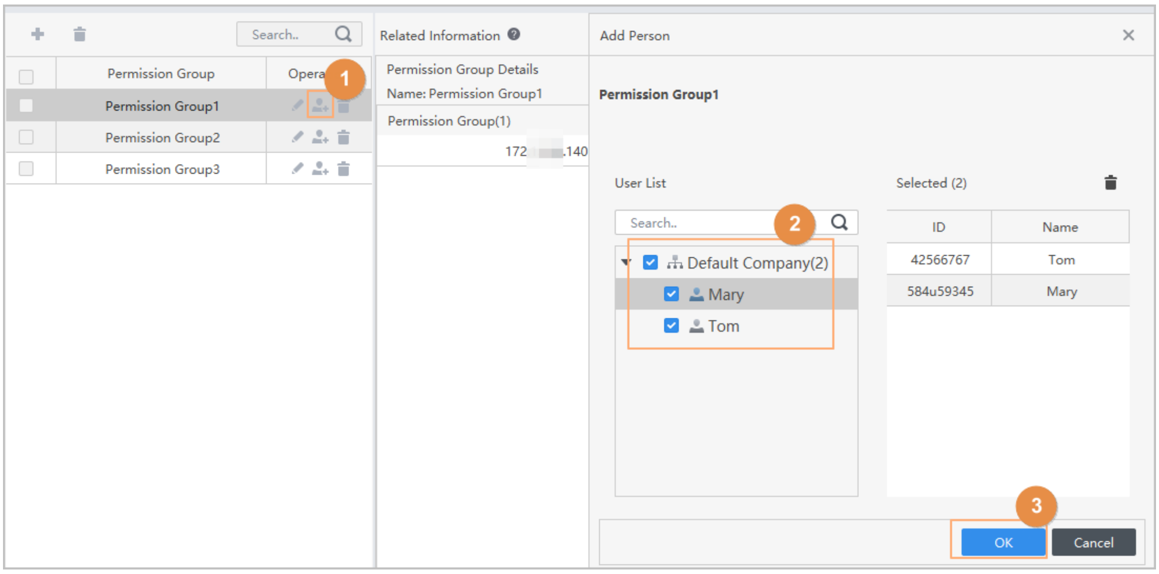
Selected (0)

- Default Group
  - 172 6.140
    - Door 1

Step 6 Click 👤+ of the permission group.

<u>Step 7</u> Select users to associate them with the permission group.

Figure 5-9 Add users to a permission group



ID	Name
42566767	Tom
584u59345	Mary

<u>Step 8</u> Click **OK**.

Users can unlock the door in this permission group after valid identity verification.

5.3.4 Assigning Attendance Permissions

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

Procedure

<u>Step 1</u> Log in to the Smart PSS Lite.

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

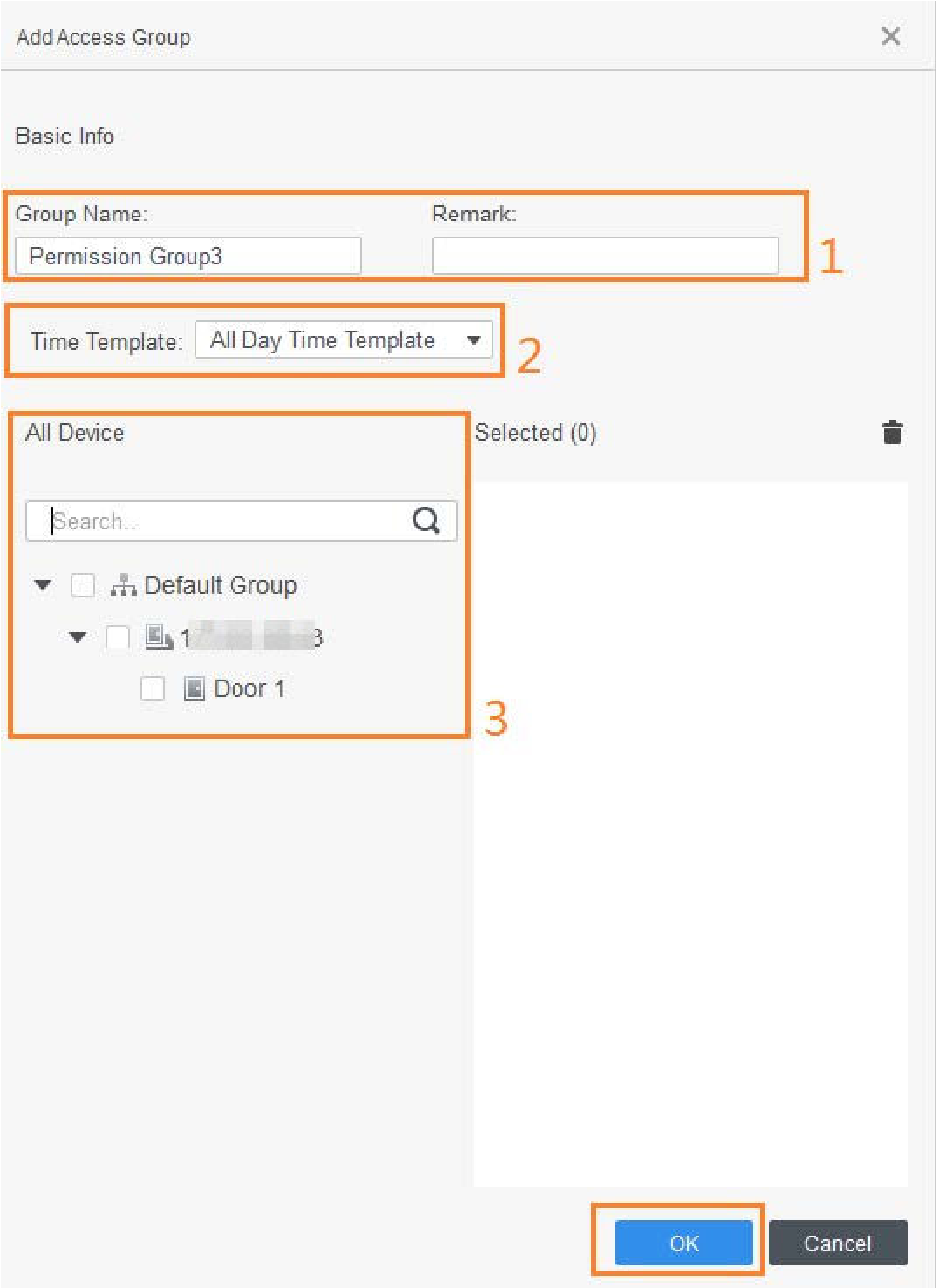
<u>Step 3</u> Click + .

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

<u>Step 5</u> Select the access control device.

<u>Step 6</u> Click **OK**.

Figure 5-10 Create a permission group



Add Access Group

Basic Info

Group Name: Permission Group3

Remark:

Time Template: All Day Time Template

All Device

Search...

Default Group

1[redacted]3

Door 1

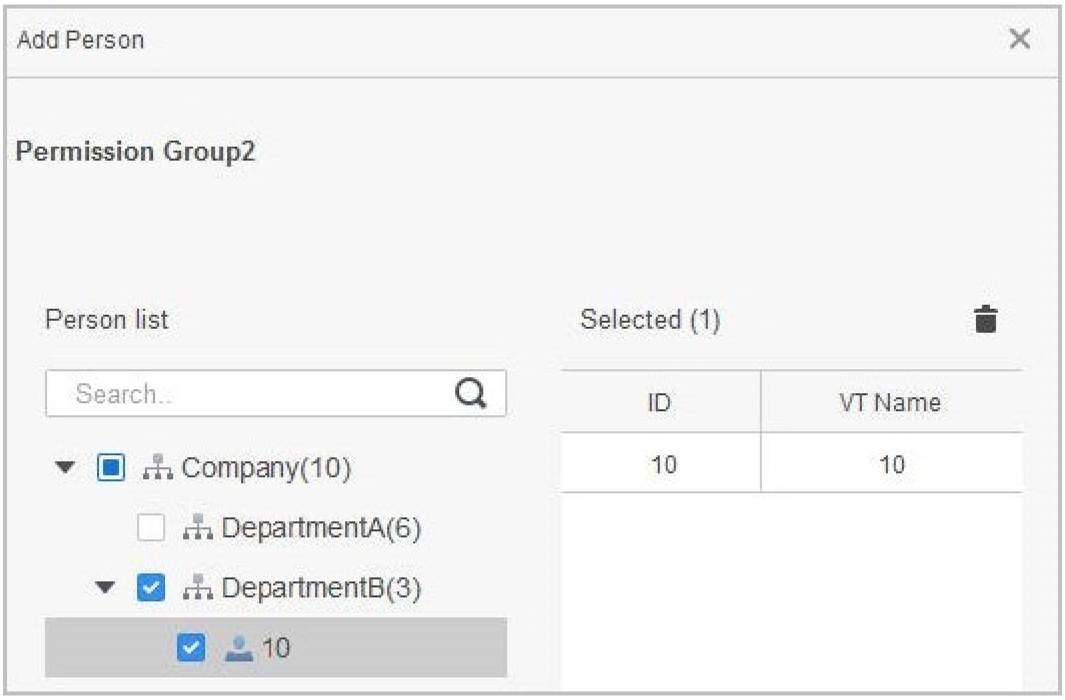
Selected (0)

- The Time & Attendance supports punch-in/out through password, face attendance, card and fingerprint attendance.
- Card and fingerprint attendance are available on select models.

Step 7 Click 👤 of the permission group you added.

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

Figure 5-11 Add users to a permission group



Add Person

Permission Group2

Person list

Search..

- ▪ Company(10)
  - □ DepartmentA(6)
  - ☑ DepartmentB(3)
    - ☑ 10

Selected (1)

ID	VT Name
10	10

Step 9 Click **OK**.

5.4 Access Management

5.4.1 Remotely Opening and Closing Door

You can remotely monitor and control door through the platform. For example, you can remotely open or close the door.

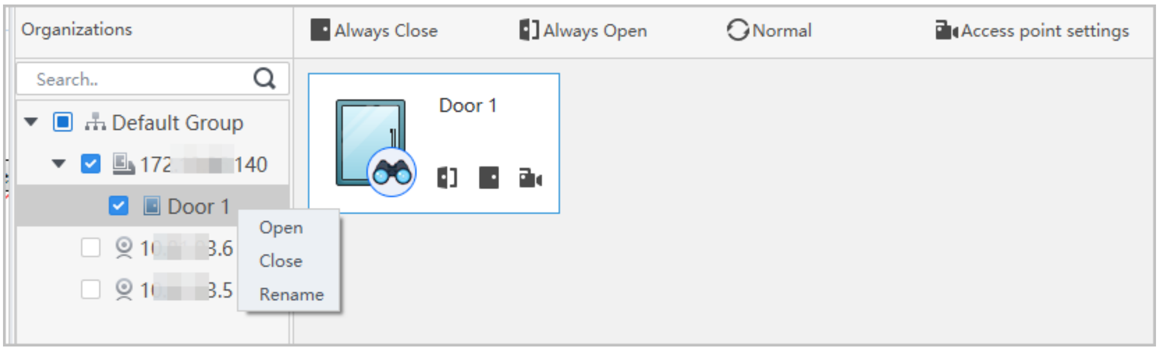
Procedure

Step 1 Click **Access Solution** > **Access Manager** on the home page.

Step 2 Remotely control the door.

- Select the door, right click and select **Open** or **Close** to open or close the door.

Figure 5-12 Open door



Organizations

Search..

- ▪ Default Group
  - ☑ 172[redacted]140
    - ☑ Door 1
  - □ 1[redacted]3.6
  - □ 1[redacted]3.5

- ▯ ■: Open or close the door.
- 🎥: View the live video of the door.

Related Operations

- Event filtering: Select the event type in the **Event Info**, and the event list displays the selected event type, such as alarm events and abnormal events.
- Event refresh locking: Click 🔓 to lock the event list, and then event list will stop refreshing. Click 🔒 to unlock.
- Event deleting: Click 🗑 to clear all events in the event list.

5.4.2 Setting Always Open and Always Close

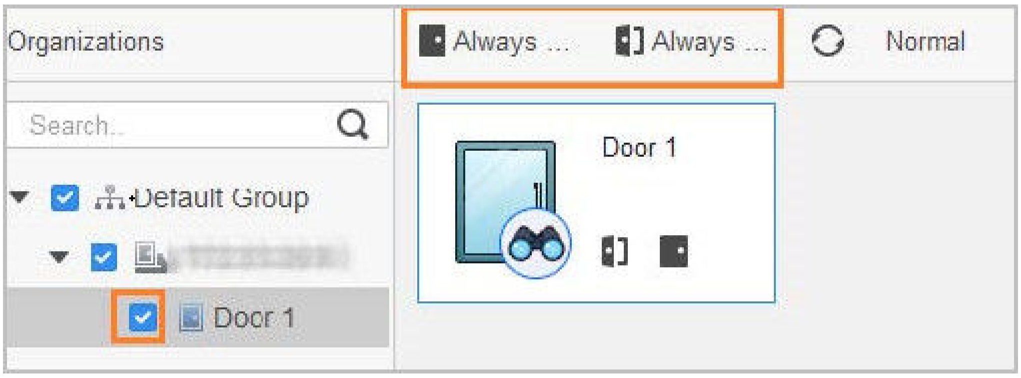
After setting always open or always close, the door remains open or closed all the time.

Procedure

Step 1 Click **Access Solution** > **Access Manager** on the Home page.

Step 2 Click **Always Open** or **Always Close** to open or close the door.

Figure 5-13 Always open or close



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

5.4.3 Monitoring Door Status

Procedure

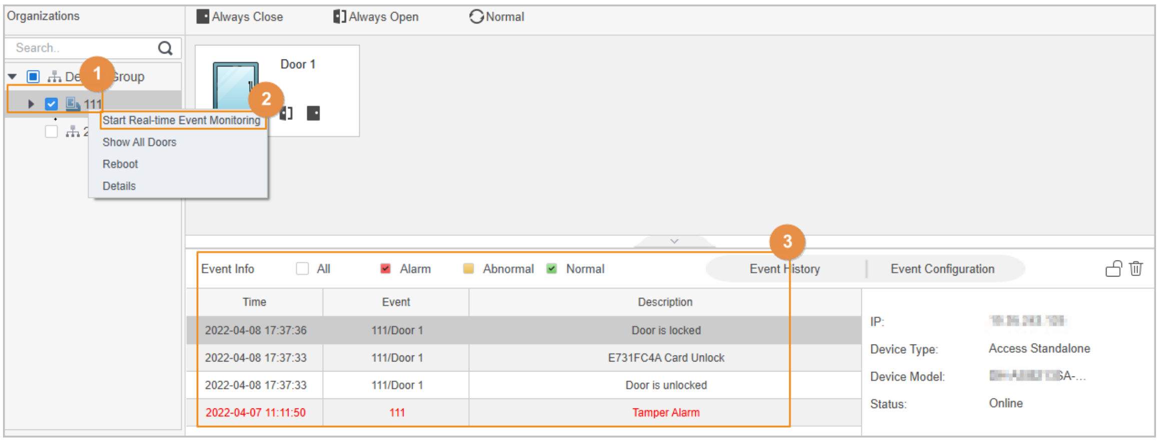
Step 1 Click **Access Solution** > **Access Manager** on the home page.

Step 2 Select the device in the device tree, and right click the device and then select **Start Real-time Event Monitoring**.

Real-time access control events will display in the event list.

Click **Stop Monitor**, real-time access control events will not display.

Figure 5-14 Monitor door status



Time	Event	Description
2022-04-08 17:37:36	111/Door 1	Door is locked
2022-04-08 17:37:33	111/Door 1	E731FC4A Card Unlock
2022-04-08 17:37:33	111/Door 1	Door is unlocked
2022-04-07 11:11:50	111	Tamper Alarm

IP:	[redacted]
Device Type:	Access Standalone
Device Model:	[redacted]SA-...
Status:	Online

Related Operations

- Show All Door: Displays all doors controlled by the Device.
- Reboot: Restart the Device.
- Details: View the device details, such as IP address, model, and status.

Appendix 1 Important Points of Face Registration

Before Registration

- Glasses, hats, and beards might influence face recognition performance.
- Do not cover your eyebrows when wearing hats.
- Do not change your beard style greatly if you use the Device; otherwise face recognition might fail.
- Keep your face clean.
- Keep the Device at least 2 meters away from light source and at least 3 meters away from windows or doors; otherwise backlight and direct sunlight might influence face recognition performance of the access controller.

During Registration

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

📖

- Do not shake your head or body, otherwise the registration might fail.
- Avoid 2 faces appear in the capture frame at the same time.

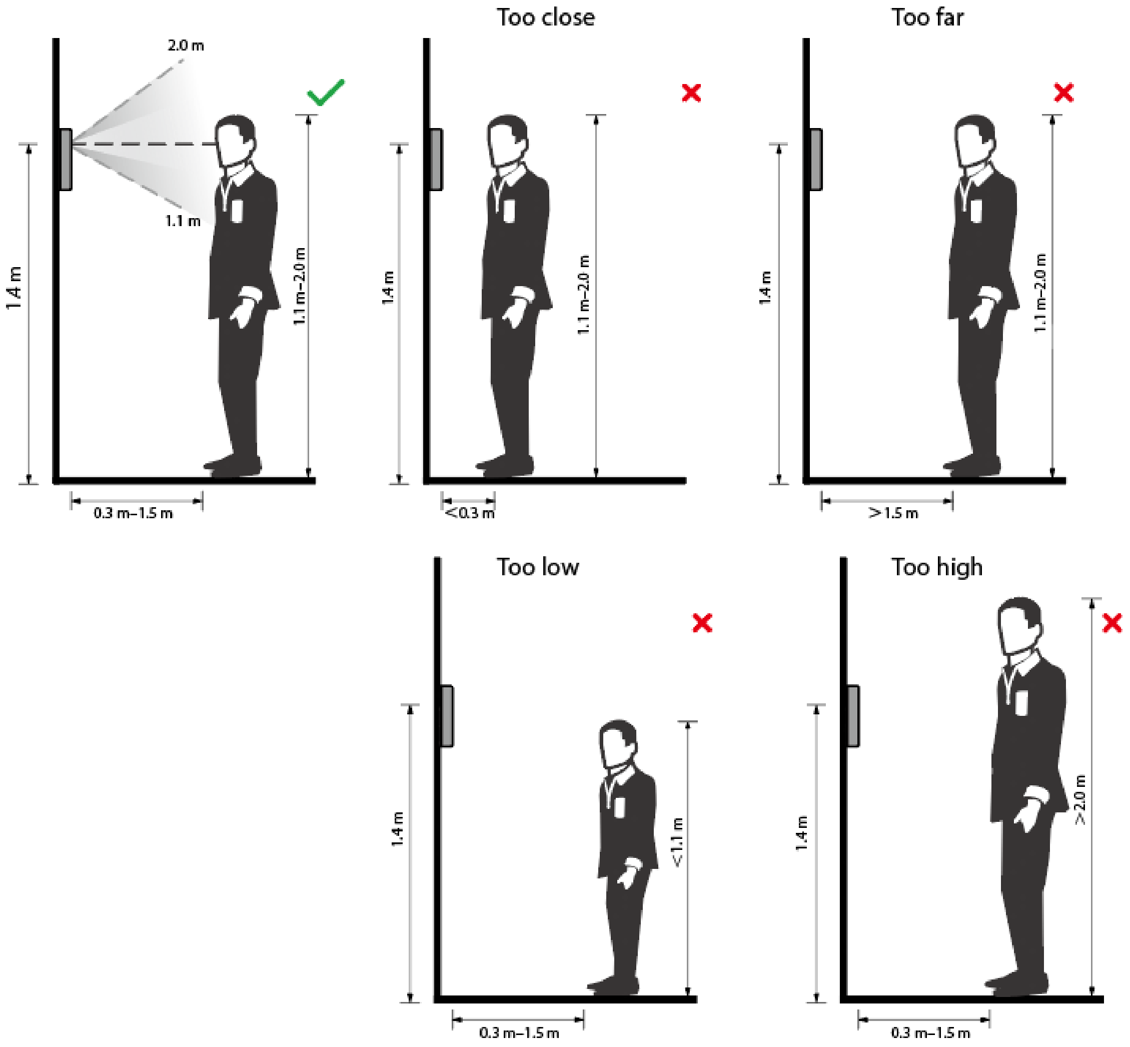
Face Position

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

📖

The face position below is for reference only, and might differ from the actual situation.

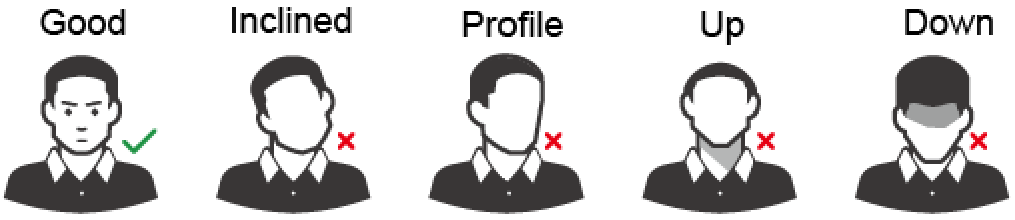
Appendix Figure 1-1 Appropriate face position



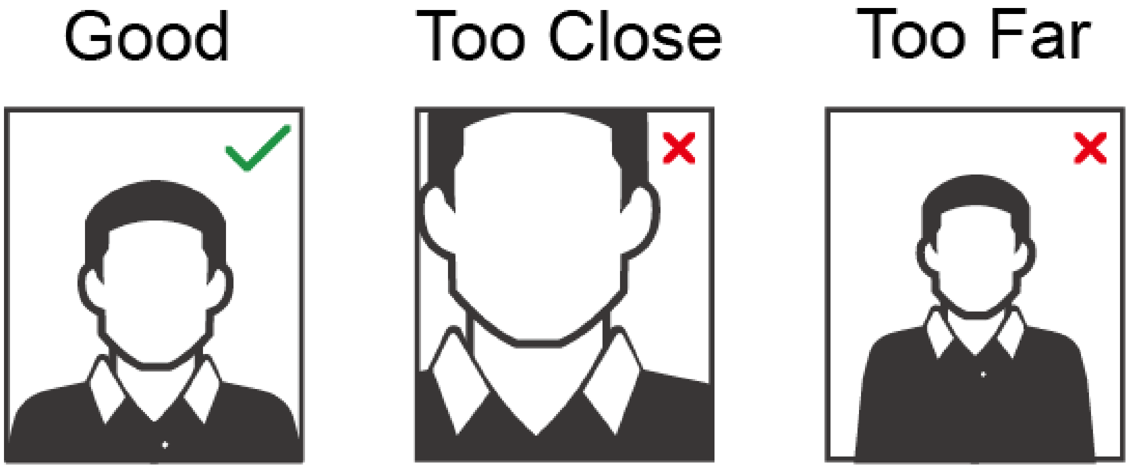
Requirements of Faces

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

Appendix Figure 1-2 Head position



Appendix Figure 1-3 Face distance



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

Appendix 2 Important Points of Fingerprint Registration Instructions

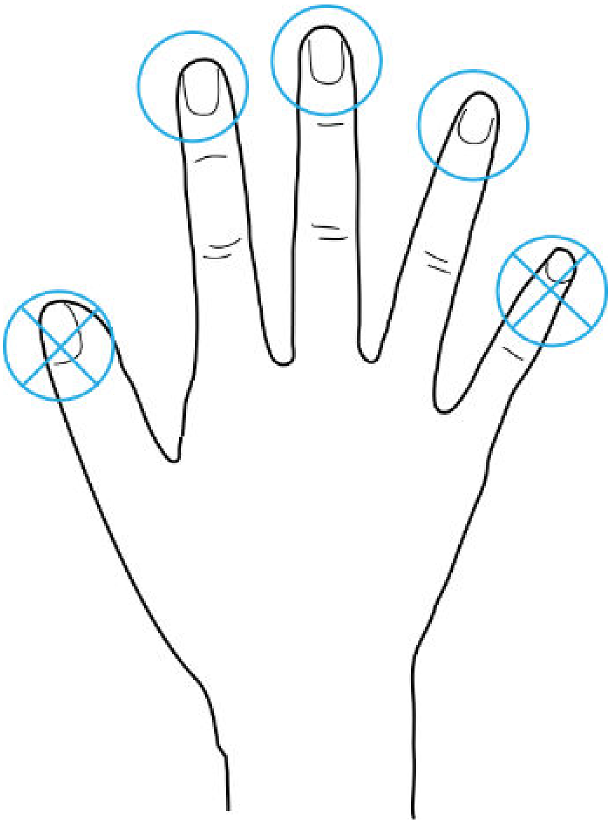
When you register the fingerprint, pay attention to the following points:

- 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

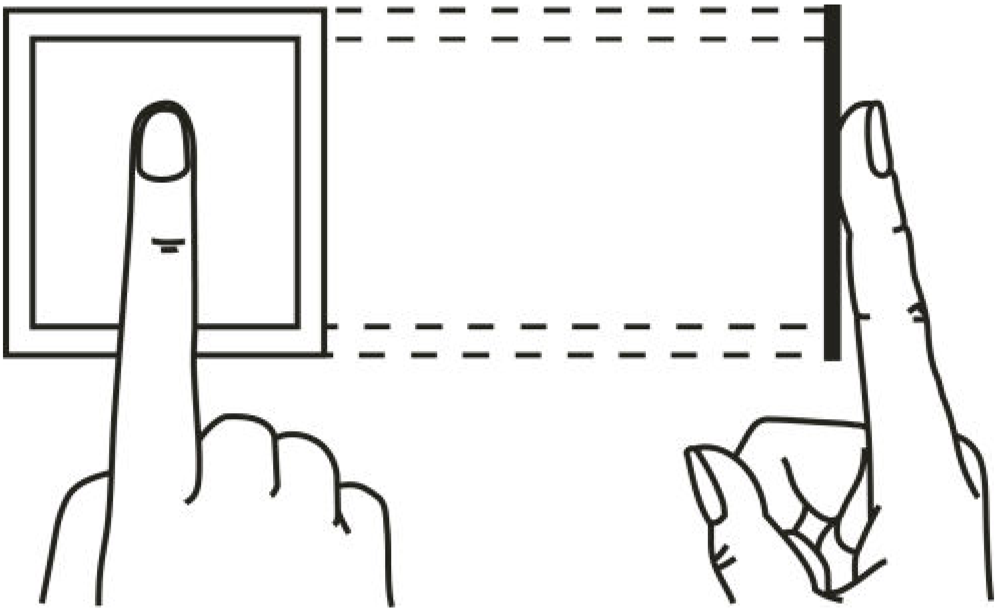
Forefingers, middle fingers, and ring fingers are recommended. Thumbs and little fingers cannot be put at the recording center easily.

Appendix Figure 2-1 Recommended fingers

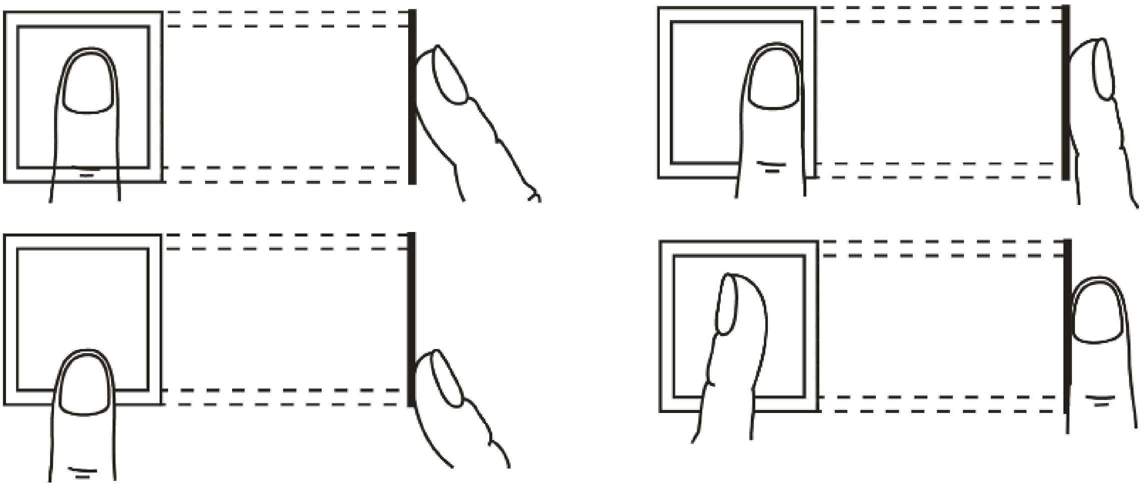


How to Press Your Fingerprint on the Scanner

Appendix Figure 2-2 Correct placement



Appendix Figure 2-3 Wrong placement



Appendix 3 Security Recommendation

Account Management

1. **Use complex passwords**

   Please refer to the following suggestions to set passwords:

   - The length should not be less than 8 characters;
   - Include at least two types of characters: upper and lower case letters, numbers and symbols;
   - Do not contain the account name or the account name in reverse order;
   - Do not use continuous characters, such as 123, abc, etc.;
   - Do not use repeating characters, such as 111, aaa, etc.
2. **Change passwords periodically**

   It is recommended to periodically change the device password to reduce the risk of being guessed or cracked.
3. **Allocate accounts and permissions appropriately**

   Appropriately add users based on service and management requirements and assign minimum permission sets to users.
4. **Enable account lockout function**

   The account lockout function is enabled by default. You are advised to keep it enabled to protect account security. After multiple failed password attempts, the corresponding account and source IP address will be locked.
5. **Set and update password reset information in a timely manner**

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

Service Configuration

1. **Enable HTTPS**

   It is recommended that you enable HTTPS to access web services through secure channels.
2. **Encrypted transmission of audio and video**

   If your audio and video data contents are very important or sensitive, it is recommended to use encrypted transmission function in order to reduce the risk of your audio and video data being eavesdropped during transmission.
3. **Turn off non-essential services and use safe mode**

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

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

   - SNMP: Choose SNMP v3, and set up strong encryption and authentication passwords.
   - SMTP: Choose TLS to access mailbox server.
   - FTP: Choose SFTP, and set up complex passwords.
   - AP hotspot: Choose WPA2-PSK encryption mode, and set up complex passwords.
4. **Change HTTP and other default service ports**

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

Network Configuration

1. **Enable Allow list**

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

   It is recommended that you bind the IP address of the gateway to the MAC address on the device to reduce the risk of ARP spoofing.
3. **Build a secure network environment**

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

   - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network;
   - According to the actual network needs, partition the network: if there is no communication demand between the two subnets, it is recommended to use VLAN, gateway and other methods to partition the network to achieve network isolation;
   - Stablish 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).