Access Standalone

User's Manual

V1.0.1

Foreword

General

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

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	Added initialization description.	December 2024
V1.0.0	First release.	August 2024

Privacy Protection Notice

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

About the Manual

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

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

Table of Contents

1 Overview

This product is an access control equipment integrating card reading, configuration and execution. The appearance of the product is simple and fashionable, and it is suitable for office buildings, schools, parks, communities, factories, public venues, business centers, government buildings and other application scenarios.

2 Local Operations

2.1 Initialization

After the Device is powered on for the first time, you need to set the administrator password. The administrator password is used to enter the main menu of the Device.

Procedure

Step 1 Power on the Device, and the indicator light will flash red slowly.

Step 2 Press **#** , enter the administrator password, and then press **#**.

The password must be 1 to 8 characters in length.

If the indicator light is solid blue, it means the Device is initialized.

After initialization, you can only use the functions on the Device. If you want to login to the webpage of the Device, initialize the Device on its webpage or through the ConfigTool.

Related Operations

- You can only set numbers as the admin account password when you initialize it through the Device.
- You can set numbers, letters and other characters as the admin account password when you initialize it through the platform of the ConfigTool.

After you complete the initialization on the Device, you can only perform operations on the Device itself. If you need to connect the Device to the network, use ConfigTool or the platform to initialize the Device.

When you use ConfigTool or the platform to initialize the Device, after configuring the network account and password, the device will automatically complete initialization and enter the standby status. The local admin password is converted from the network password. If the password exceeds 8 characters, only the first 8 characters are kept. The letters are converted into digits according to the E.161 standard. The password conversion is case-insensitive, and all other symbols are converted to 0.

- After the initialization, if you modify the network password, the local admin password will not be affected.
- If you initialize through the Device first, then initialize through the ConfigTool or the platform, the local admin password will not be affected.

Figure 2-1 E.161 (T9 keypad)

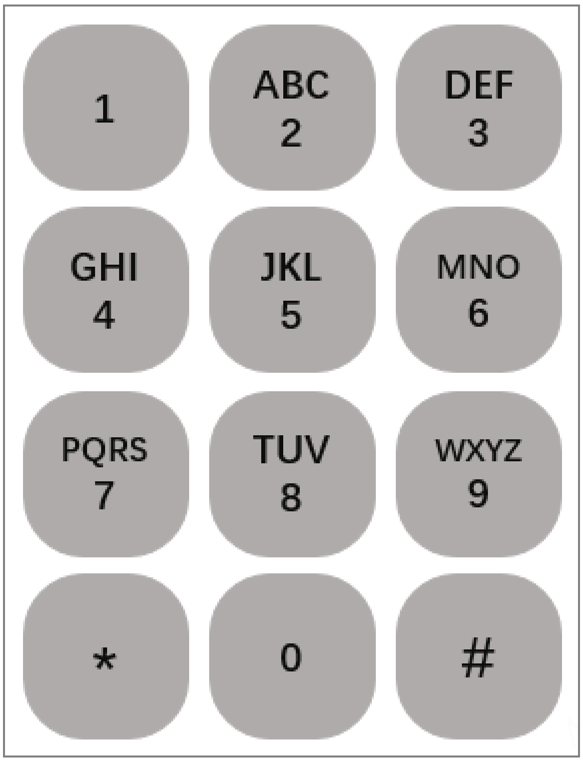


Table 2-1 Conversion example

Network Password	Local Admin Password
ABC12345	22212345
admin123	23646123
admin12!	23646120
admin123456	23646123

2.2 Main Menu

Entering Main Menu

Press **#** , enter the administrator password, and then press **#**.

- The indicator flashes blue, and it means you have entered the main menu.
- The indicator flashes red once, the buzzer beeps 3 times, and then the indicator turns solid blue, which means the password is wrong.

Related Prompts

- The indicator flashes green once, and the buzzer beeps once, which means that the operation or access control verification is successful.
- The indicator flashes red once, and the buzzer beeps 3 times, which means that the operation or access control verification failed.
- If the indicator flashes red slowly, it means the Device is not uninitialized.

- If the indicator is solid blue, it means the Device is in the standby status.
- The indicator flashes blue, it means the Device enters the main menu.
- The keypad is white when you operate the device. If there is no operation within 10 seconds, the light turns off and the Device exits the current screen.

2.3 User Management

2.3.1 Adding User

- You can add only one card, one password or one fingerprint for one user. At least one method of card, password, and fingerprint must be added.
- Fingerprint function is available on select models.

Procedure

Step 1 Press **#** , enter the administrator password, and then press **#**.

Enter the main menu, and the indicator flashes blue.

Step 2 Press **1** and **#** to add users.

Step 3 Enter the user ID, and then press **#**.

- If the indicator does not light up and the Device beeps, the user ID is added successfully.
- If the indicator flashes red and the Device beeps, you fail to add the user ID. The possible reason is the ID already exists. Please try the other ID.

You can only enter numbers for the ID on the Device.

Step 4 After swiping the card, press **#** to add the card.

If you do not need to add the card, press **#** to skip it.

Step 5 Enter the user password, and then press **#**.

If you do not need to set the user password, press **#** to skip it.

The password can be 1 to 8 characters in length.

Step 6 Add the fingerprint, and then press **#**.

If you do not need to set the fingerprint, press **#** to skip it.

This function is available on select models.

Step 7 Repeat Step 2 to Step 6 to add more users.

After adding the user, press ***** to return to the main menu, and then press ***** to return to the standby status.

2.3.2 Deleting User

Procedure

Step 1 Press **#** , enter the administrator password, and then press **#**.

Enter the main menu, and the indicator flashes blue.

Step 2 Press **2** and **#**.

Step 3 Delete a user.

- Swipe the card, and then press **#**.

  If you swipe a card that has not been added, the deletion fails.
- Enter the user ID, and then press **#**.

  If you enter the ID that has not been added, the deletion fails.
- Enter 0000, and then press **#** to delete all users.

After deletion, press * to return to the main menu, and then press * to exit the main menu.

2.4 Configuring Door Unlock Mode

Background Information

The fingerprint function is available on select models.

Procedure

Step 1 Press **#** , enter the administrator password, and then press **#**.

Enter the main menu and the indicator flashes blue.

Step 2 Press **3** and **#**.

Step 3 Select the unlock mode.

- Press **0** and **#** to set unlocking by card, password or fingerprint.

  Swipe the card, enter the password, or use the fingerprint to open the door. The password consists of the following methods.

  - ◇ On the standby screen, enter the user ID, press **#** , and the Device beeps once. Enter the password, and then press **#** to verify the identity.
  - ◇ On the standby screen, enter the public password, and then press **#** to verify the identity.
  - ◇ When the **PIN Code Authentication** is enabled on the webpage of the Device, people can verify the identity by simply entering the password.
  - ◇ When the Device is used with the DMSS app, the temporary password is supported and can be configured on the app.
- Press **1** and **#** to set unlocking by card and user password.

  Swipe the card first. After the Device beeps once, enter the password, and then press **#** to verify the identity.
- Press **2** and **#** to set unlocking by card and user password.

Swipe the card first. After the Device beeps once, press the fingerprint to verify the identity.

- Press **3** and **#** to set unlocking by card, password and fingerprint.

  Swipe the card first. After the Device beeps once, press the fingerprint. The Device beeps again. Enter the password, and then press **#** to verify the identity.

Step 4 Press ***** to exit the main menu.

2.5 Configuring Unlock Duration

The door remains open after a defined time after it unlocks, which allows people to pass through.

Procedure

Step 1 Press **#** , enter the administrator password, and then press **#**.

Enter the main menu and the indicator flashes blue.

Step 2 Press **4** and **#**.

Step 3 Enter the time, and then press **#**.

The value ranges from 1 second to 600 seconds. The default value is 3 seconds.

Step 4 Press ***** to exit the main menu.

2.6 Configuring Door Sensor

After the door sensor is enabled, the door timeout alarm is enabled at the same time by default. If the door stays open after the set door timeout period, the buzzer of the Device generates alarms.

Procedure

Step 1 Press **#** , enter the administrator password, and then press **#**.

Enter the main menu and the indicator flashes blue.

Step 2 Press **5** and **#**.

Step 3 Turn on or turn off the door sensor.

The door sensor is turned off by default.

- Press **0** and **#** to turn off the door sensor.
- Press **1** and **#** to turn on the door sensor.

Step 4 Press ***** to exit the main menu.

2.7 Password Management

- Administrator password: Used to enter the main menu of the Device.
- Public password: Used to verify the authentication to unlock the door.

2.7.1 Changing the Administrator Password

To ensure device security, we recommend that you change the administrator password from time to time.

Procedure

Step 1 Press **#** , enter the administrator password, and then press **#**.

Enter the main menu and the indicator flashes blue.

Step 2 Press **0** and **#**.

Step 3 Enter the new password, and then press **#**.

Step 4 Enter the new password again, and then press **#**.

- Flashing green means the password is modified successfully.
- Flashing red means that you fail to modify the password.
- After modification, the Device automatically exits the main menu, and the indicator turns solid blue. Enter the main menu using the new password if you modify the password successfully. Enter the main menu using the original password if you fail to modify the password.

2.7.2 Adding Public Password

Procedure

Step 1 Press **#** , enter the administrator password, and then press **#**.

Enter the main menu and the indicator flashes blue.

Step 2 Press **6** and **#**.

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

The password can be 1 to 8 characters in length.

You can add only one public password. If you repeat the operations, the new password will replace the original one.

Step 4 Press ***** to exit the main menu.

2.7.3 Deleting Public Password

Procedure

Step 1 Press **#** , enter the administrator password, and then press **#**.

Enter the main menu and the indicator flashes blue.

Step 2 Press **7** and **#**.

Step 3 Enter the public password and press **#**.

Step 4 Press ***** to exit the main menu.

2.8 Main Card Management

2.8.1 Adding Main Card

After adding the main card, you can quickly add and delete other user cards through the main card.

Background Information

The main card cannot be used to unlock the door.

Procedure

Step 1 Press **#** , enter the administrator password, and then press **#**.

Enter the main menu and the indicator flashes blue.

Step 2 Press **8** and **#**.

Step 3 Swipe the card, and then press **#**.

- If the indicator flashes green, and the Device beeps, it means the card is added as the main card.
- If the indicator flashes red, and the Device beeps, it means you fail to add the card as the main card.

🕮

- User cards that have been added can also be set as main card.
- If a user card is set to main card, it will not be able to unlock the door.
- Only supports one main card. If a new main card is added, the old main card will be overwritten.

Step 4 Press ***** to exit the main menu.

2.8.2 Deleting Main Card

Procedure

Step 1 Press **#** , enter the administrator password, and then press **#**.

Enter the main menu, and the indicator flashes blue.

Step 2 Press **9** and **#**.

Step 3 Swipe the card, and the press **#**.

Step 4 Press ***** to exit the main menu.

2.8.3 Managing User Cards through Main Card

If no operation is performed in 3 seconds after you swipe the main card, the Device enters the main card mode, and the Device will determine the corresponding function according to the swipe times of the main card. In the main card mode, the indicator flashes red and blue alternately, and if there is no operation for 10 seconds or you swipe the main card again for one time, it returns to the standby status.

- Add user card: Swipe the main card once, and then swipe the user card to add it. User cards can be added continuously.
- Delete the user card: Swipe the main card twice, and then swipe the user card to delete it. User cards can be deleted continuously.
- Clear all user cards: Swipe the main card 5 times in a row.

2.9 Configuring Door Timeout Period

After the door sensor is enabled, if the door stays open after the set time, the buzzer of the Device will give an alarm.

Procedure

Step 1 Press **#** , enter the administrator password, and then press **#**.

Enter the main menu and the indicator flashes blue.

Step 2 Press **10** and **#**.

Step 3 Enter the door timeout period, and then press **#**.

The value range is from 1 second to 9999 seconds. The default value is 60 seconds.

Step 4 Press ***** to exit the main menu.

2.10 Restoring to Factory Settings

Procedure

Step 1 Press **#** , enter the administrator password, and then press **#**.

Enter the main menu, and the indicator flashes blue.

Step 2 Press **11** and **#**.

Step 3 Restore the Device to factory settings.

- Press **00** and **#** to restore factory settings (retain user information).
- Press **000** and **#** to restore factory settings (restore all information).

Related Operations

You can use the reset button to restore the Device to factory settings.

3 Webpage Operations

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

Web configurations differ depending on models of the Device.

3.1 Initialization

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

Prerequisites

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

Procedure

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

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

Step 2 Select a language for the Device.

Step 3 Set the password and email address according to the screen instructions.

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

Related Operations

- You can only set numbers as the admin account password when you initialize it through the Device.
- You can set numbers, letters and other characters as the admin account password when you initialize it through the platform of the ConfigTool.

After you complete the initialization on the Device, you can only perform operations on the Device itself. If you need to connect the Device to the network, use ConfigTool or the platform to initialize the Device.

When you use ConfigTool or the platform to initialize the Device, after configuring the network account and password, the device will automatically complete initialization and enter the standby status. The local admin password is converted from the network password. If the password exceeds 8 characters, only the first 8 characters are kept. The letters are converted into digits according to the E.161 standard. The password conversion is case-insensitive, and all other symbols are converted to 0.

- After the initialization, if you modify the network password, the local admin password will not be affected.
- If you initialize through the Device first, then initialize through the ConfigTool or the platform, the local admin password will not be affected.

Figure 3-1 E.161 (T9 keypad)

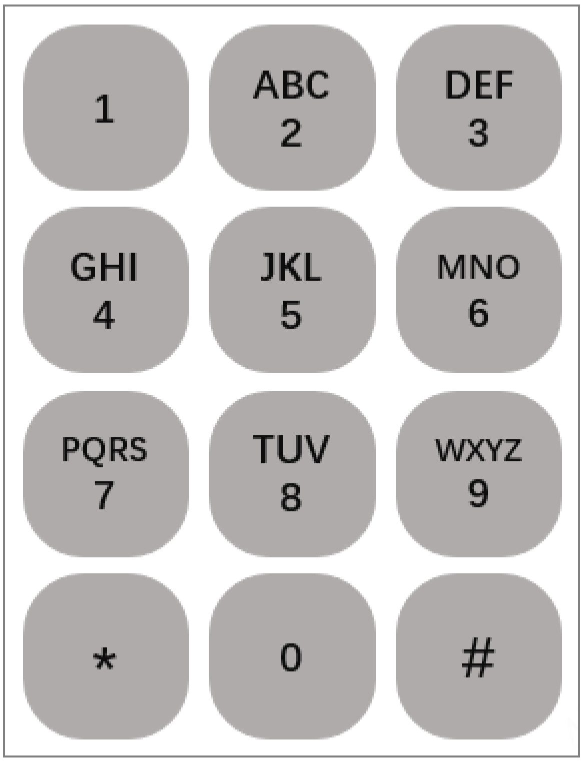


Table 3-1 Conversion example

Network Password	Local Admin Password
ABC12345	22212345
admin123	23646123
admin12!	23646120
admin123456	23646123

3.2 Resetting the Password

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

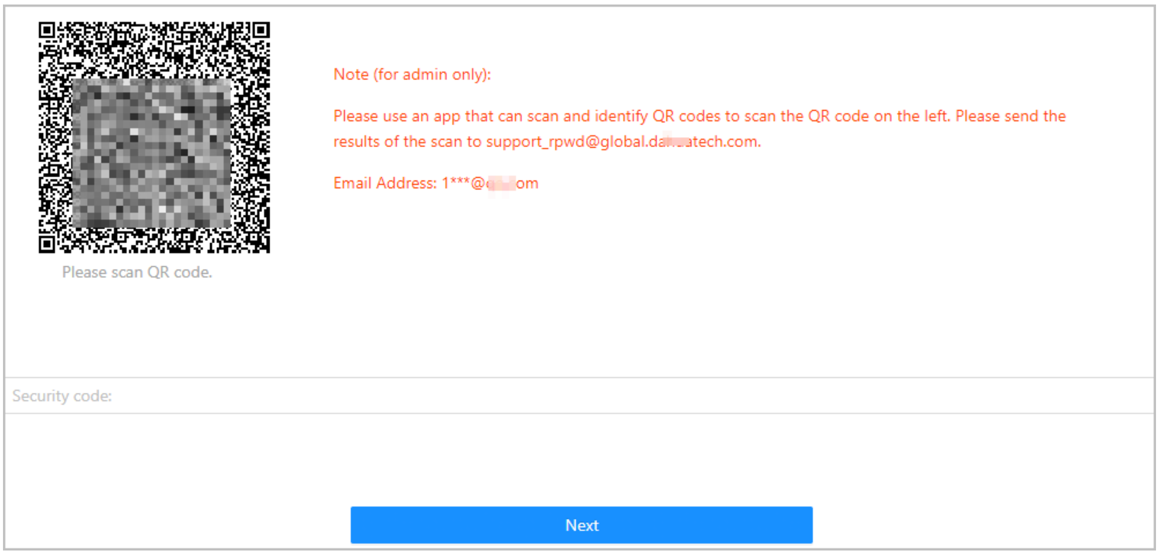
Procedure

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 3-2 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

Security code:

- 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 3-3 Home page

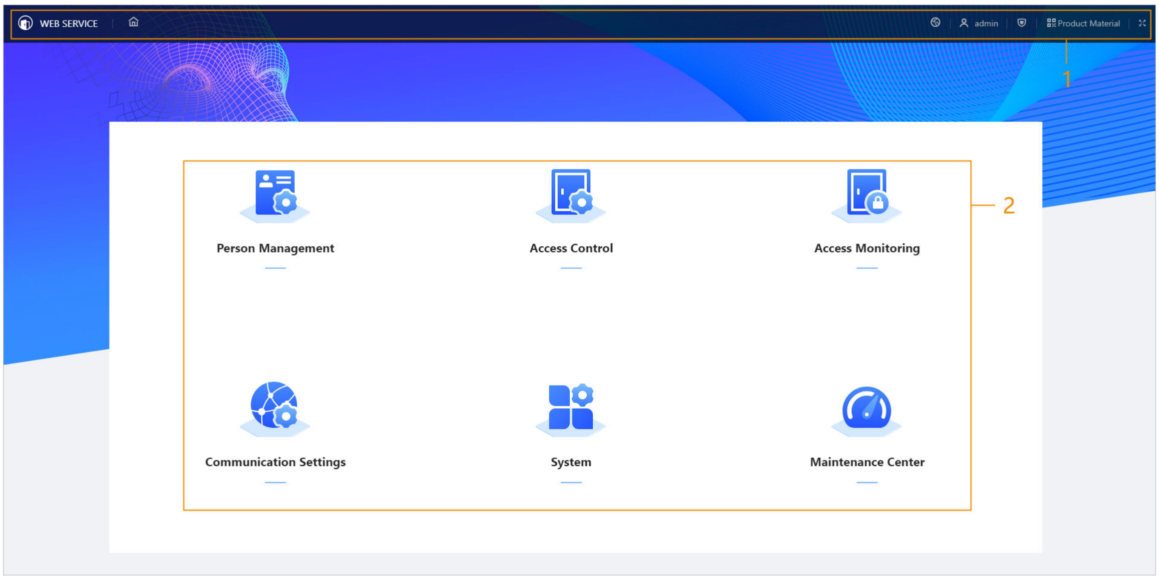


Table 3-2 Home page description

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

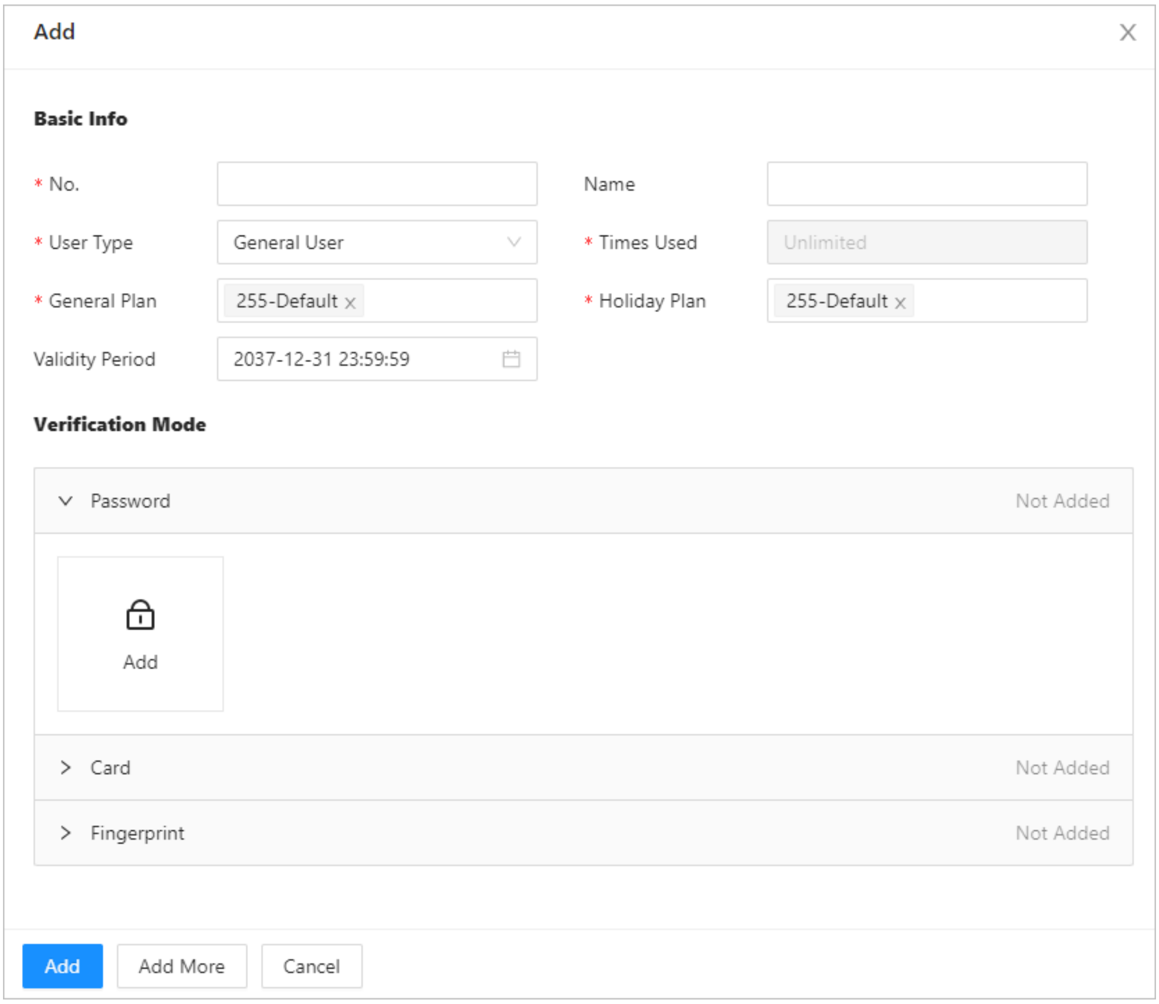
3.4 Person Management

Procedure

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

Step 2 Configure user information.

Figure 3-4 Add users



Add

Basic Info

* No.

Name

* User Type: General User

* Times Used: Unlimited

* General Plan: 255-Default

* Holiday Plan: 255-Default

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

Verification Mode

Password — Not Added

Card — Not Added

Fingerprint — Not Added

Table 3-3 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 number is 30 characters.
Name	The name can have up to 32 characters (including numbers, symbols, and letters).

Parameter	Description
User Type	● **General User** : General users can unlock the door. ● **Blocklist User** : When users in the blocklist unlock the door, service personnel will receive a notification. ● **Guest User** : Guests can unlock the door within a defined period or for certain amount of times. After the defined period expires or the unlocking times runs out, they cannot unlock the door. ● **Patrol User** : Patrol users can take attendance on the Device, but they do not have door permissions. ● **VIP User** : When VIP unlock the door, 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 as general users.
Times Used	Set an unlock limit for guest users. After the unlock times run out, they cannot unlock the door.
General Plan	People can unlock the door or take attendance during the defined period. 📖 You can select more than one plan.
Holiday Plan	People can unlock the door or take attendance during the defined holiday. 📖 You can select more than one holiday.
Validity Period	Set a date on which the door access and attendance permissions of the person will be expired.
Password	Enter the user password. The maximum length of the password is 8 digits. The duress password is the unlock password + 1. For example, if the user password is 12345, the duress password will be 12346. A duress alarm will be triggered when a duress password is used to unlock the door.

Parameter	Description
Card	● Enter the card number manually. 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.
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 set 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** , download the template and enter user information in it. Click **Import** to import the folder.

  Up to 10,000 users can be imported at a time.
- Clear: Clear all users.
- Refresh: Refresh the user list.
- Click ✎ to edit the person information.
- Select people, and then click **Delete** to delete users.
- Search: Search by user name or user ID.

3.5 Configuring Access Control

3.5.1 Configuring Access Control Parameters

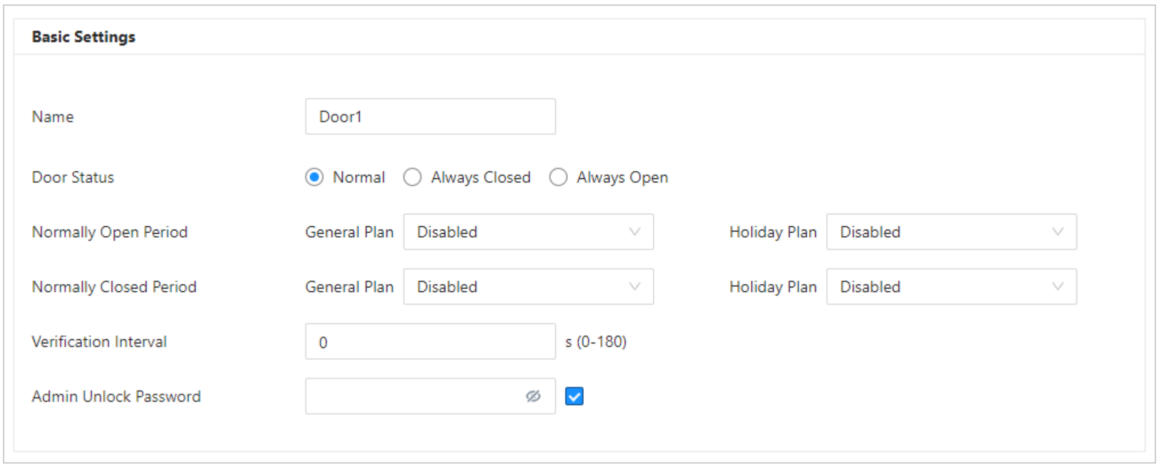
3.5.1.1 Configuring Basic Parameters

Procedure

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

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

Figure 3-5 Basic parameters



Basic Settings

Name	Door1		
Door Status	● Normal ○ Always Closed ○ Always Open		
Normally Open Period	General Plan: Disabled	Holiday Plan	Disabled
Normally Closed Period	General Plan: Disabled	Holiday Plan	Disabled
Verification Interval	0 s (0-180)		
Admin Unlock Password	☑		

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.

Parameter	Description
Normally Open Period	When you select **Normal**, you can select a time template from the drop-down list. The door remains open or closed during the defined time. ● When normally open period conflicts with normally closed period, normally open period takes priority over normally closed period. ● When period conflicts with holiday plan, holiday plans take priority over periods.
Normally Closed Period	
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.
Admin Unlock Password	You can configure one administrator password for opening the door. The password must contain 1 to 8 numbers.

Step 3 Click **Apply**.

3.5.1.2 Configuring Unlock Methods

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

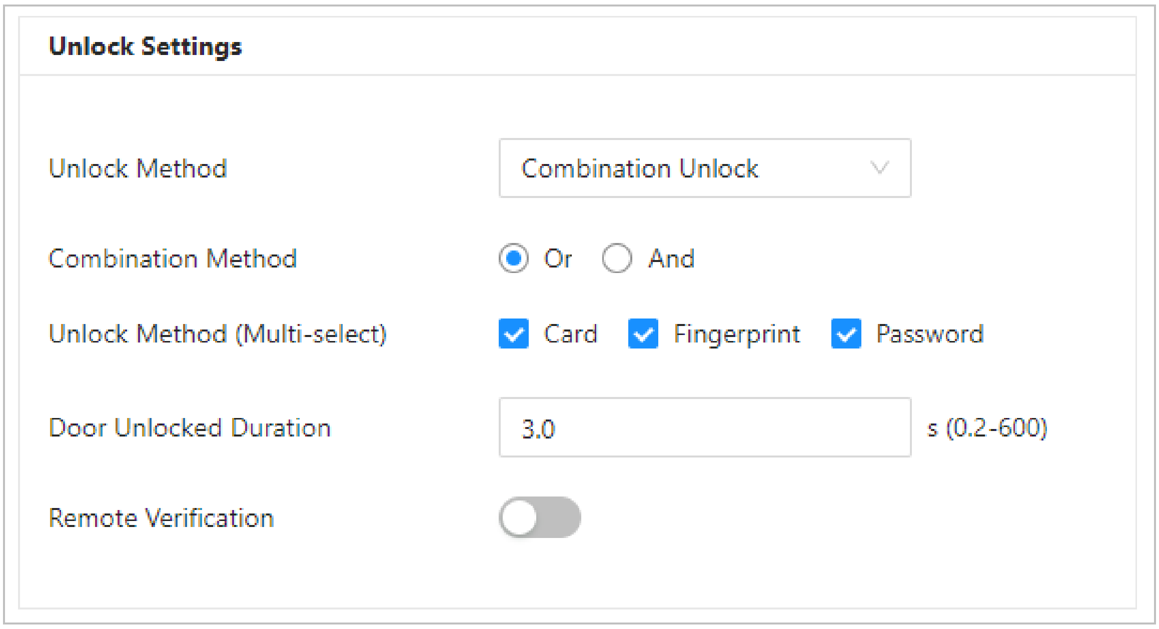
Procedure

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

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

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

Figure 3-6 Unlock settings



Unlock Settings

Unlock Method: Combination Unlock

Combination Method: ● Or ○ And

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

Door Unlocked Duration: 3.0 s (0.2-600)

Remote Verification: ○

Table 3-5 Unlock settings description

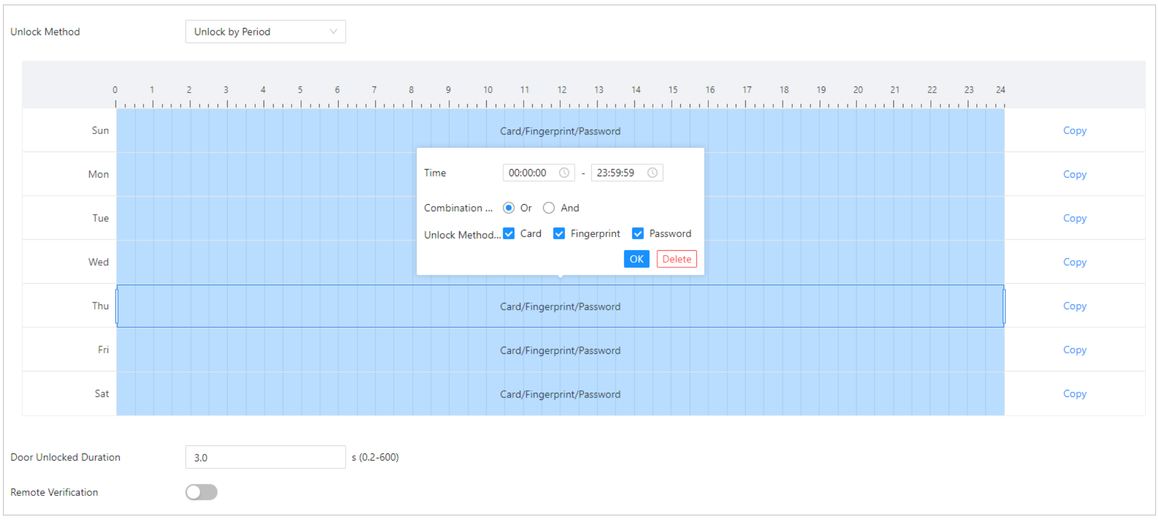
Parameter	Description
Unlock Method (Multi-select)	Unlock methods might differ depending on the models of product.
Door Unlock Duration	After a person is granted access, the door will remain unlocked for a defined time for the person to pass through. It ranges from 0.2 to 600 seconds.
Remote Verification	If this function is enabled, you can control the door on the corresponding platform.

- Unlock by period

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

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

Figure 3-7 Unlock by period



Unlock Method: Unlock by Period

Sun: Card/Fingerprint/Password

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

Combination ...: ● Or ○ And

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

Thu: Card/Fingerprint/Password

Fri: Card/Fingerprint/Password

Sat: Card/Fingerprint/Password

Door Unlocked Duration: 3.0 s (0.2-600)

Remote Verification

- Unlock by multiple users.

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

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

Step 3 Click **Apply**.

3.5.2 Configuring Alarms

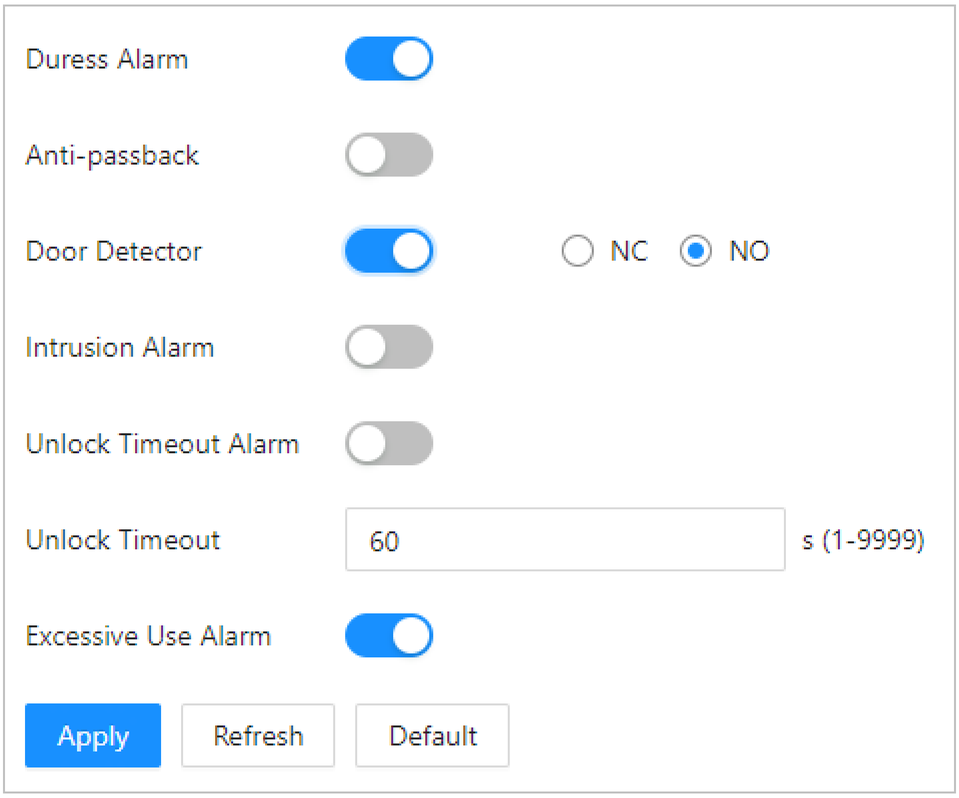
An alarm will be triggered when an abnormal access event occurs.

Procedure

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

Step 2 Configure alarm parameters.

Figure 3-8 Alarm



Duress Alarm ☑

Anti-passback ☐

Door Detector ☑ ○ NC ● NO

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.
Anti-passback	Users need to verify their identities both for entry and exit; otherwise an alarm will be triggered. It helps prevent 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 the person 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 the person 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.

Parameter	Description
Door Detector	With the door detector wired to your device, alarm can be triggered when doors are opened or closed abnormally. The door detector includes 2 types, including NC detector and NO detector. ● NC: The sensor is in a shorted position when the door or window is closed. ● NO: An open circuit is created when the window or door is actually closed.
Intrusion Alarm	If the door is opened abnormally, an intrusion alarm will be triggered and last for a defined time. The door detector and intrusion need to be enabled at the same time.
Unlock Timeout Alarm	When the door remains unlocked for longer than the defined timeout duration, the door timeout alarm will be triggered and last for the defined time. 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 last for a defined time.

Step 3 Click **Apply**.

3.5.3 Configuring Alarm Linkages (Optional)

You can configure alarm linkages.

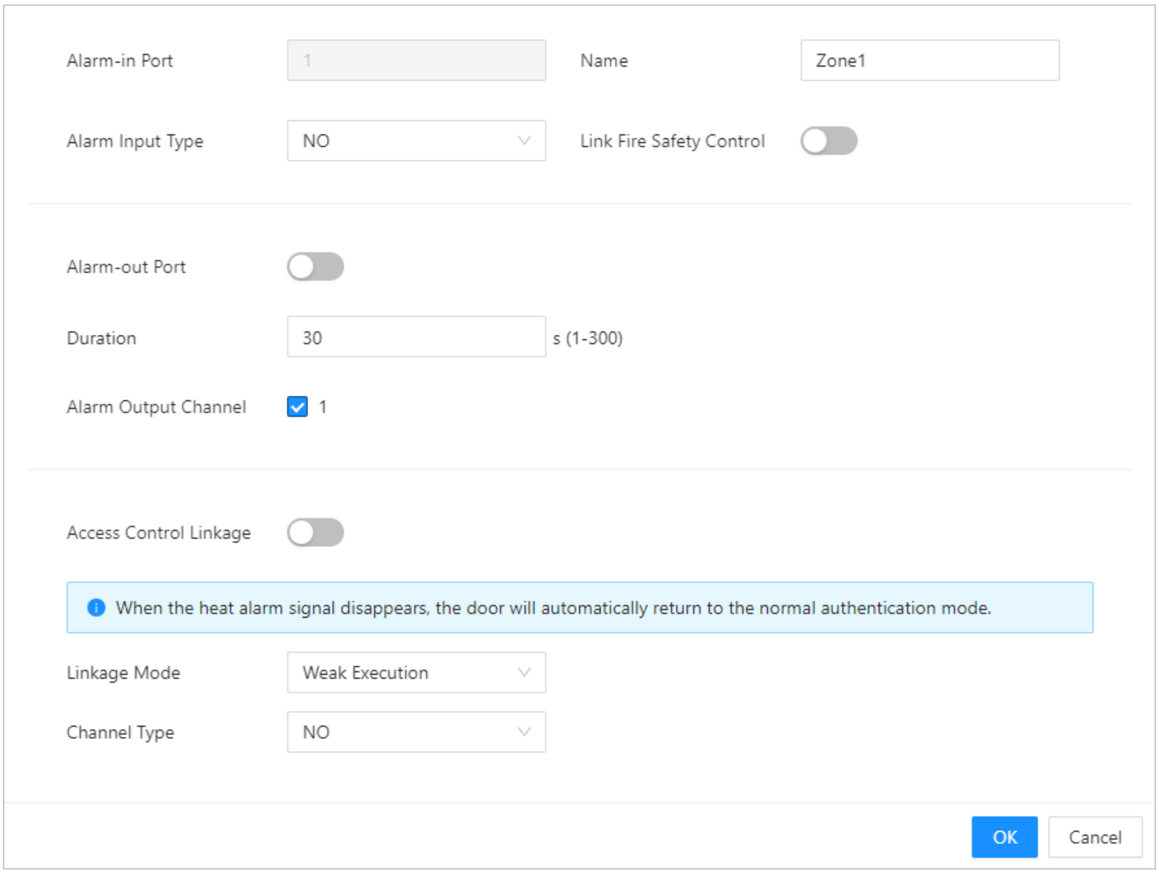
Procedure

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

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

Step 2 Click ✎ to configure alarm.

Figure 3-9 Alarm linkage



Alarm-in Port: 1

Name: Zone1

Alarm Input Type: NO

Link Fire Safety Control: ○

Alarm-out Port: ○

Duration: 30 s (1-300)

Alarm Output Channel: ☑ 1

Access Control Linkage: ○

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

Linkage Mode: Weak Execution

Channel Type: NO

Step 3 Create a name for the alarm zone.

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

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

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

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

Step 6 Select a linkage mode.

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

Step 7 Select a channel type.

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

Step 8 Click **OK**.

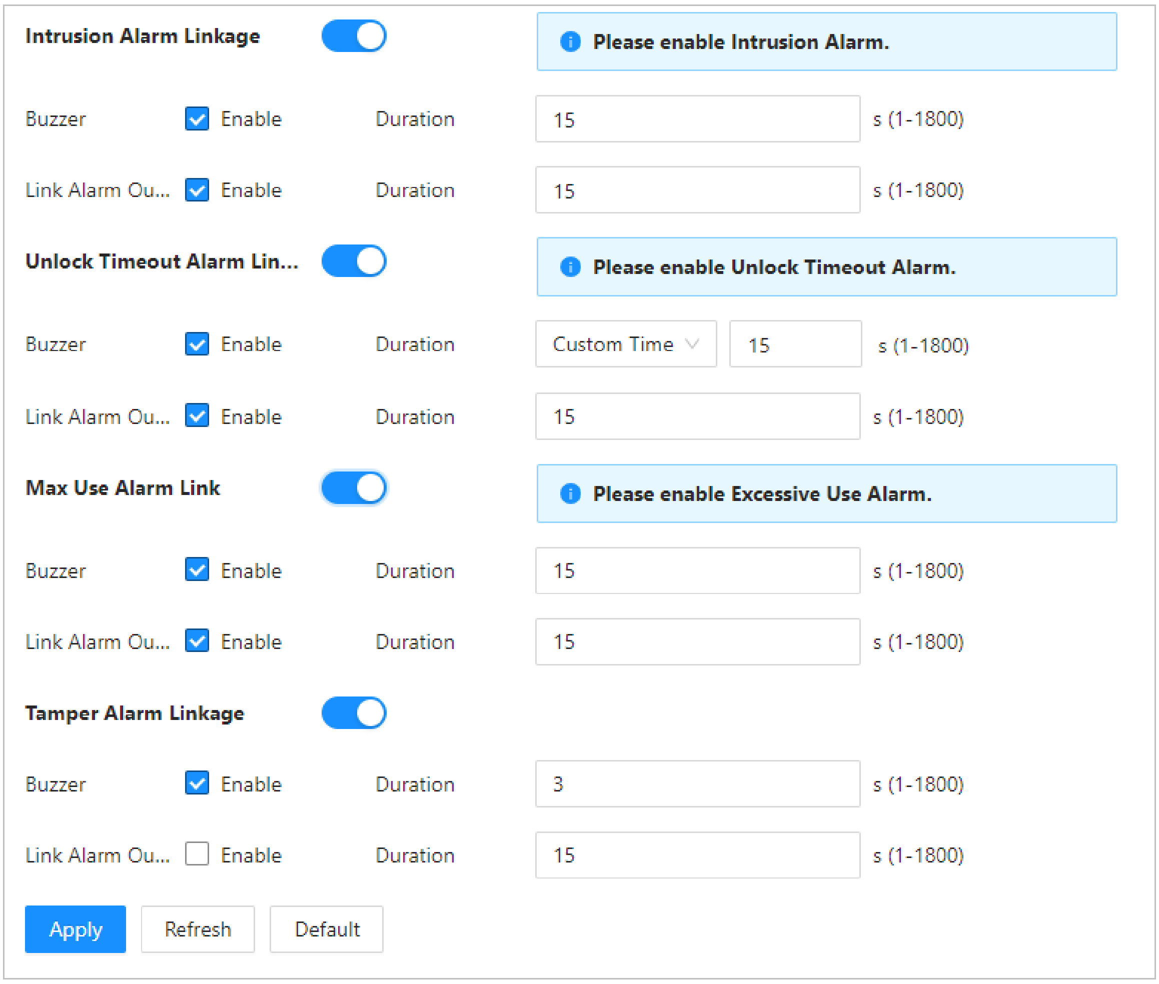
3.5.4 Configuring Alarm Event Linkage

Procedure

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

Step 2 Configure alarm event linkages.

Figure 3-10 Alarm event linkage



Intrusion Alarm Linkage ● Please enable Intrusion Alarm.

Buzzer ☑ Enable Duration 15 s (1-1800)

Link Alarm Ou... ☑ Enable Duration 15 s (1-1800)

Unlock Timeout Alarm Lin... ● Please enable Unlock Timeout Alarm.

Buzzer ☑ Enable Duration Custom Time 15 s (1-1800)

Link Alarm Ou... ☑ Enable Duration 15 s (1-1800)

Max Use Alarm Link ● Please enable Excessive Use Alarm.

Buzzer ☑ Enable Duration 15 s (1-1800)

Link Alarm Ou... ☑ Enable Duration 15 s (1-1800)

Tamper Alarm Linkage ●

Buzzer ☑ Enable Duration 3 s (1-1800)

Link Alarm Ou... □ Enable Duration 15 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. ● Link Alarm Output: The external alarm device generates alarms when the intrusion alarm is triggered. You can configure the alarm duration.

Parameter	Description
Unlock Timeout Alarm Linkage	When the door remains unlocked for longer than the defined timeout duration, the door timeout alarm will be triggered and last for the defined time. ● Buzzer: The buzzer sounds when the unlock timeout alarm is triggered. You can configure the alarm duration. ● Local Alarm Output: The external alarm device generates alarms 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. ● Local Alarm Output: The external alarm device generates alarms when the unlock timeout alarm is triggered. You can configure the alarm duration.
Tamper Alarm Linkage	The tamper alarm is triggered when someone has tried to physically damage the Device. ● Buzzer: The buzzer sounds when the tamper alarm is triggered. You can configure the alarm duration. ● Local Alarm Output: The external alarm device generates alarms when the tamper alarm is triggered. You can configure the alarm duration.

Step 3 Click **Apply**.

3.5.5 Configuring Card Settings

Background Information

This function is only available on select models.

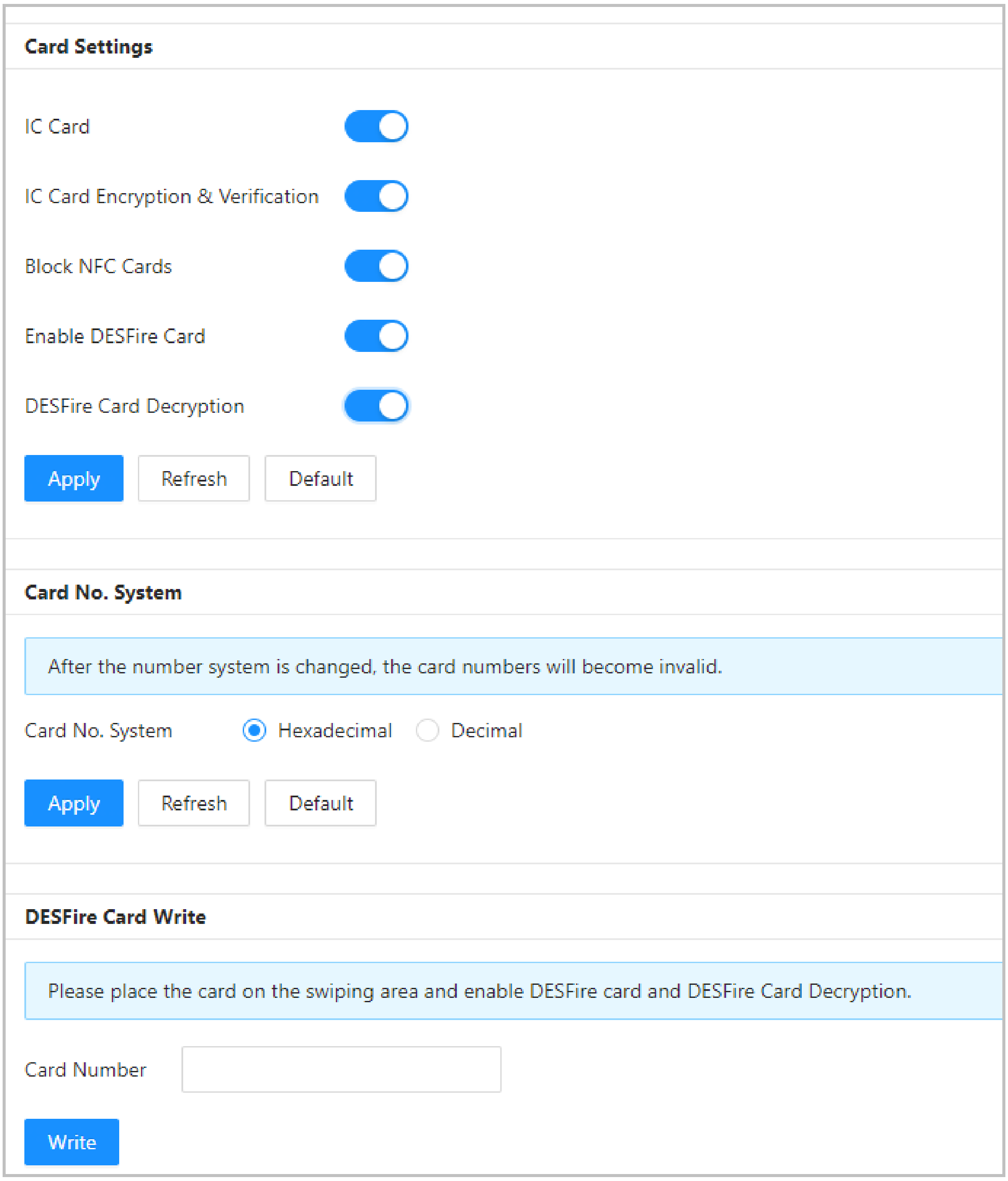
Procedure

Step 1 Log in to the webpage.

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

Step 3 Configure the card parameters.

Figure 3-11 Card parameters


Card Settings

IC Card ●

IC Card Encryption & Verification ●

Block NFC Cards ●

Enable DESFire Card ●

DESFire Card Decryption ●

Apply Refresh Default

Card No. System

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

Card No. System ● Hexadecimal ○ Decimal

Apply Refresh Default

DESFire Card Write

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

Card Number

Write

Table 3-8 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 and **IC Card** are enabled at the same time. 📖 ● 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 **IC Card** , **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**.

3.5.6 Configuring Periods

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

3.5.6.1 Configuring General Plan

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

Procedure

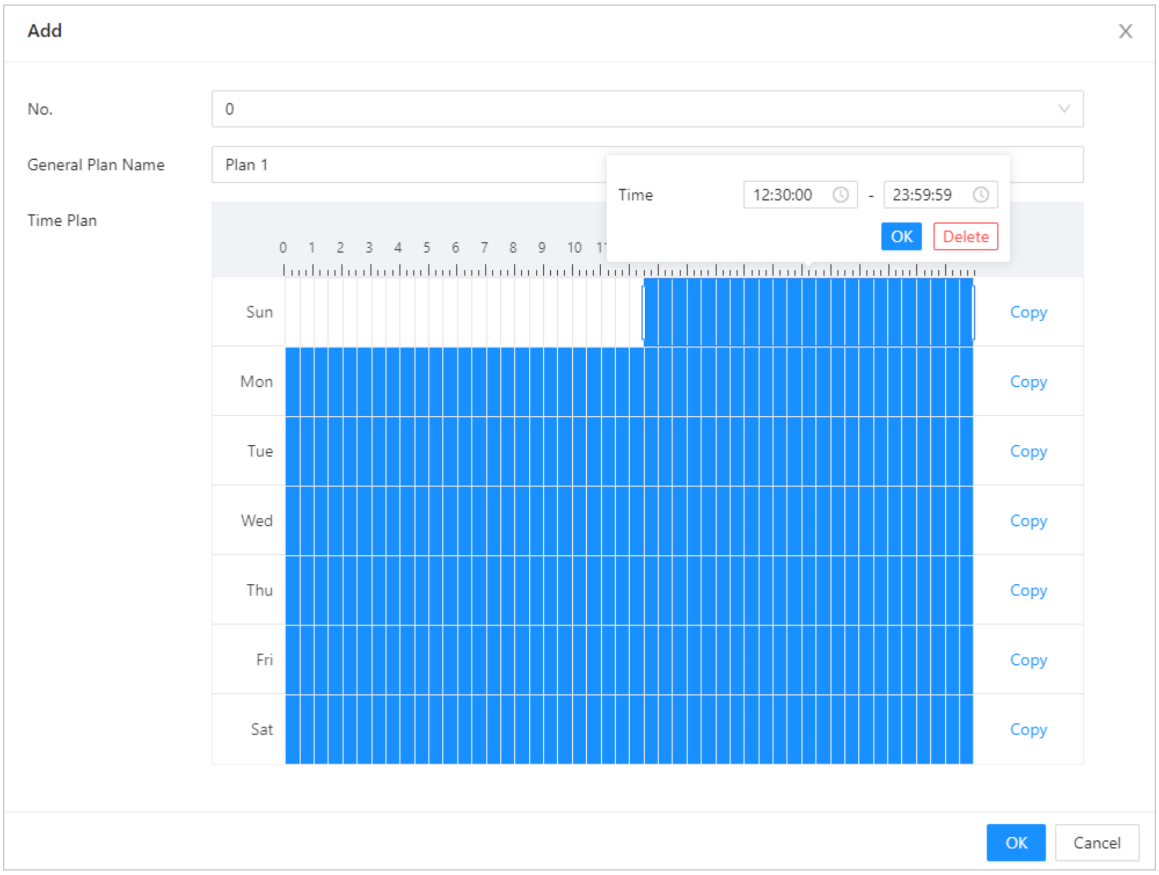
Step 1 Log in to the webpage.

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

Step 3 Click **Add**.

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

Figure 3-12 Configure general plan



Add

No. 0

General Plan Name Plan 1

Time Plan

Time 12:30:00 - 23:59:59

Step 4 Click **OK**.

3.5.6.2 Configuring Holiday Plan

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

Procedure

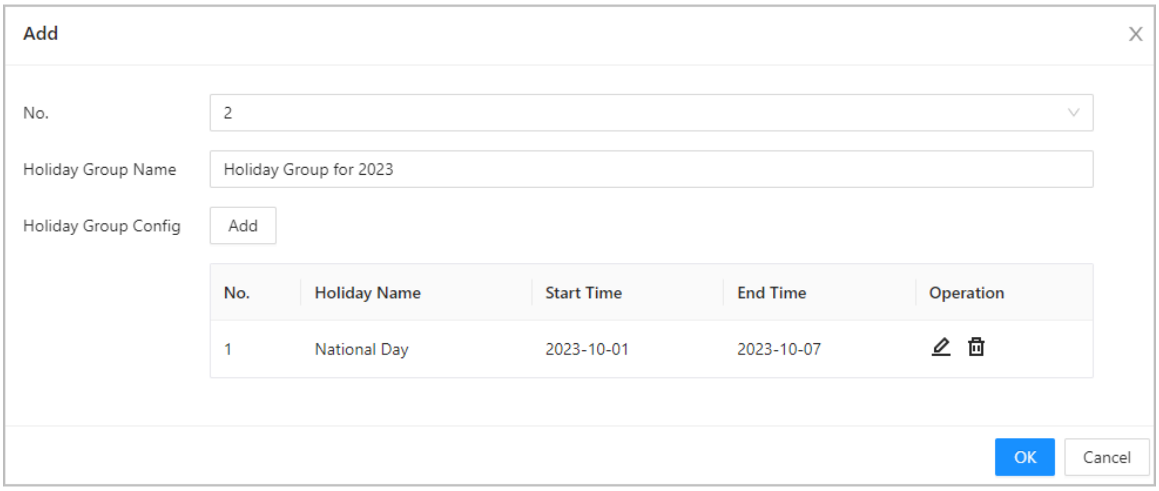
Step 1 Log in to the webpage.

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

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

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

Figure 3-13 Add a holiday group



Add

No. 2

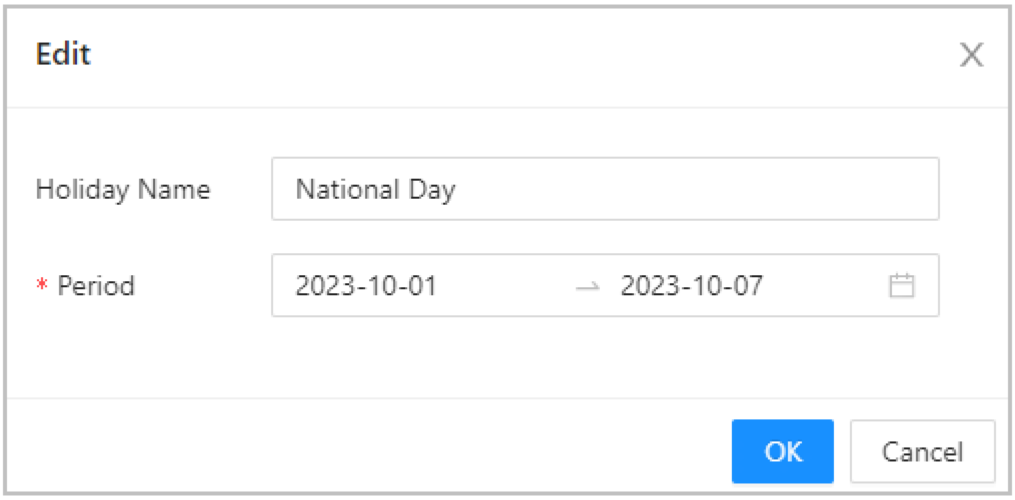
Holiday Group Name Holiday Group for 2023

Holiday Group Config

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

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

Figure 3-14 Add a holiday to a holiday group



Edit

Holiday Name National Day

* Period 2023-10-01 → 2023-10-07

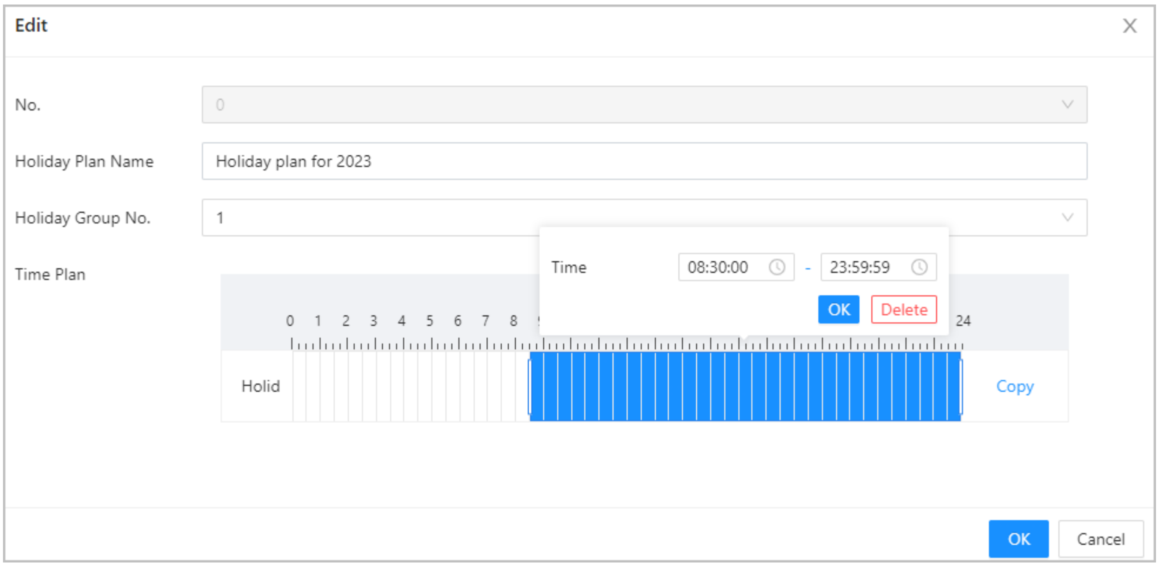
Step 4 Click **OK**.

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

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

   Supports adding up to 4 time sections on a day.

Figure 3-15 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 6 Click **OK**.

3.5.7 Configuring Port Functions

Some ports can function as different ports, you can set them to different ports based on the actual needs.

Background Information

- This function is only available on select models.
- Ports might differ depending on the models of the product.

Procedure

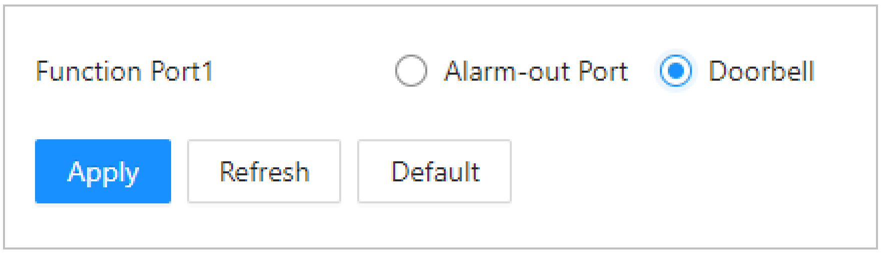
Step 1 On the webpage, select **Access Control** > **Port Config**.

Step 2 Select the type of the port.

It is **Doorbell** by default.

Step 3 Click **Apply**.

Figure 3-16 Configure ports


Function Port1 ○ Alarm-out Port ● Doorbell

3.5.8 Configuring the Password Unlock

When the **PIN Code Authentication** is enabled, people can unlock the door by simply entering the password.

Background Information

- If PIN code authentication is not enabled, you can unlock the door by entering the unlock password in the format of **user ID#password#** . For example, if the user ID is 123, and the password you set is 12345, and then you must enter **123#12345#** to unlock the door.
- If PIN code authentication is enabled, you can unlock the door by entering the unlock password in the format of **password#** . For example, if the user ID is 123, and the password you set is 12345, and then you must enter **12345#** to unlock the door.

Procedure

Step 1 On the home page, select **Access Control** > **Unlock Method Config**.

Step 2 Turn on **PIN Code Authentication** , and then click **Apply**.

There are some safety risks in enabling PIN code authentication. When it is turned on, the user types and roles become ineffective, and the following situations occur.

- First-card holders and users in multi-person unlock groups need to verify their identities through the defined unlock methods, except password. If they verify through password, the first-card unlock or multi-person unlock function will become ineffective.
- Users need to verify their through defined unlock methods except password. If they gain access through password, the anti-passback function will become ineffective.
- Patrol users and block-listed users can simply enter their password to unlock the door.
- Frozen and expired accounts can still unlock doors by simply entering their password.
- When the password unlock method is turned off at the same time, all types of users cannot unlock the door using their password.

3.5.9 Configuring First-Person Unlock

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

Prerequisites

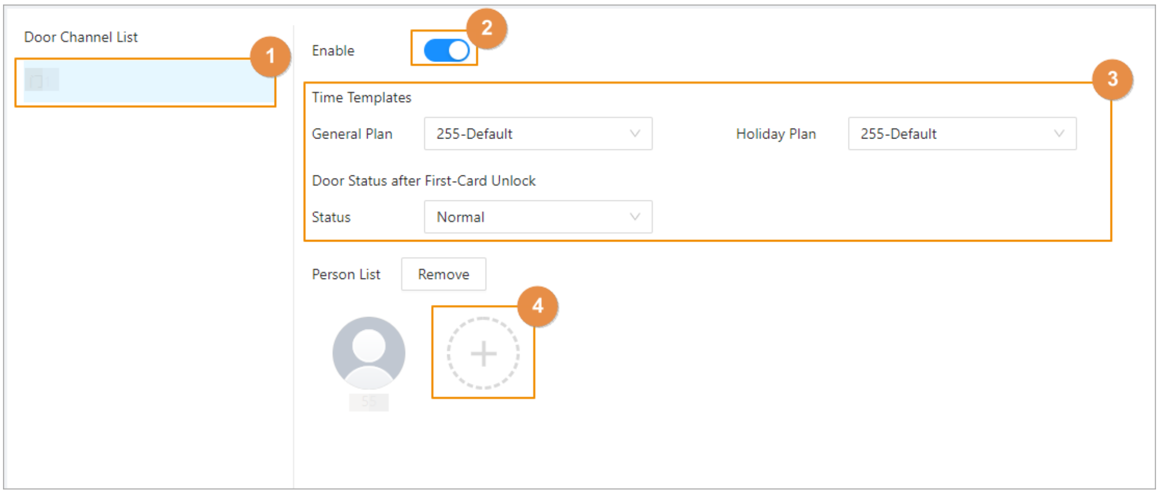
Persons can only be set as first persons when they have permissions to access doors.

Procedure

Step 1 On the home page, select **Access Control** > **First-Person Unlock**.

Step 2 Select the door channel, and then enable the function.

Figure 3-17 First-person unlock



Enable

Time Templates

General Plan: 255-Default

Holiday Plan: 255-Default

Door Status after First-Card Unlock

Status: Normal

Person List

Step 3 Configure the parameters.

Table 3-9 Parameter description

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

Step 4 Click **Apply**.

3.5.10 Configuring Anti-Passback

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

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

- When you have configured anti-passback for sub controllers through the main controller, and you plan on restoring the main controller to its factory defaults, we recommend you also restore the sub controller to its factory defaults at the same time.
- If the anti-passback rule is used when the network is not stable, the door might open after an identity is verified, but a time-out alarm might be triggered on the card reader. Please make sure your network is stable.

Procedure

Step 1 On the home page, select **Access Control** > **Anti-passback Group Config**.

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

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

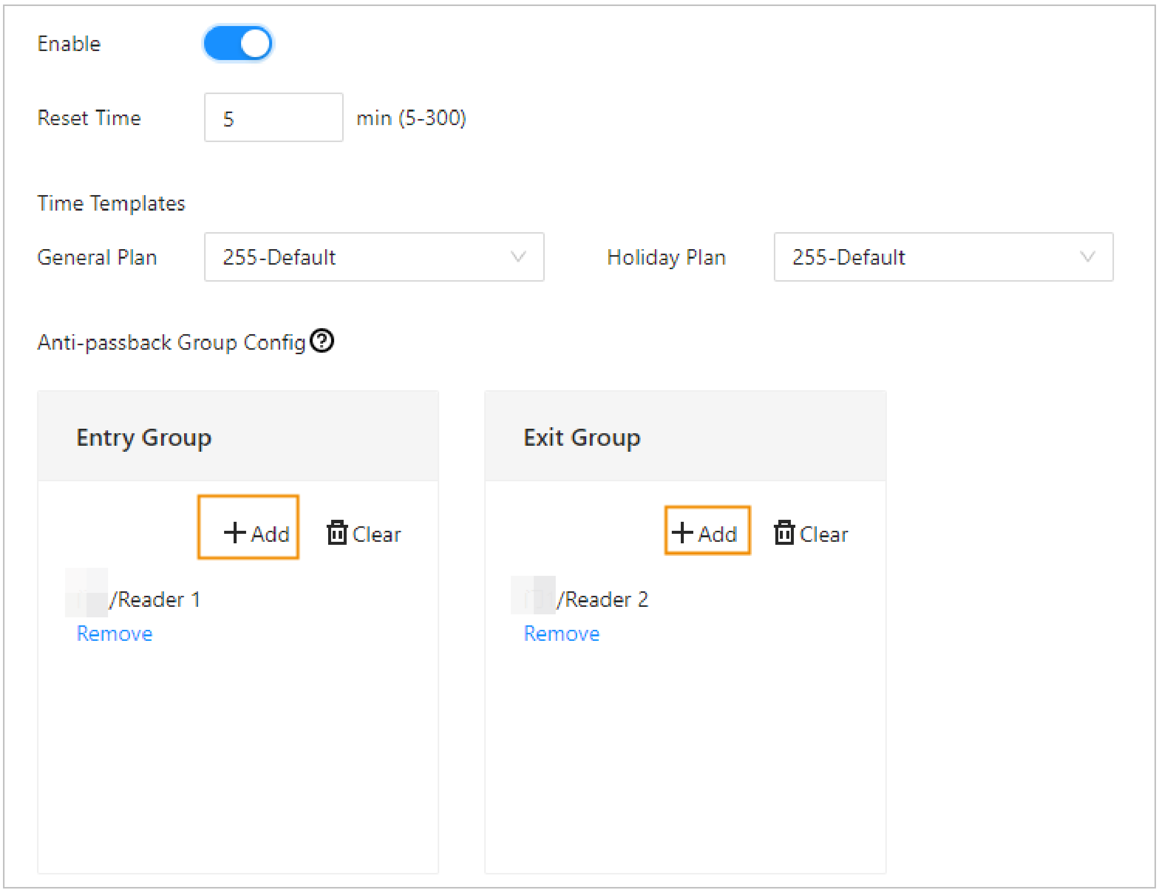
Step 3 Select the general plan and the holiday plan.

Anti-passback is effective during the defined time.

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

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

Figure 3-18 Anti-passback



Enable: on

Reset Time: 5 min (5-300)

Time Templates

General Plan: 255-Default

Holiday Plan: 255-Default

Anti-passback Group Config

Entry Group: /Reader 1

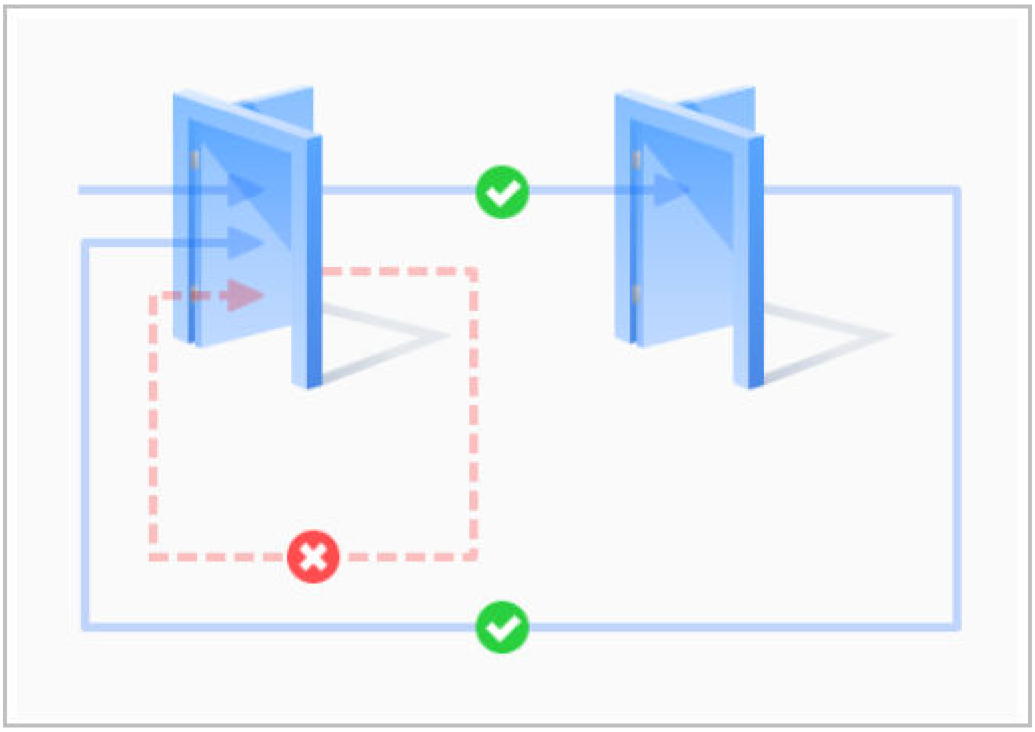
Exit Group: /Reader 2

Step 6 Click **Apply**.

Results

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

Figure 3-19 Anti-passback function



3.6 Access Monitoring

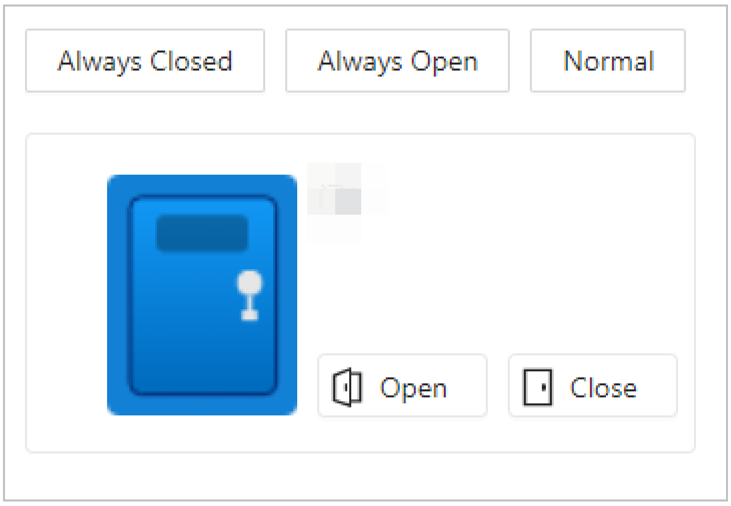
Log in to the webpage, select **Access Monitoring**, and all the connected doors are displayed.

Operations to control the door

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

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

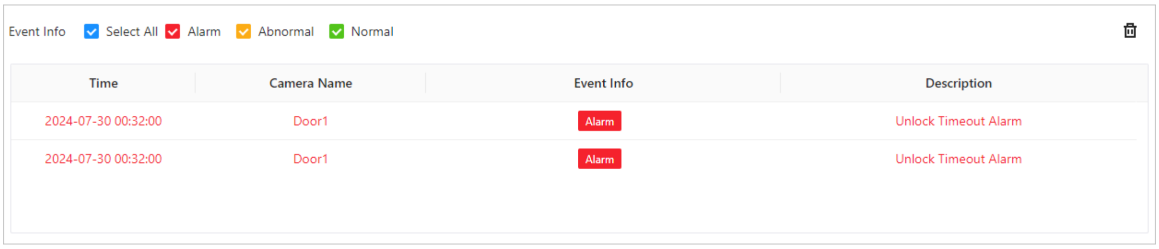
Figure 3-20 Operations to control the door



Event information

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

Figure 3-21 Event information



Event Info ☑ Select All ☑ Alarm ☑ Abnormal ☑ Normal 🗑

Time	Camera Name	Event Info	Description
2024-07-30 00:32:00	Door1	Alarm	Unlock Timeout Alarm
2024-07-30 00:32:00	Door1	Alarm	Unlock Timeout Alarm

Details

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

3.7 Communication Settings

3.7.1 Network Settings

3.7.1.1 Configuring TCP/IP

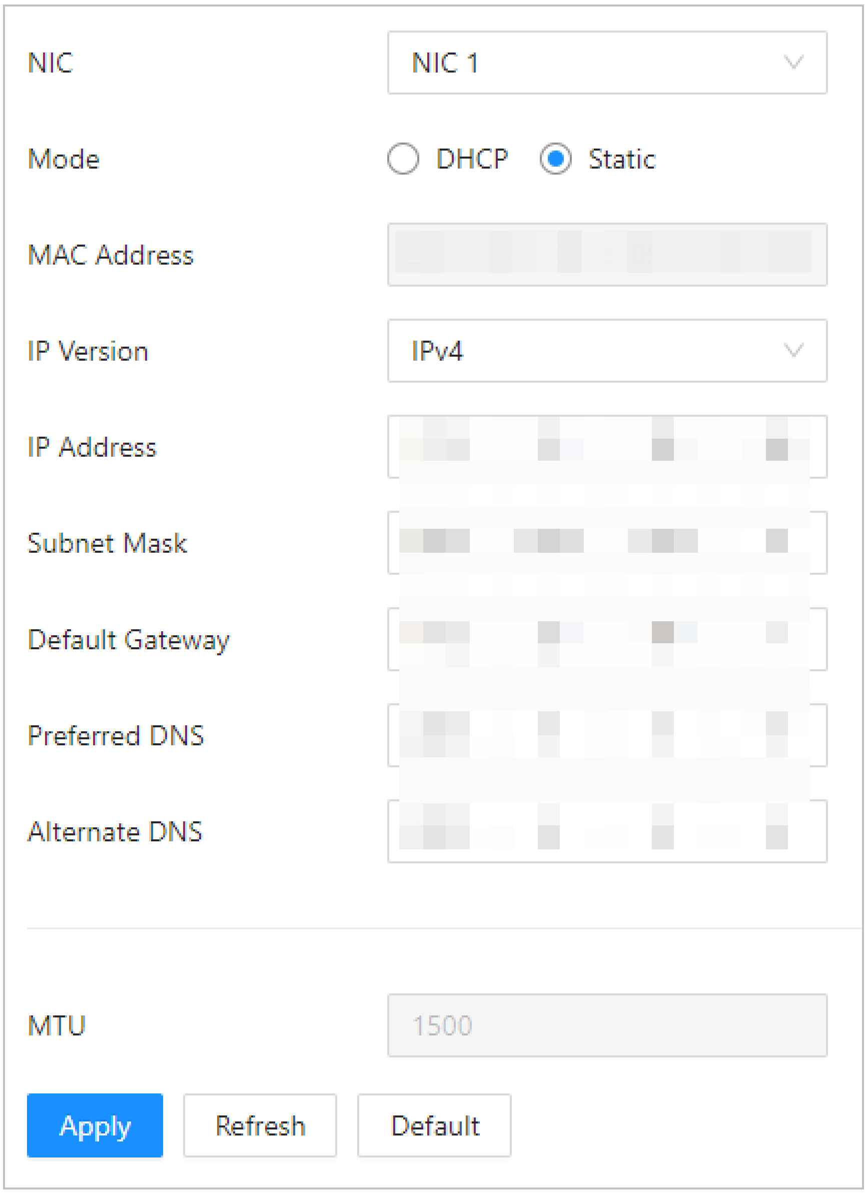
You need to configure IP address of Device to make sure that it can communicate with other devices.

Procedure

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

Step 2 Configure the parameters.

Figure 3-22 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 3-10 Description of TCP/IP

Parameter	Description
Mode	● Static: Manually enter IP address, subnet mask, and gateway. ● DHCP: It stands for Dynamic Host Configuration Protocol. When DHCP is turned on, the Device will automatically be assigned with IP address, subnet mask, and gateway.
MAC Address	MAC address of the Device.
IP Version	IPv4 or IPv6.

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**.

3.7.1.2 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.

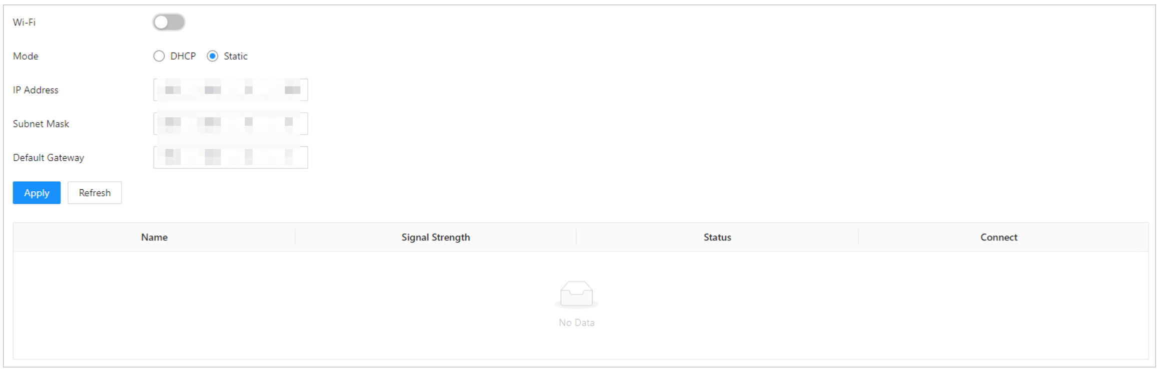
Procedure

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

Step 2 Turn on Wi-Fi.

All available Wi-Fi are displayed.

Figure 3-23 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.

3.7.1.3 Configuring Wi-Fi AP

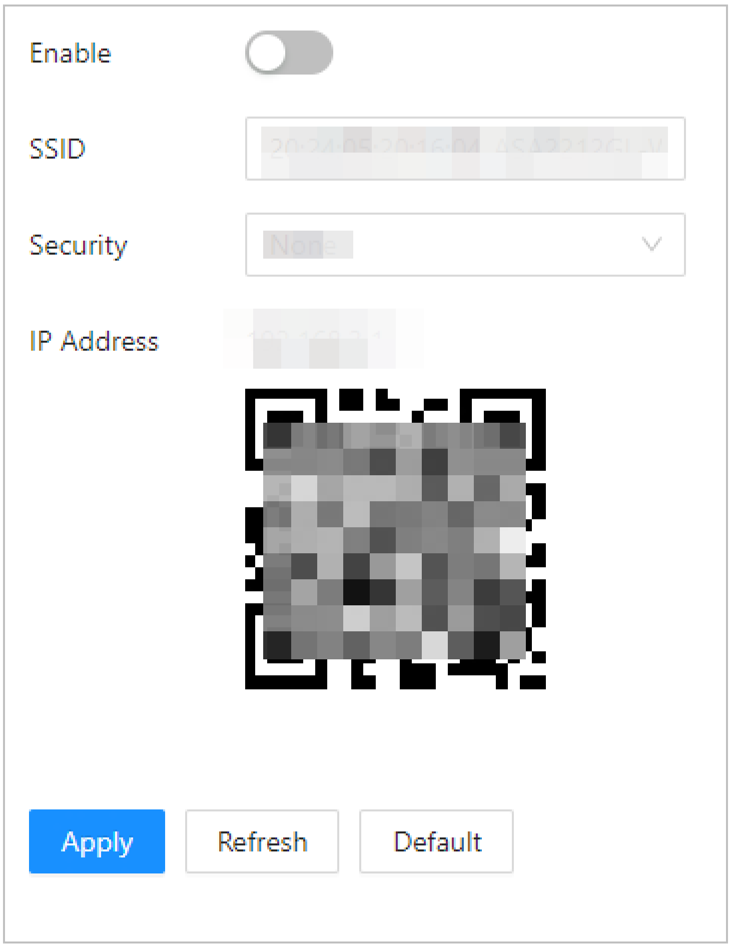
- The Wi-Fi function is available on select models.
- The Wi-Fi and Wi-Fi AP cannot be enabled at the same time.

Procedure

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

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

Figure 3-24 Wi-Fi AP



Enable ○

SSID [redacted]

Security [redacted]

IP Address [redacted]

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.

3.7.1.4 Configuring Port

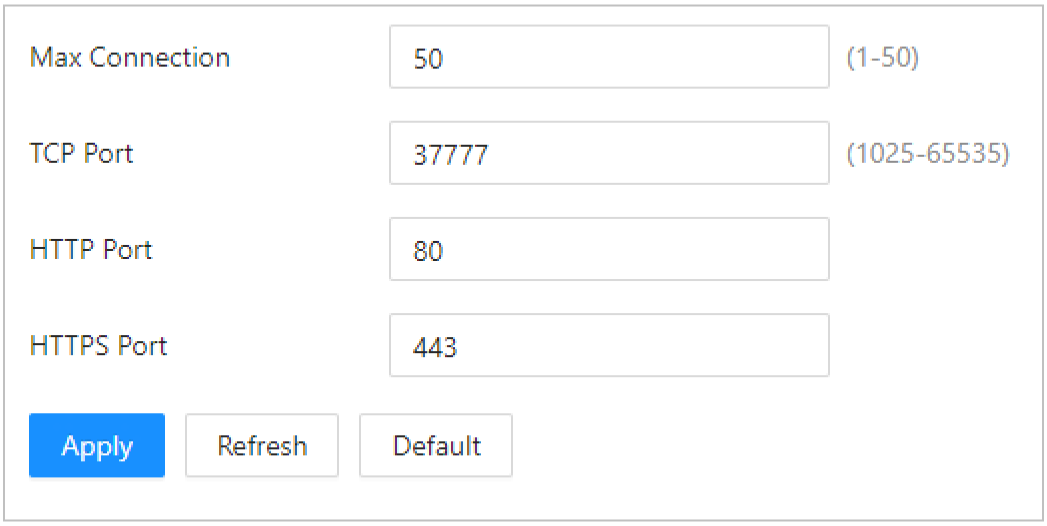
You can limit access to the Device at the same time through webpage, desktop client and mobile client.

Procedure

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

Step 2 Configure the ports.

Figure 3-25 Configure ports



Max Connection 50 (1-50)

TCP Port 37777 (1025-65535)

HTTP Port 80

HTTPS Port 443

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

Table 3-11 Description of ports

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

Step 3 Click **Apply**.

3.7.1.5 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 3-26 Basic service

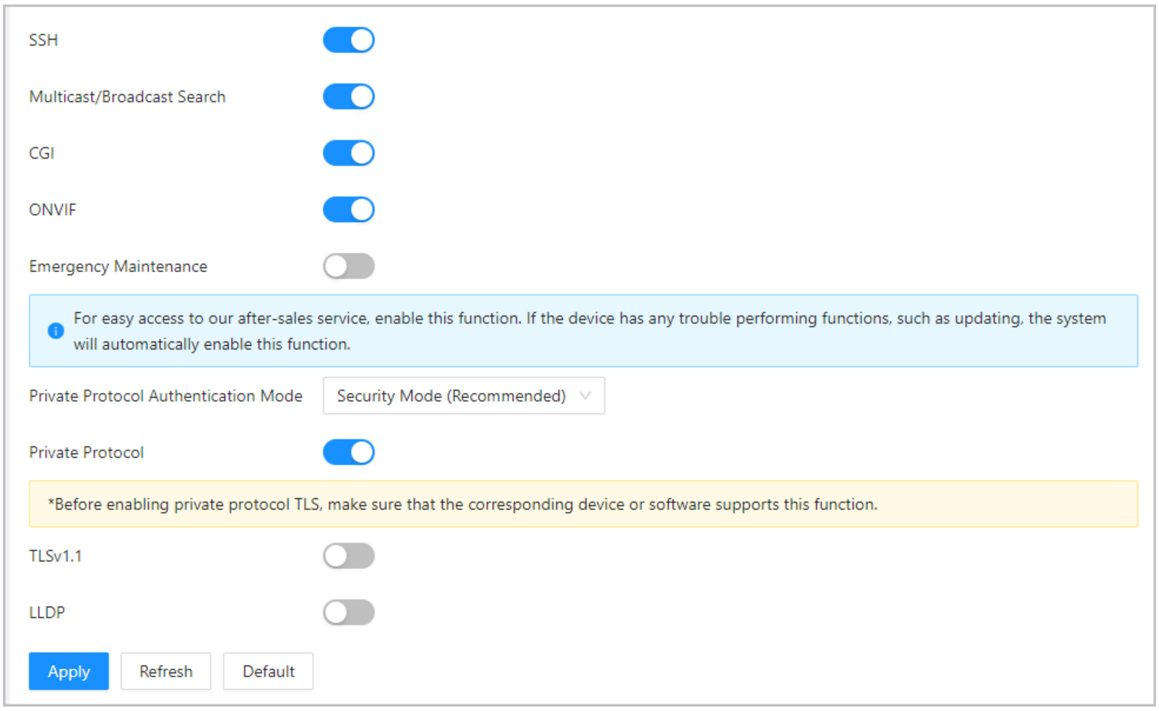

SSH
Multicast/Broadcast Search
CGI
ONVIF
Emergency Maintenance
For easy access to our after-sales service, enable this function. If the device has any trouble performing functions, such as updating, the system will automatically enable this function.
Private Protocol Authentication Mode: Security Mode (Recommended)
Private Protocol
*Before enabling private protocol TLS, make sure that the corresponding device or software supports this function.
TLSv1.1
LLDP

Table 3-12 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**.

3.7.1.6 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.

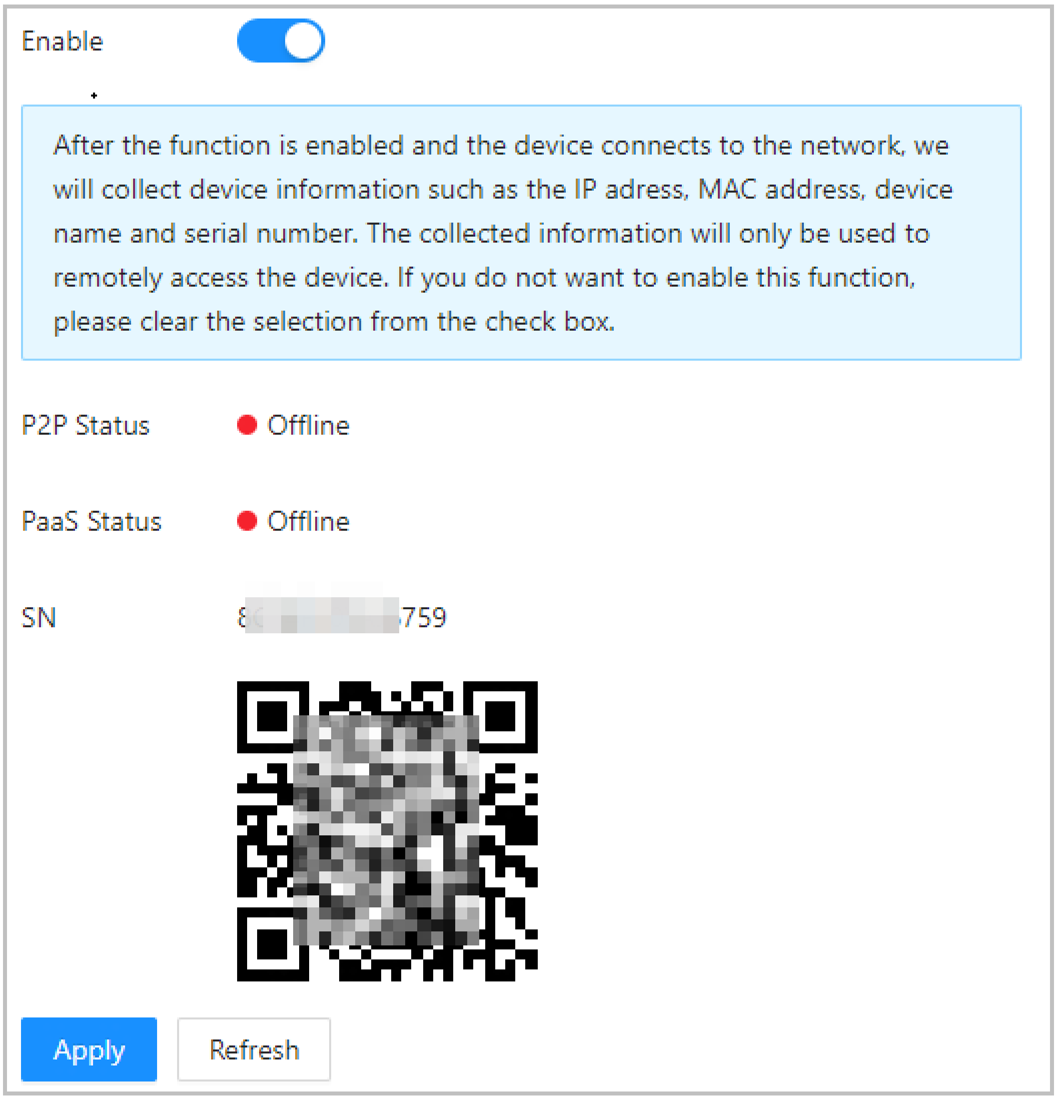
Procedure

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 3-27 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.

3.7.1.7 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.

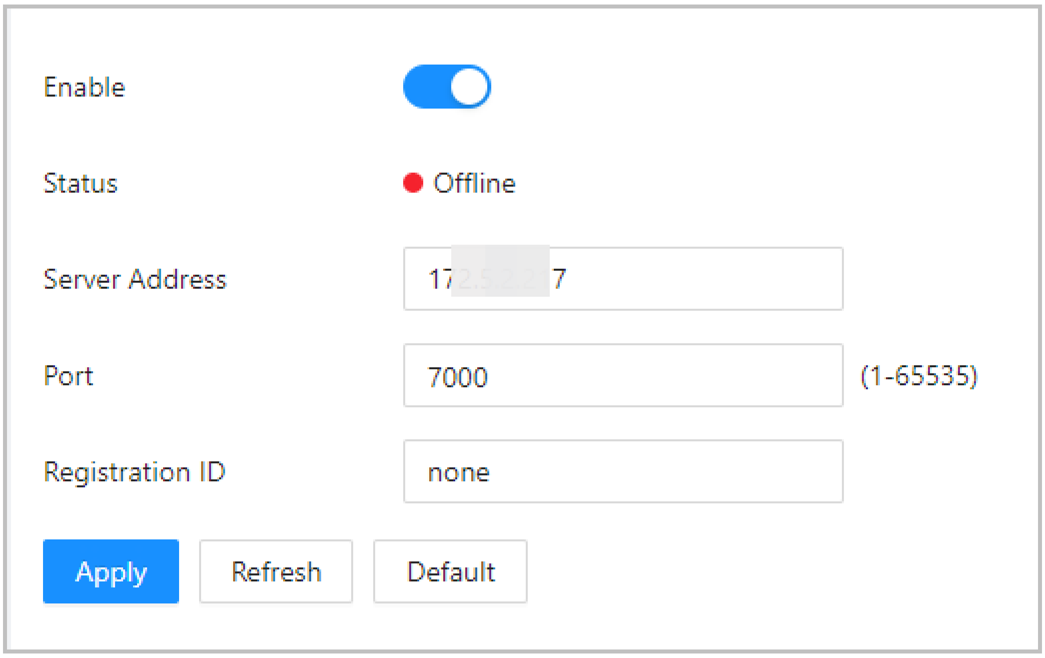
Background Information

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.



Enable

Status ● Offline

Server Address 17[redacted]7

Port 7000 (1-65535)

Registration ID none

Figure 3-28 Auto Registration

Table 3-13 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**.

3.7.1.8 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 3-14 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**.

3.7.1.9 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**.

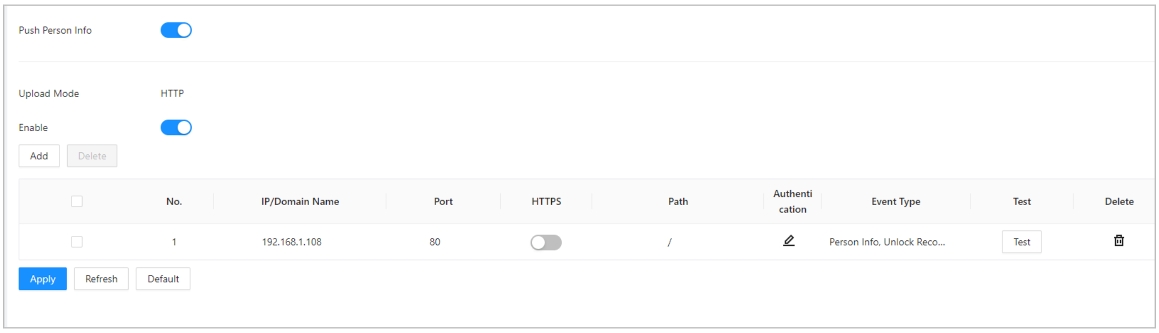
Step 2 (Optional) Enable **Push Person Info**.

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 3-29 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 3-15 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**.

3.7.2 Configuring RS-485

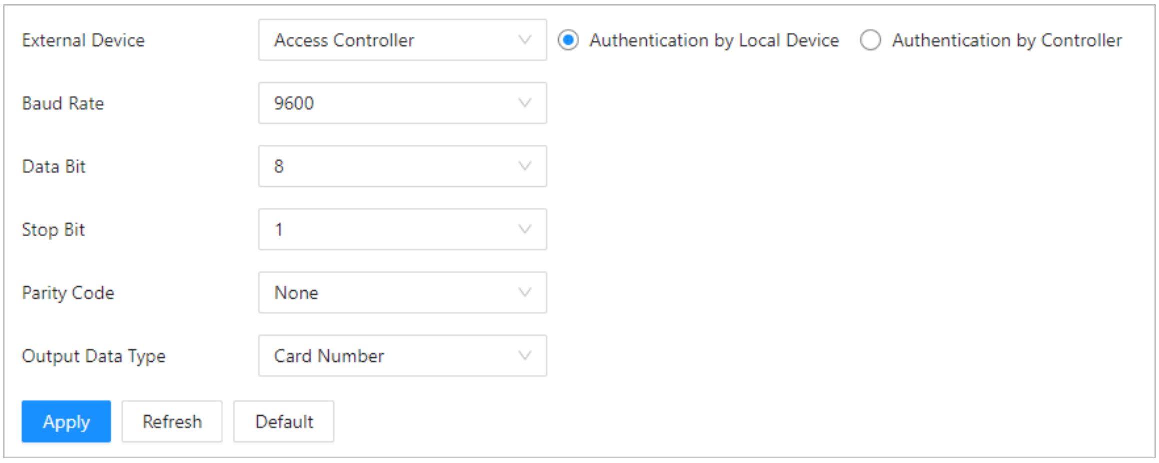
Configure the RS-485 parameters if you connect an external device to the RS-485 port.

Procedure

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

Step 2 Configure the parameters.

Figure 3-30 Configure parameters



External Device: Access Controller ● Authentication by Local Device ○ Authentication by Controller

Baud Rate: 9600

Data Bit: 8

Stop Bit: 1

Parity Code: None

Output Data Type: Card Number

Table 3-16 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. ◇ **Authentication by Local Device** : The identity is verified on both the Device and the controller. ◇ **Authentication by Controller** : The identity is verified only on the controller. ● 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**.

3.7.3 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**.

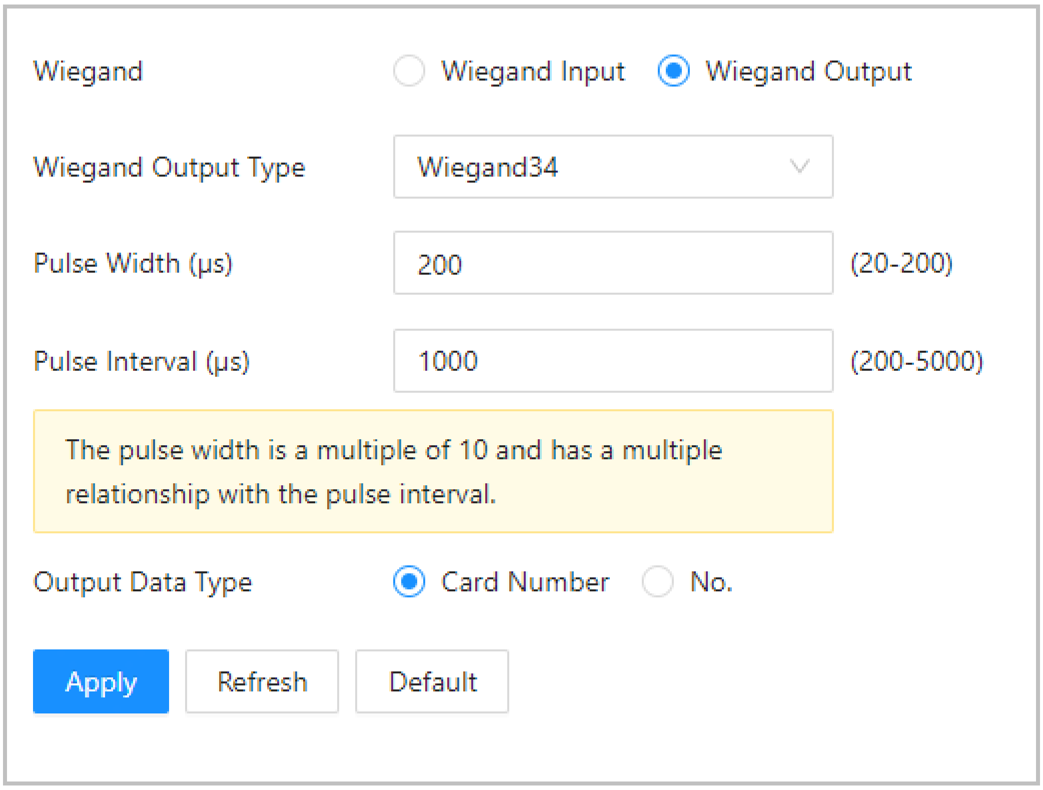
Step 2 Select a Wiegand type, and then configure parameters.

- 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 3-31 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 3-17 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**.

3.8 Configuring the System

3.8.1 User Management

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

3.8.1.1 Adding Administrators

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

Procedure

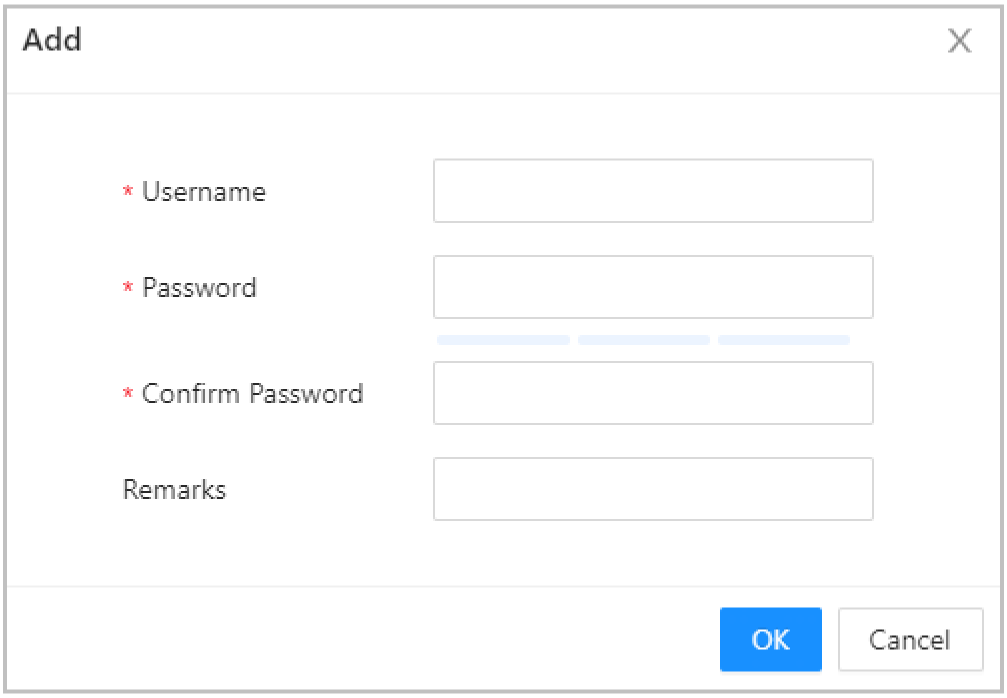
Step 1 On the home page, select **System** > **Account** > **Account**.

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

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

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

Figure 3-32 Add administrators



Step 3 Click **OK**.

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

3.8.1.2 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 3-33 Add ONVIF user

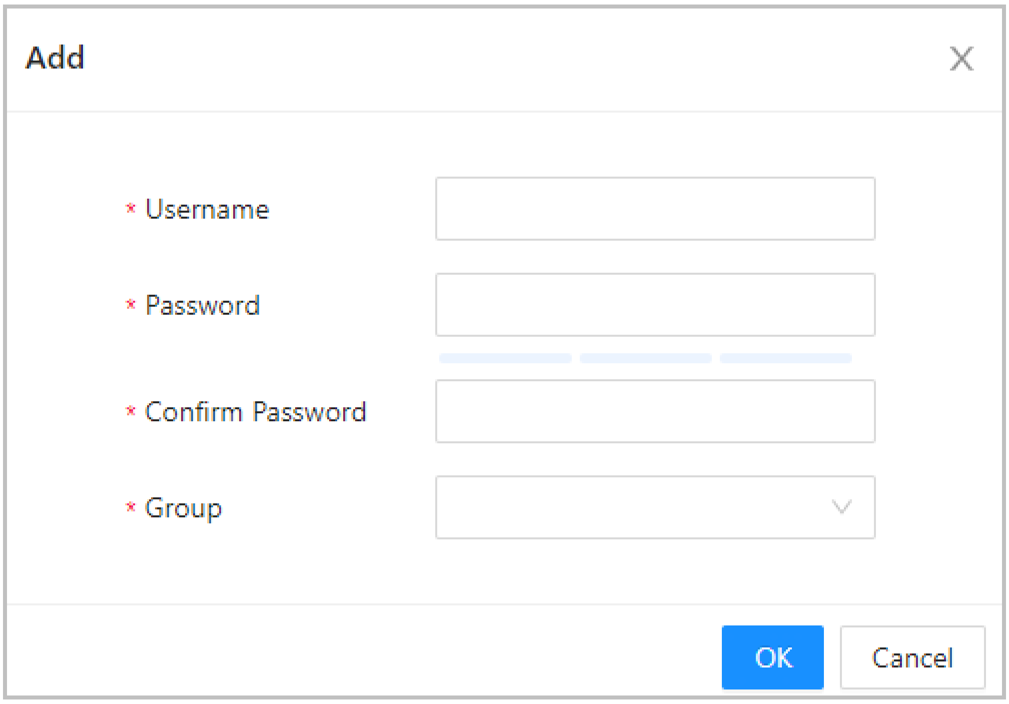


Table 3-18 ONVIF user description

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

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**.

3.8.1.3 Resetting the Password

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

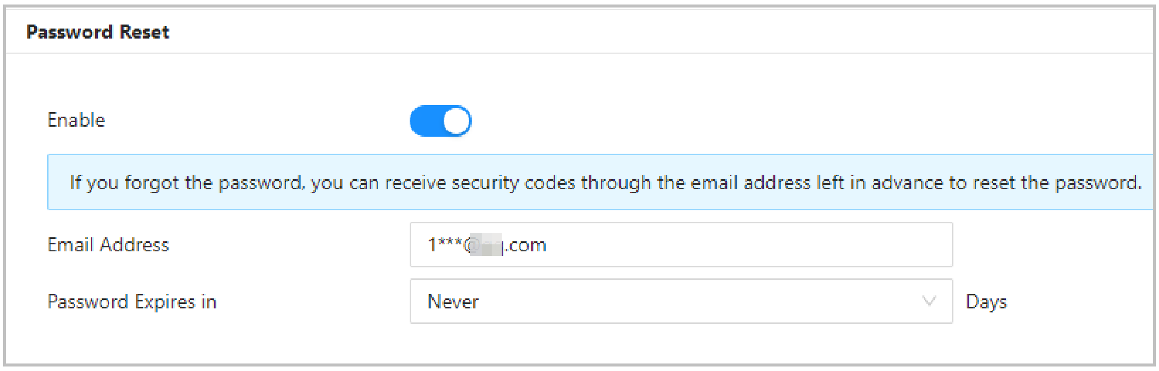
Procedure

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

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

Step 3 Turn on the password reset function.

Figure 3-34 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**.

3.8.2 Viewing Online Users

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

3.8.3 Configuring Time

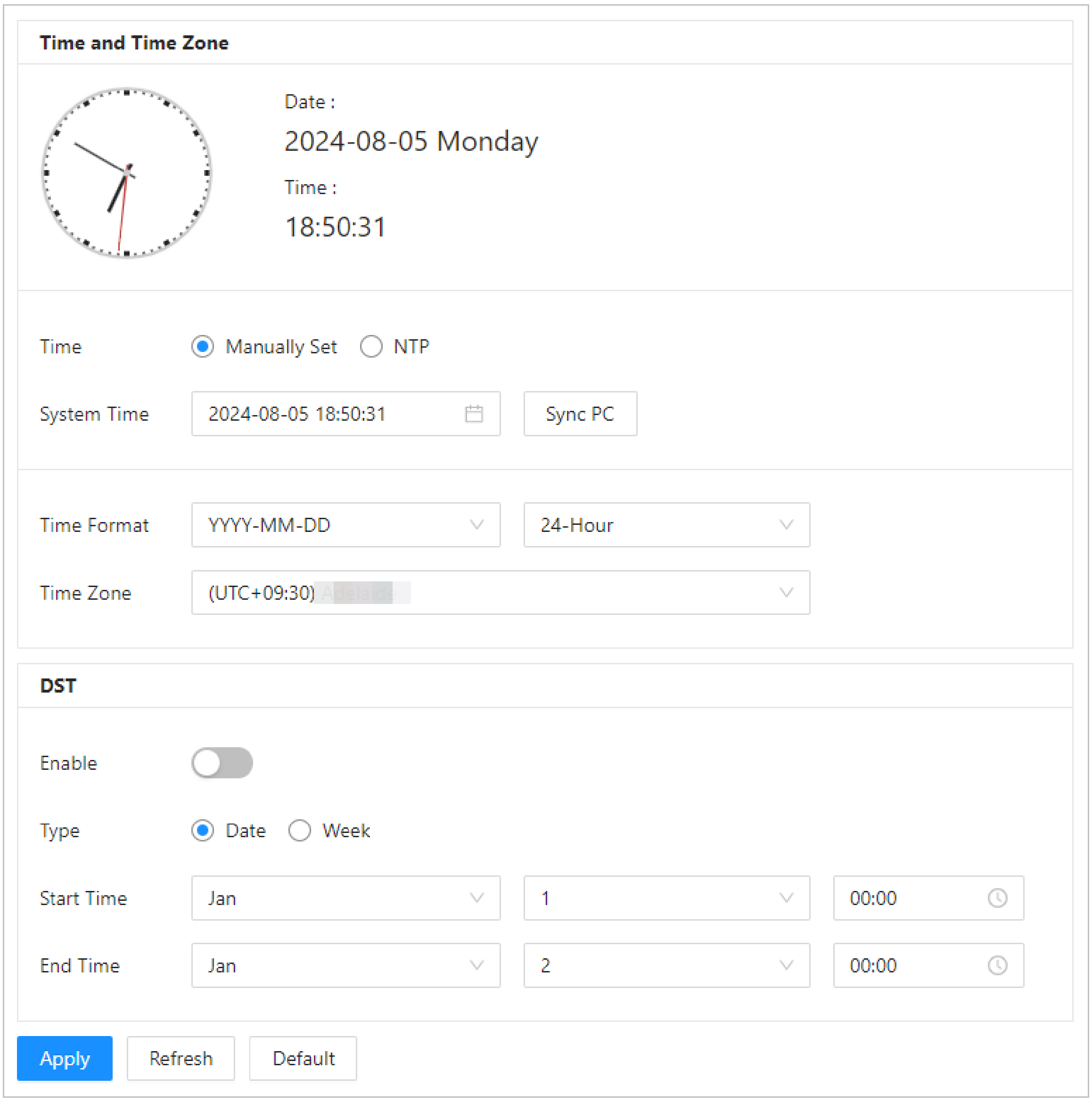
Procedure

Step 1 Log in to the webpage.

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

Step 3 Configure the time of the Platform.

Figure 3-35 Time settings



Time and Time Zone

Date :

2024-08-05 Monday

Time :

18:50:31

Time ● Manually Set ○ NTP

System Time 2024-08-05 18:50:31

Time Format YYYY-MM-DD 24-Hour

Time Zone (UTC+09:30) [redacted]

DST

Enable

Type ● Date ○ Week

Start Time Jan 1 00:00

End Time Jan 2 00:00

Table 3-19 Time settings description

Parameter	Description
Time	● Manual Set: Manually enter the time or you can click **Sync PC** 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	Select the time zone.

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

Step 4 Click **Apply**.

3.9 Maintenance Center

3.9.1 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**.

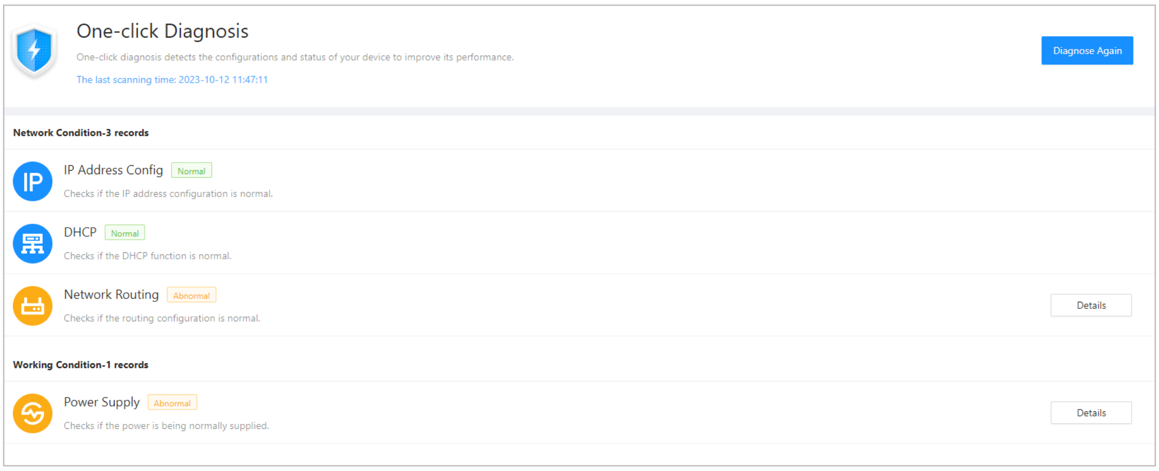
Step 2 Click **Diagnose**.

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 3-36 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.

3.9.2 System Information

3.9.2.1 Viewing Version Information

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

3.9.2.2 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.

3.9.3 Data Capacity

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

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

3.9.4 Viewing Logs

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

3.9.4.1 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.

3.9.4.2 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.

3.9.4.3 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**.

3.9.4.4 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.

3.9.5 Maintenance Management

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

3.9.5.1 Exporting and Importing Configuration Files

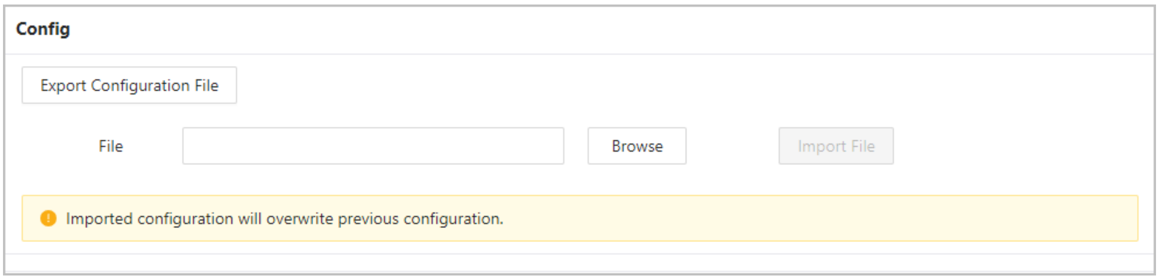
You can import and export the configuration file for the Device. When you want to apply the same configurations to multiple devices, you can import the configuration file to them.

Procedure

Step 1 Log in to the webpage.

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

Figure 3-37 Configuration management


Config
Export Configuration File
File
Browse
Import File
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.

3.9.5.2 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

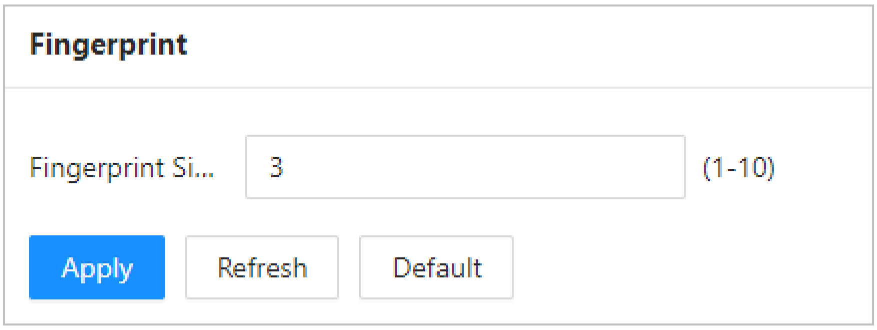
Step 1 Log in to the webpage.

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 3-38 Fingerprint similarity threshold



Fingerprint

Fingerprint Si... 3 (1-10)

3.9.5.3 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.

3.9.5.4 Maintenance

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

Procedure

Step 1 Log in to the webpage.

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

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

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

3.9.6 Updating the System

⚠

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

3.9.6.1 File Update

Procedure

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

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

🕮

The update file should be a .bin file.

Step 3 Click **Update**.

The Device will restart after the update finishes.

3.9.6.2 Online Update

Procedure

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

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

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

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

3.9.7 Advanced Maintenance

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

3.9.7.1 Exporting

Procedure

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

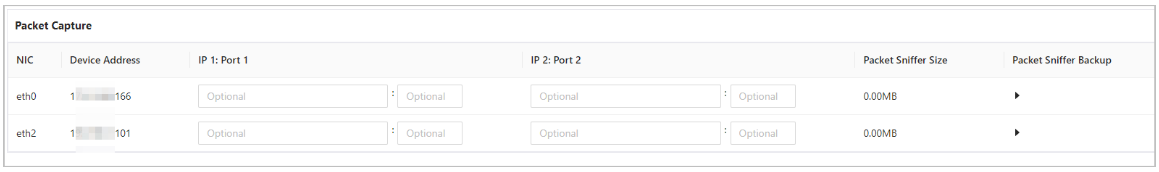
Step 2 Click **Export** to export the serial number, firmware version, device operation logs and configuration information.

3.9.7.2 Packet Capture

Procedure

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

Figure 3-39 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.

3.10 Security Settings(Optional)

3.10.1 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.

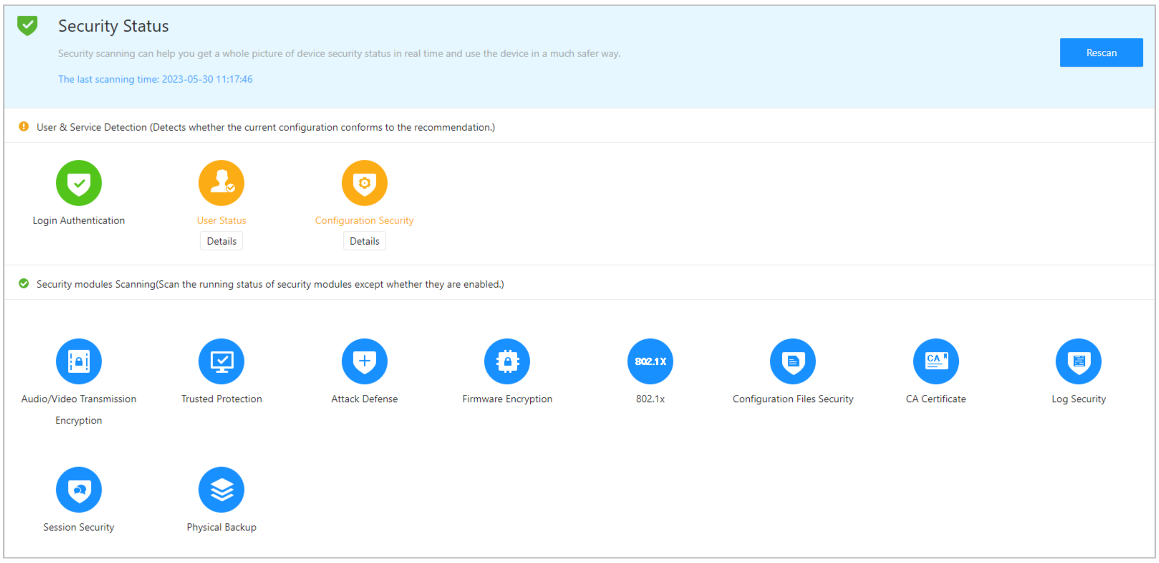
Procedure

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 3-40 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

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

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

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.

3.10.2 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.

⚠

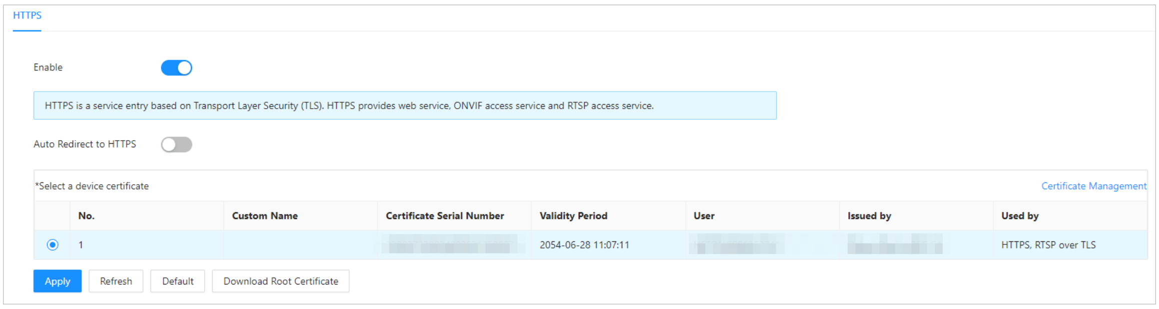
If you turn on the compatible with TLS v1.1 and earlier versions, security risks might occur. Please be advised.

Step 3 Select the certificate.

📖

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

Figure 3-41 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

Certificate Management

	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.

3.10.3 Attack Defense

3.10.3.1 Configuring Firewall

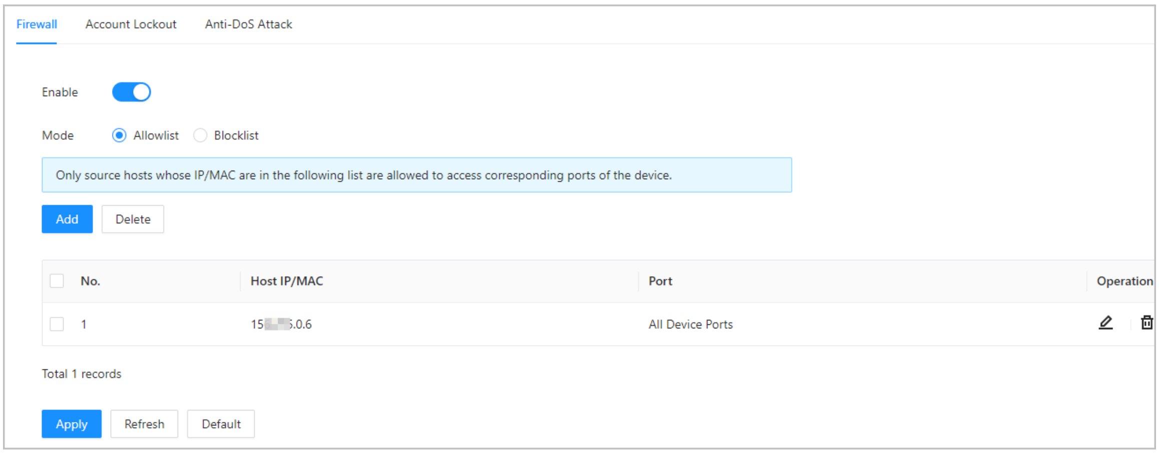
Configure firewall to limit access to the Device.

Procedure

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

Step 2 Click ○ to enable the firewall function.

Figure 3-42 Firewall



Enable

Mode ● Allowlist ○ Blocklist

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

□	No.	Host IP/MAC	Port	Operation
□	1	15[redacted]5.0.6	All Device Ports	✎ 🗑

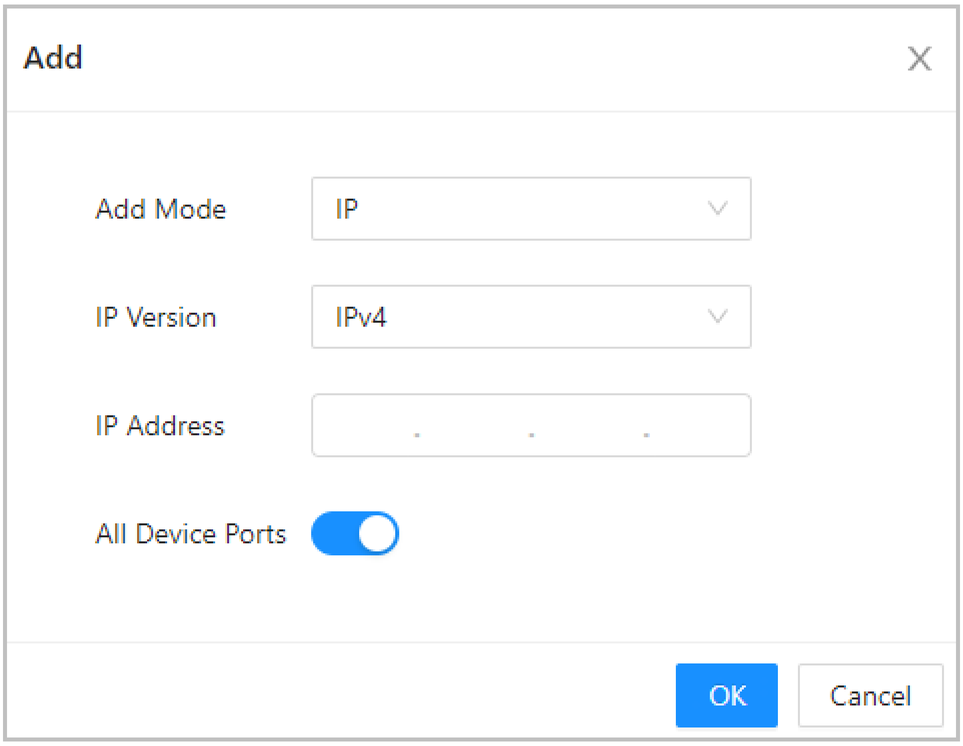
Total 1 records

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 3-43 Add IP information



Add

Add Mode: IP

IP Version: IPv4

IP Address: . . .

All Device Ports: ●

Step 5 Click **OK**.

Related Operations

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

3.10.3.2 Configuring Account Lockout

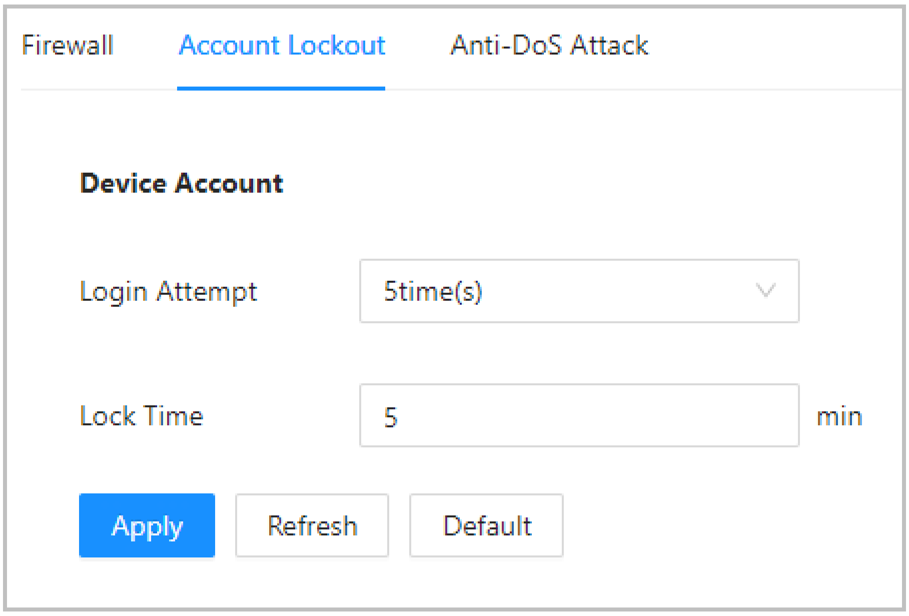
If the incorrect password is entered for a defined number of times, the account will be locked.

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 3-44 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**.

3.10.3.3 Configuring Anti-DoS Attack

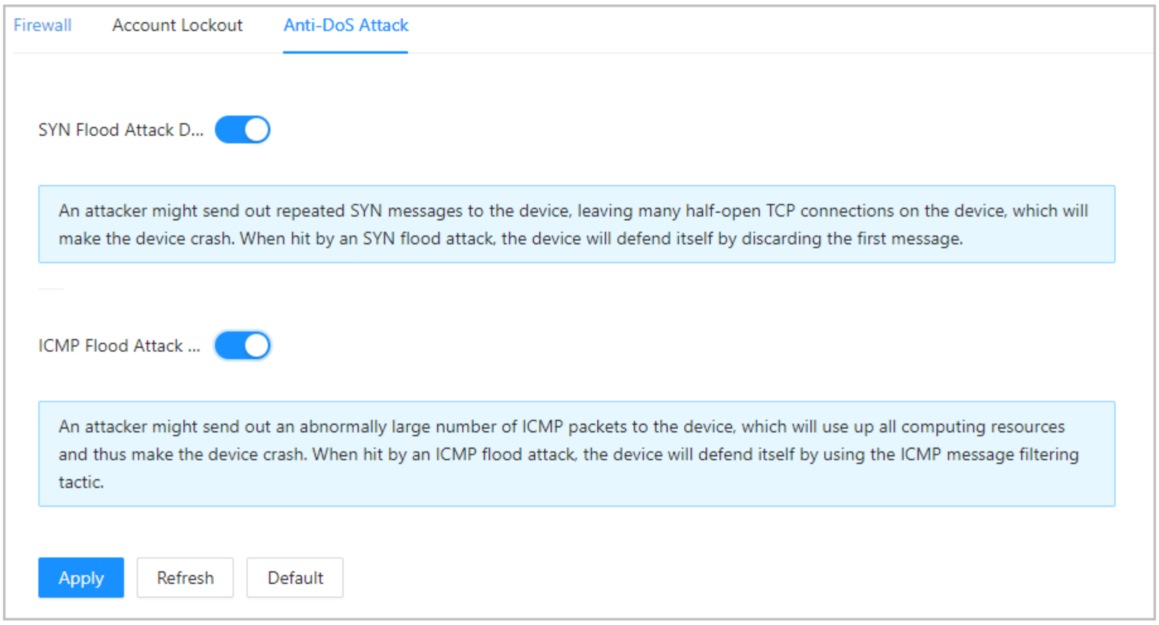
You can enable **SYN Flood Attack Defense** and **ICMP Flood Attack Defense** to defend the Device against Dos attacks.

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 3-45 Anti-DoS attack



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.

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**.

3.10.4 Installing Device Certificate

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

3.10.4.1 Creating Certificate

Create a certificate for the Device.

Procedure

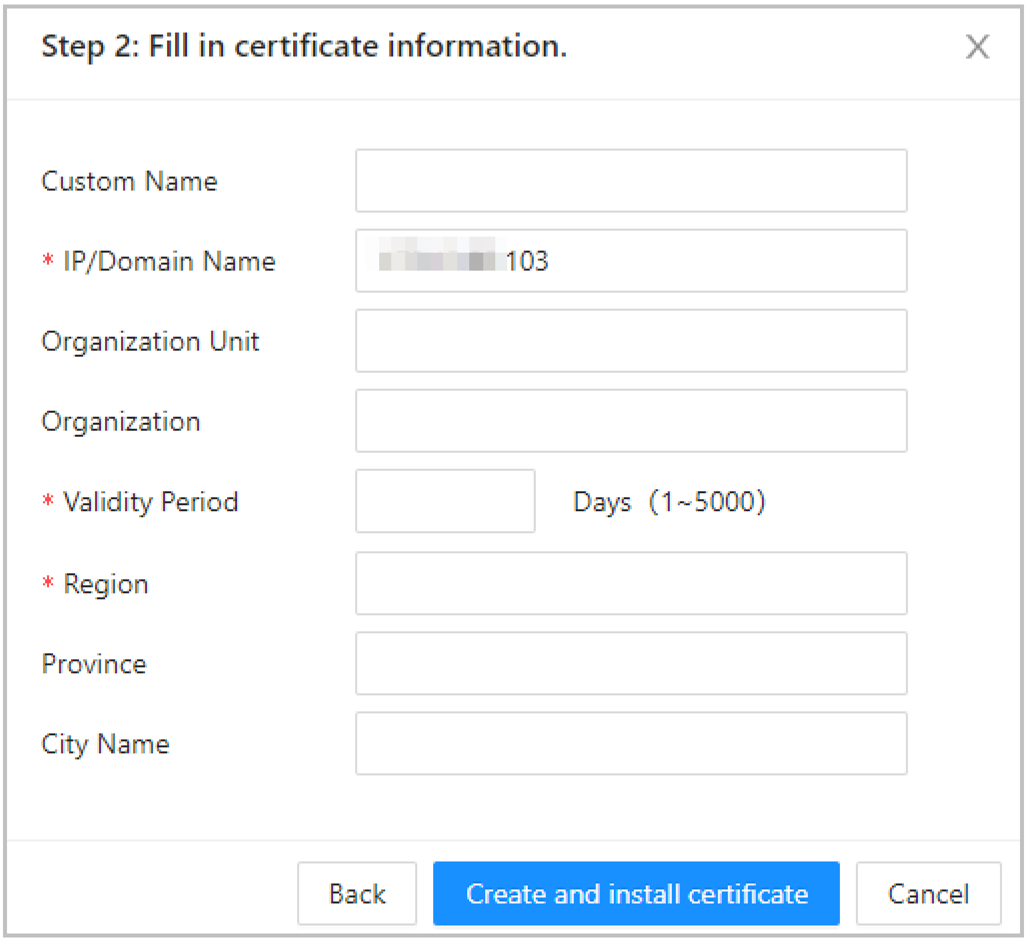
Step 1 Select ⛨ > **CA Certificate** > **Device Certificate**.

Step 2 Select **Install Device Certificate**.

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

Step 4 Enter the certificate information.

Figure 3-46 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.

3.10.4.2 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**.

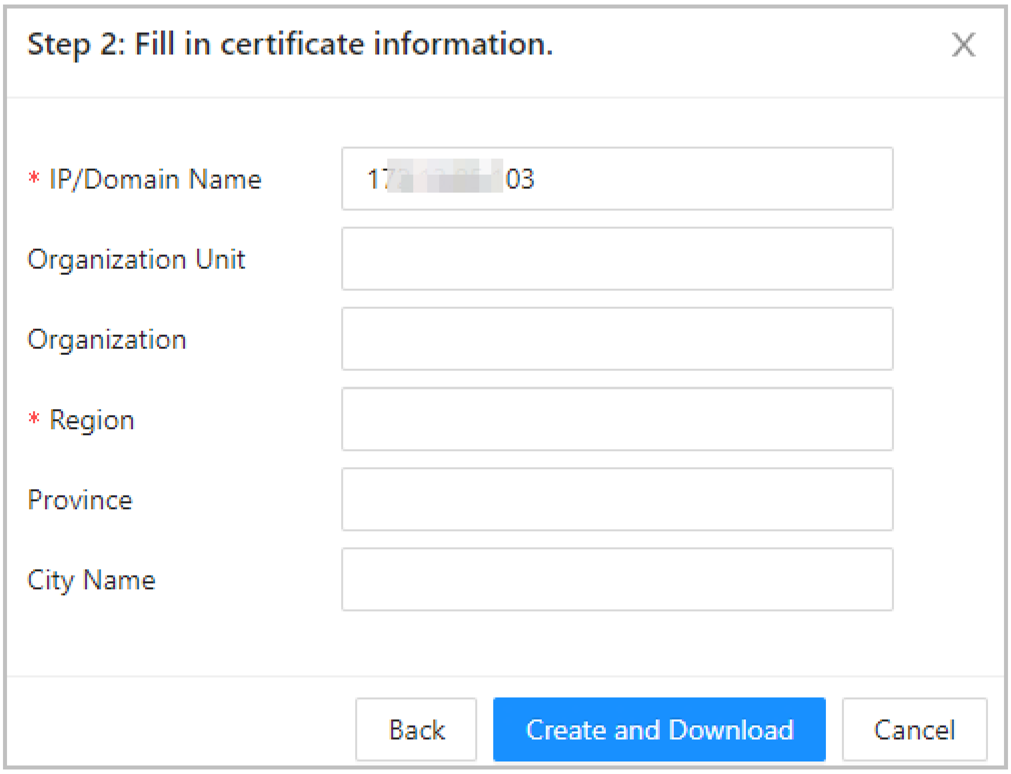
Step 3 Select **Apply for CA Certificate and Import (Recommended)** , and click **Next**.

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 3-47 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.

3.10.4.3 Installing Existing Certificate

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

Procedure

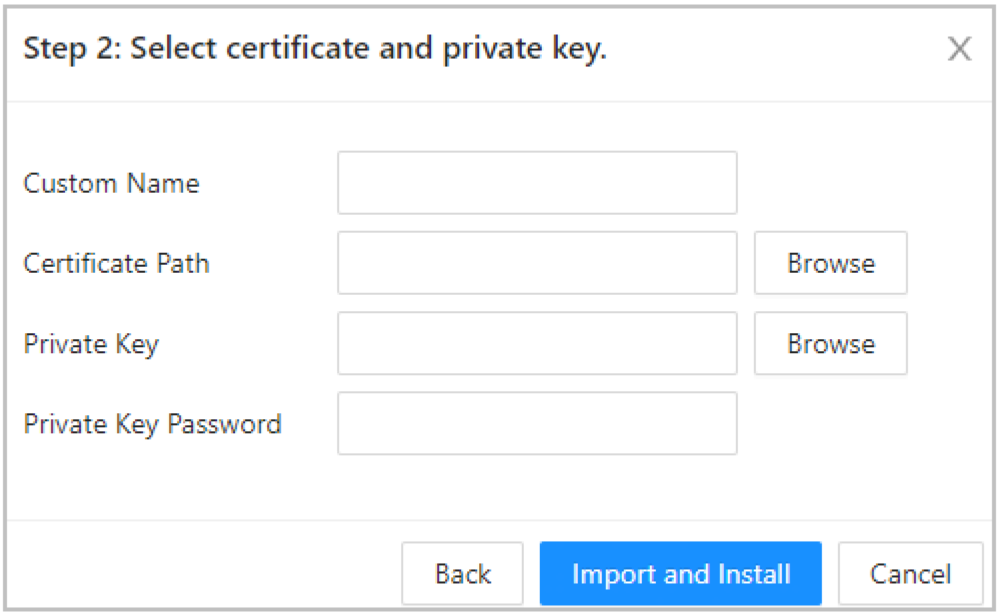
Step 1 Select **Security** > **CA Certificate** > **Device Certificate**.

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 3-48 Certificate and private key



Step 5 Click **Import and Install**.

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

Related Operations

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

3.10.5 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.

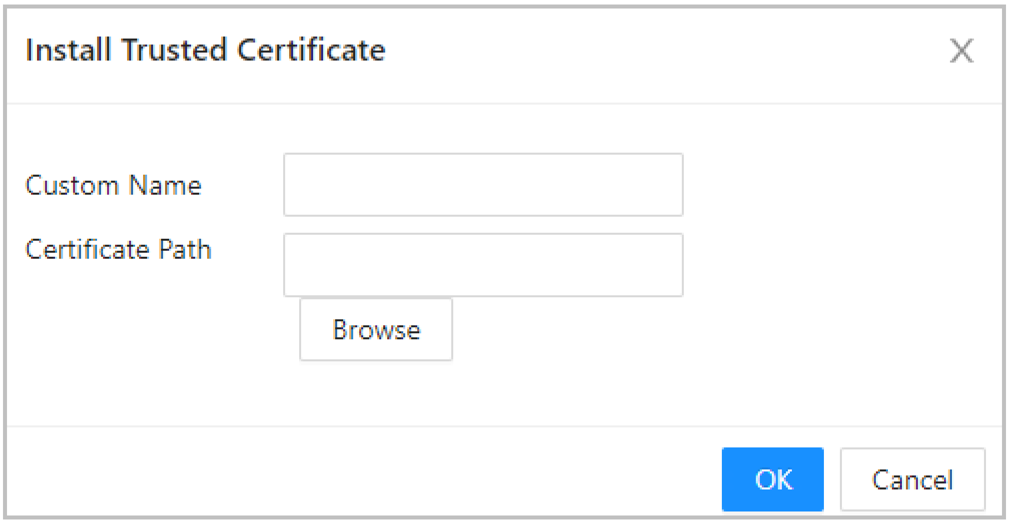
Procedure

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

Step 2 Select **Install Trusted Certificate**.

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

Figure 3-49 Install the trusted certificate



Step 4 Click **OK**.

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

Related Operations

- Click **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.

3.10.6 Security Warning

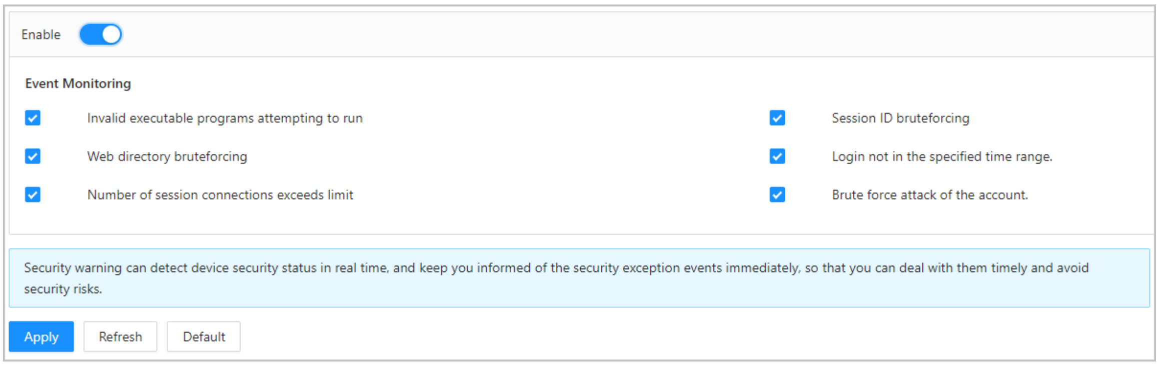
Procedure

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

Step 2 Enable the security warning function.

Step 3 Select the monitoring items.

Figure 3-50 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**.

3.10.7 Security Authentication

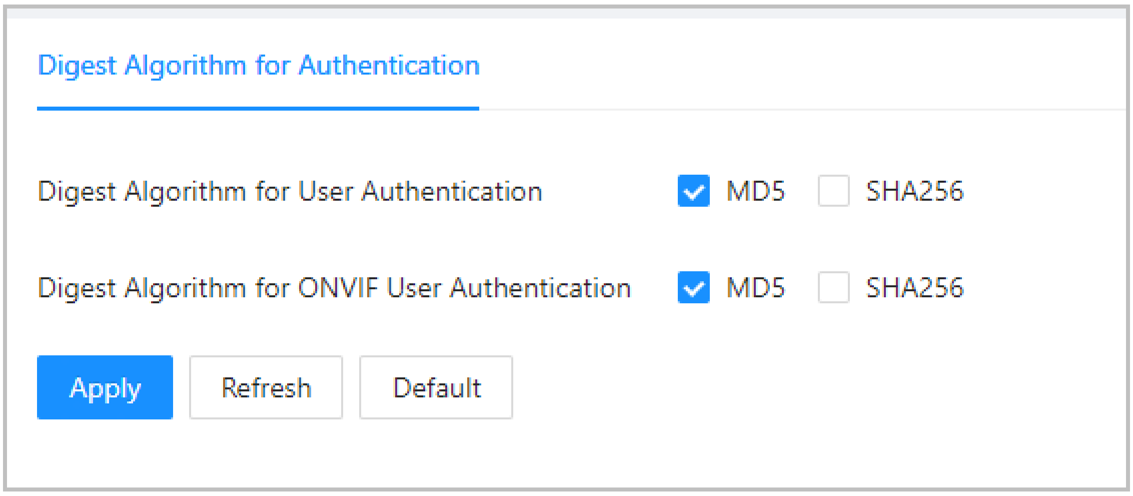
Procedure

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

Step 2 Select a message digest algorithm.

Step 3 Click **Apply**.

Figure 3-51 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 Initialization

When the phone is on the same LAN as the Access Controller, you can initialize the Access Controller for the first time or after the Device is restored to the factory defaults on the webpage of the phone.

Prerequisites

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

There are mainly 3 ways to connect the Device and the phone to the same network. This section introduces initialization on the phone through Wi-Fi AP.

- Connect the Device to the network through the network cable. Make sure the phone and the Device are on 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 Wi-Fi and Wi-Fi AP are available on select models.

Procedure

Step 1 Power on the Access Controller.

Step 2 Connect to the Wi-Fi hotspot on your phone. The hotspot name is **product serial number + device model**.

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

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

Step 4 Tap **Starting initialization**.

Step 5 Enter and confirm the password, enter an email address.

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

Step 6 (Optional) Enable the e-mail address, and then configure the address.

If you want to reset the administrator password by scanning the QR code, you need to enable the e-mail function and configure the e-mail address to receive the security code.

Step 7 (Optional) Select **I have read and agree Software License Agreement Privacy Policy**.

Step 8 Tap **Next**.

Step 9 Enable **Auto Check for Updates** as needed, and then tap **Completed**.

The login page is displayed.

4.2 Logging in to the Webpage

Prerequisites

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

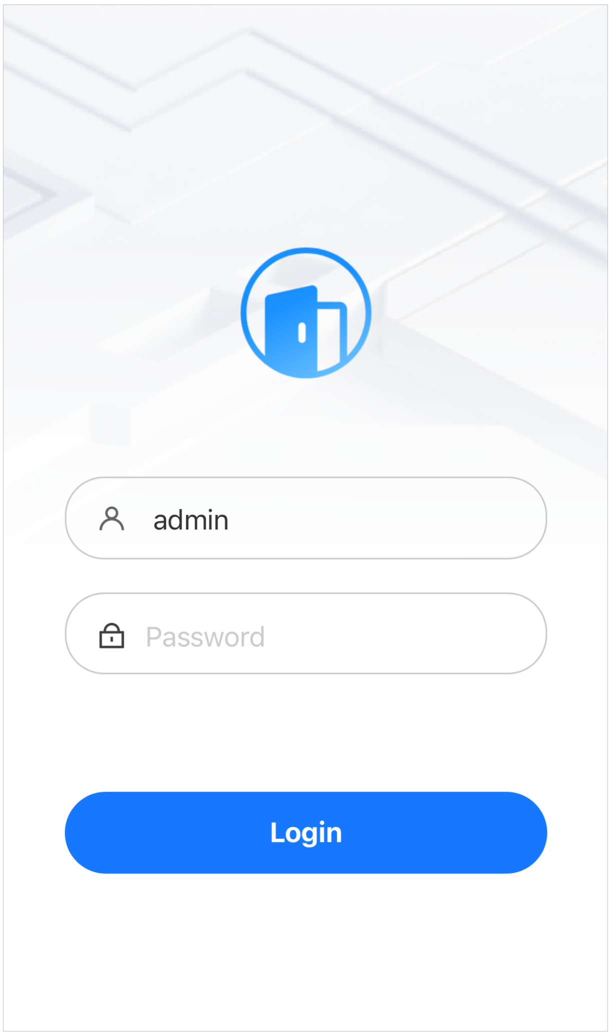
Procedure

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

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.

Figure 4-1 Login page



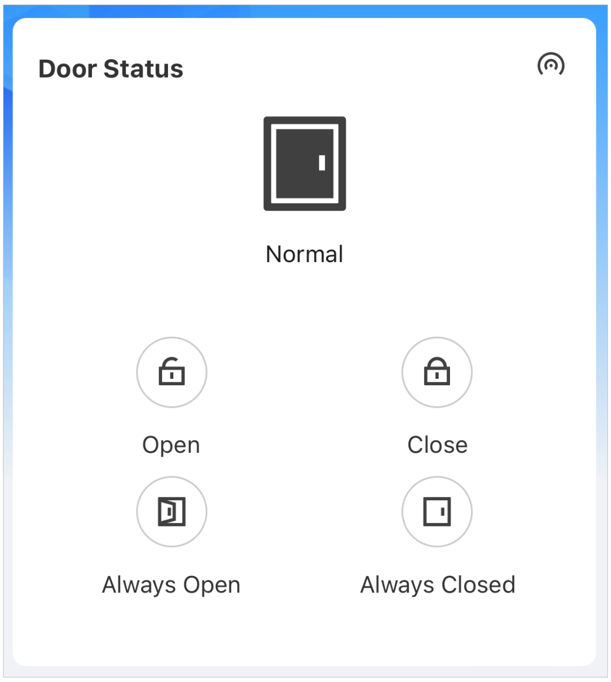
Step 3 Click **Login**.

4.3 Home Page

The home page is displayed after you successfully log in.

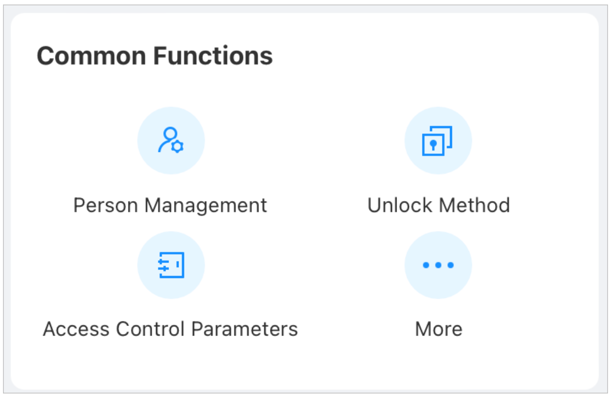
- The **Door Status** area displays the status of the door. You can remotely open or close the door. You can also configure the door status as **Always Open** or **Always Closed**.

Figure 4-2 Door status



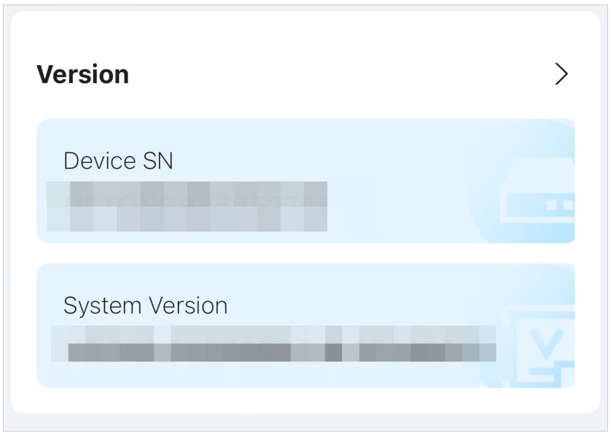
- The **Common Function** area displays the configuration menu of the Device. Click **More** to view all the configuration menus.

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

4.4 Person Management

Add the person and configure the permissions.

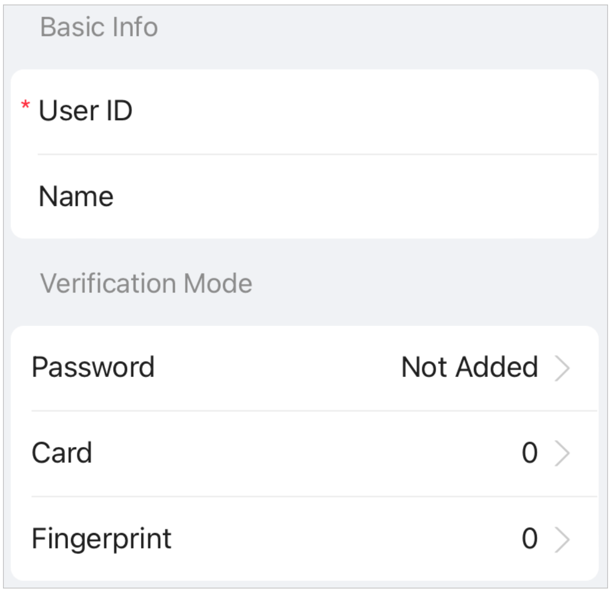
Procedure

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

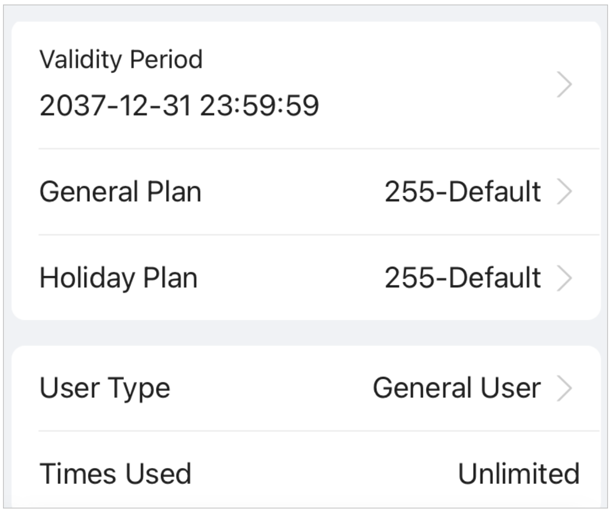
Verification Mode

Password Not Added

Card 0

Fingerprint 0

Figure 4-6 Add the person (2)



Validity Period

2037-12-31 23:59:59

General Plan: 255-Default

Holiday Plan: 255-Default

User Type: General User

Times Used: Unlimited

Table 4-1 Parameters description

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

Parameter	Description
Card	● Enter the card number manually. 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
General Plan	People can unlock the door or take attendance during the defined period. You can select more than one plan.
Holiday Plan	People can unlock the door or take attendance during the defined holiday. You can select more than one holiday.
User Type	● **General User** : General users can unlock the door. ● **Blocklist User** : When users in the blocklist unlock the door, service personnel will receive a notification. ● **Guest User** : Guests can unlock the door within a defined period or for certain amount of times. After the defined period expires or the unlocking times runs out, they cannot unlock the door. ● **Patrol User** : Patrol users can take attendance on the Device, but they do not have door permissions. ● **VIP User** : When VIP unlock the door, service personnel will receive a notice. ● **Other User** : When they unlock the door, the door will stay unlocked for 5 more seconds. ● Custom User 1/Custom User 2: Same with general users.
Time Used	Set an unlock limit for guest users. After the unlock times run out, they cannot unlock the door.

Step 4 Click **Add**.

4.5 Configuring the System

4.5.1 Viewing Version Information

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

4.5.2 Maintenance

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

Procedure

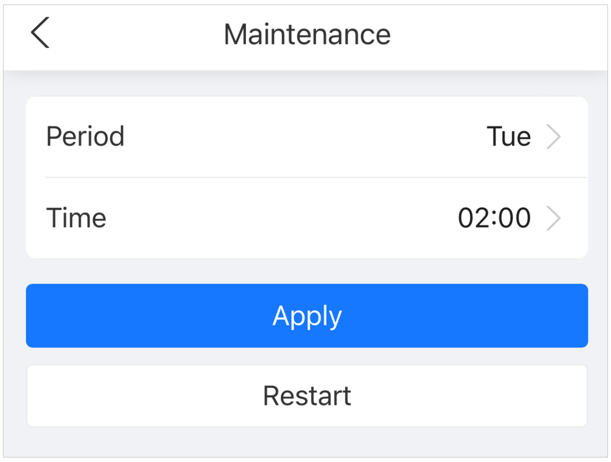
Step 1 Log in to the webpage.

Step 2 Select **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



Period: Tue

Time: 02:00

4.5.3 Configuring Time

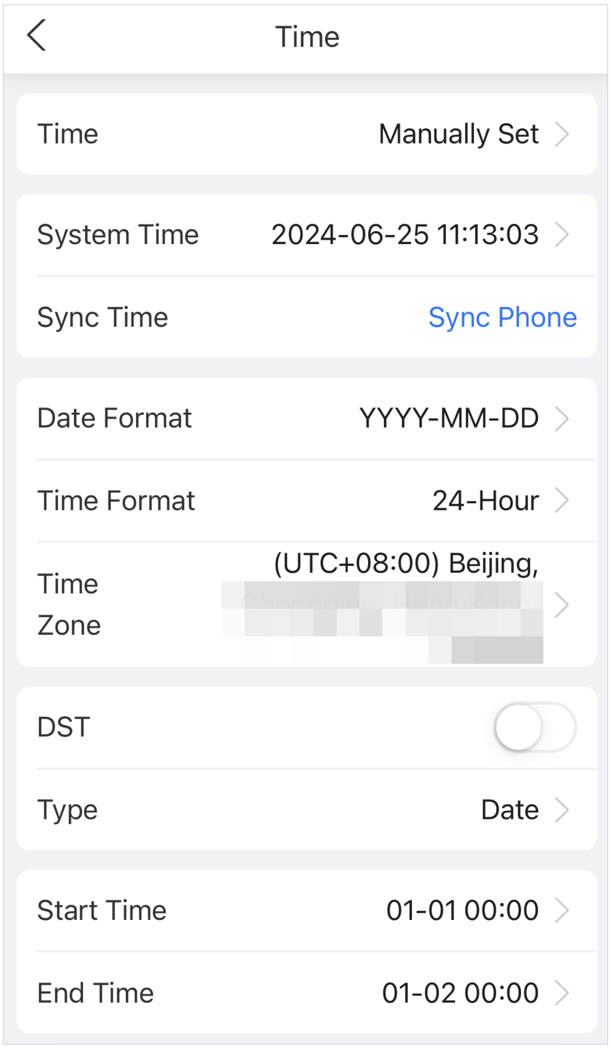
Procedure

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**.

4.5.4 Data Capacity

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

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

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.

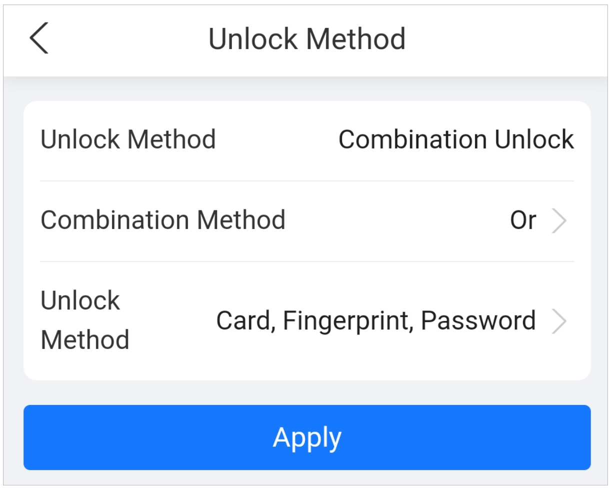
Step 2 Click **Unlock Method** on the main menu, or select **More** > **Access Control** > **Unlock Method**.

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 4-9 Unlock method



Unlock Method

Unlock Method: Combination Unlock

Combination Method: Or

Unlock Method: Card, Fingerprint, Password

4.6.2 Configuring Access Control Parameters

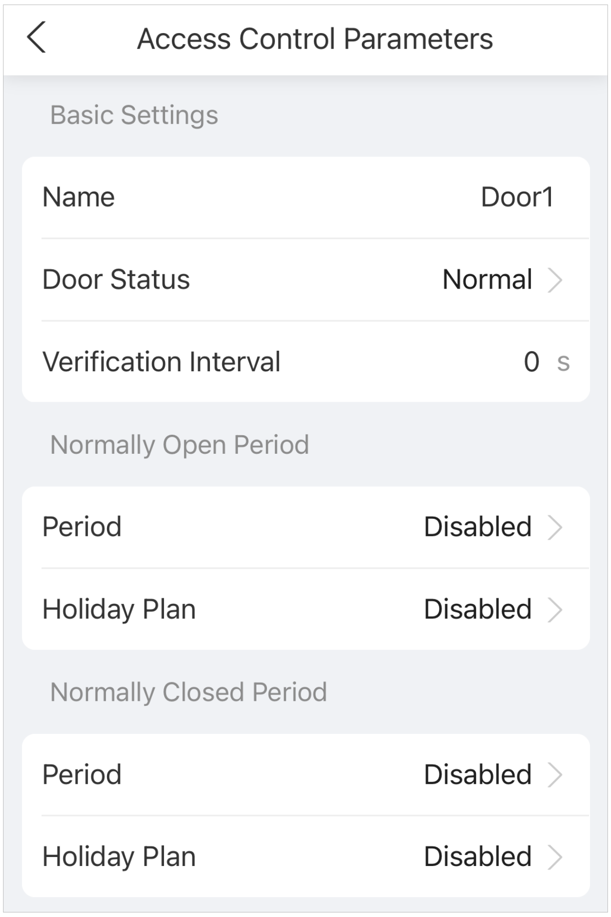
Procedure

Step 1 Log in to the webpage.

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

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

Figure 4-10 Access control parameters (1)



Access Control Parameters

Basic Settings

Name Door1

Door Status Normal

Verification Interval 0 s

Normally Open Period

Period Disabled

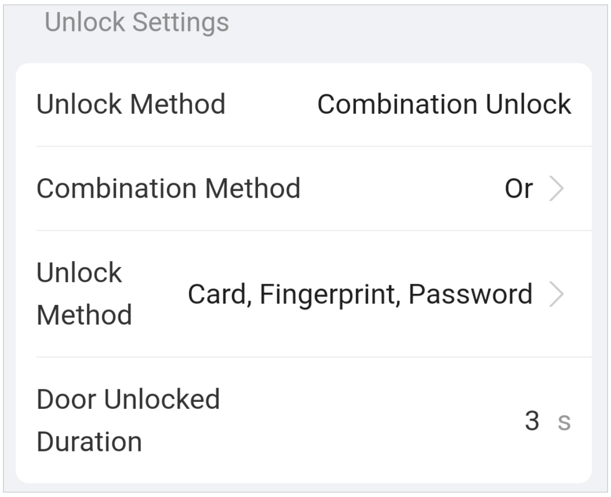
Holiday Plan Disabled

Normally Closed Period

Period Disabled

Holiday Plan Disabled

Figure 4-11 Access control parameters (2)



Unlock Settings

Unlock Method Combination Unlock

Combination Method Or

Unlock Method Card, Fingerprint, Password

Door Unlocked Duration 3 s

Table 4-3 Description of access control parameters

Parameter		Description
Basic Settings	Name	The name of the door.

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

Step 4 Click **Apply**.

4.6.3 Configuring Alarms

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

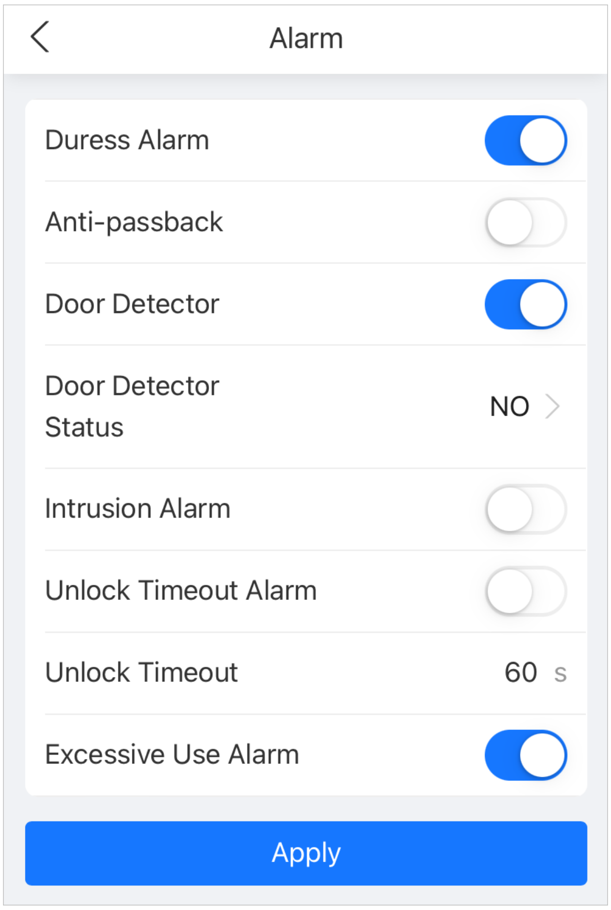
Procedure

Step 1 Log in to the webpage.

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

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

Figure 4-12 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 4-4 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 prevent 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 the person 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 the person attempt to enter again, and access is denied at the same time. 📖 If the Device can only connect one lock, verifying on the Device means entry direction, and verifying on the external card reader means exit direction by default. You can modify the setting on the management platform.
Door Detector	With the door detector wired to your device, alarm can be triggered when doors are opened or closed abnormally. The door detector includes 2 types, including NC detector and NO detector. ● NC: The sensor is in a shorted position when the door or window is closed. ● NO: An open circuit is created when the window or door is actually closed.
Intrusion Alarm	If the door is opened abnormally, an intrusion alarm will be triggered and last for a defined time. 📖 The door detector and intrusion need to be enabled at the same time.
Unlock Timeout Alarm	When the door remains unlocked for longer than the defined timeout duration, the door timeout alarm will be triggered and last for the defined time. 📖 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 last for a defined time.

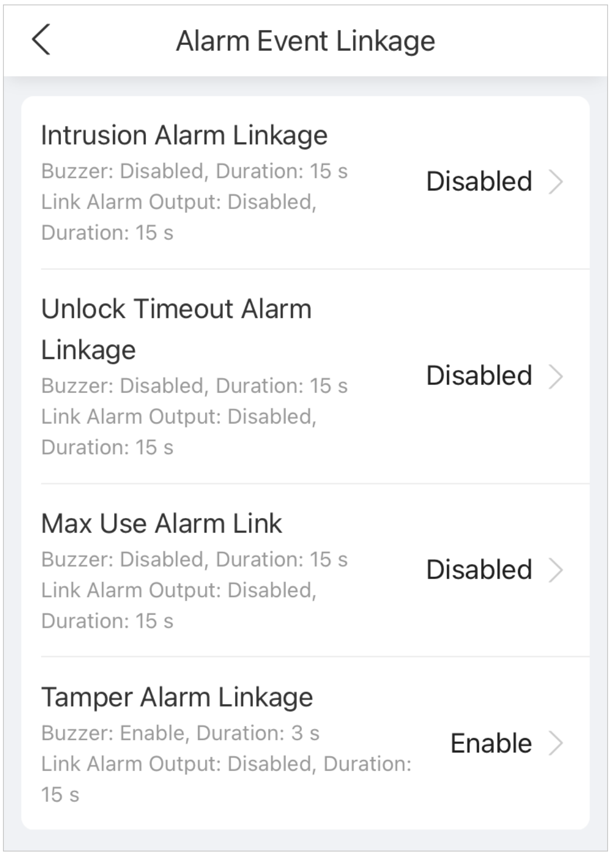
4.6.4 Configuring Alarm Event Linkage

Procedure

Step 1 Log in to the webpage.

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

Figure 4-13 Alarm event linkage



Alarm Event Linkage

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

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

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

Tamper Alarm Linkage
Buzzer: Enable, Duration: 3 s
Link Alarm Output: Disabled, Duration: 15 s
Enable

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

Table 4-5 Alarm event linkage

Parameter	Description
Intrusion Alarm Linkage	If the door is opened abnormally, an intrusion alarm will be triggered. Buzzer: The buzzer sounds when an intrusion alarm is triggered. You can configure the alarm duration.
Unlock Timeout Alarm Linkage	When the door remains unlocked for longer than the defined timeout duration, the door timeout alarm will be triggered and last for the defined time. Buzzer: The buzzer sounds when the unlock timeout alarm is triggered. You can configure the alarm duration.

Parameter	Description
Max Use Alarm Link	If the wrong password or card is used 5 times in a row within 60 seconds, the alarm for excessive use of illegal card will be triggered and lasts for a defined time. Buzzer: The buzzer sounds when the excessive use alarm is triggered. You can configure the alarm duration.
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. ● Local Alarm Output: The external alarm device generates alarms when the tamper alarm is triggered. You can configure the alarm duration.

4.6.5 Configuring Card Settings

Background Information

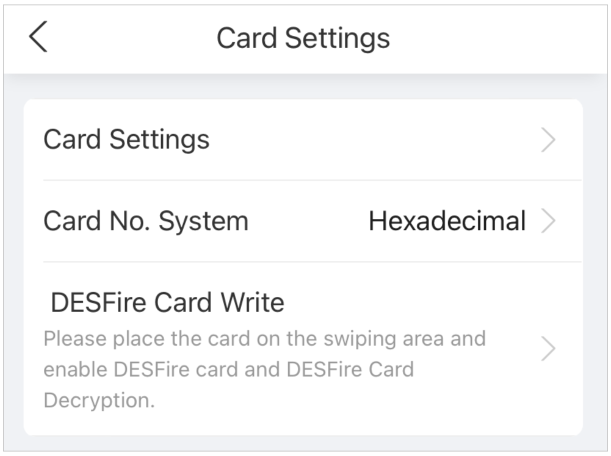
Procedure

Step 1 Log in to the webpage.

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

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

Figure 4-14 Card settings



Card Settings

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.

Table 4-6 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 and **IC Card** are enabled at the same time. 📖 ● 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 **IC Card** , **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**.

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.

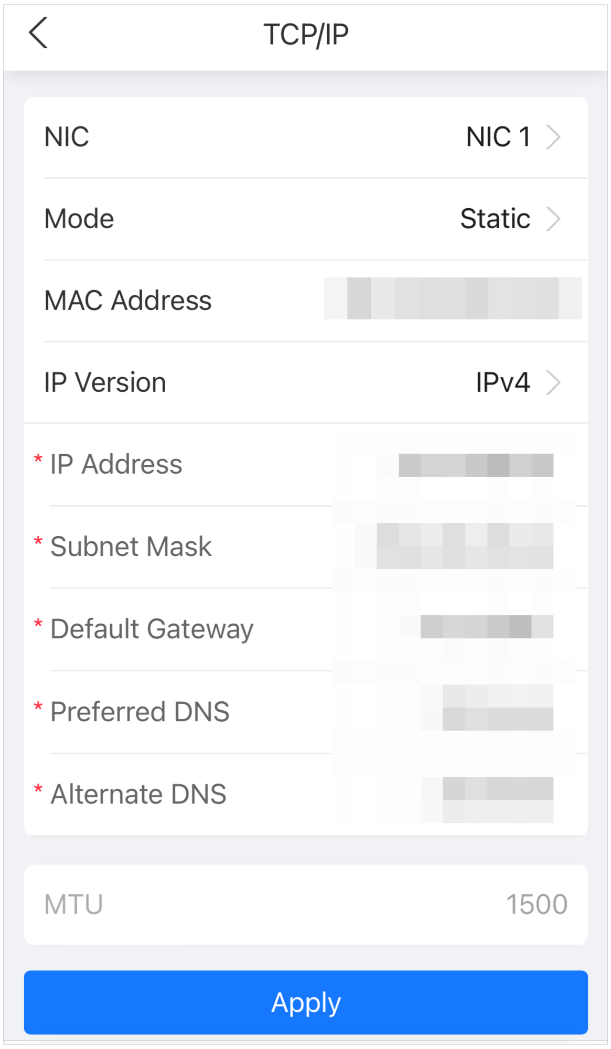
Procedure

Step 1 Log in to the webpage.

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

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

Figure 4-15 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 4-7 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	
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.

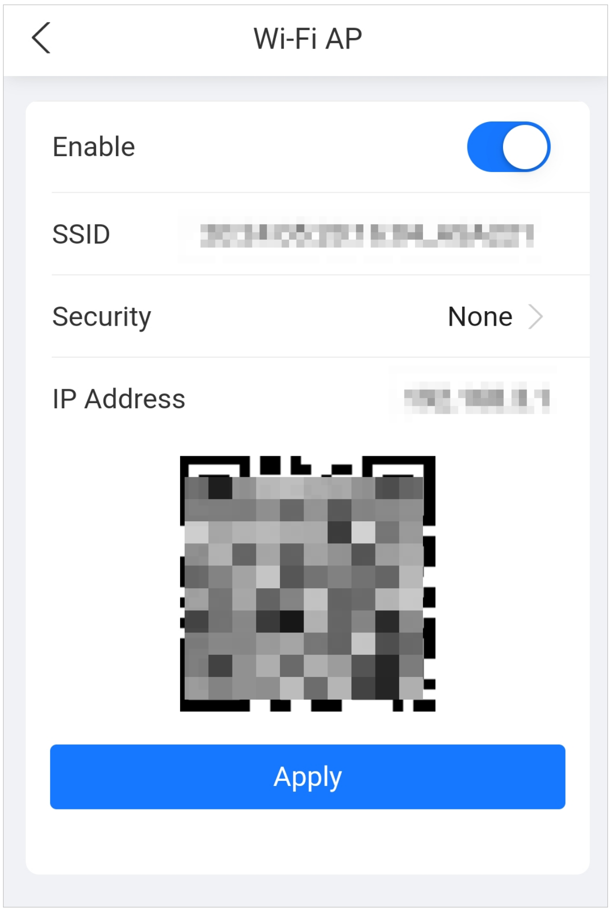
Procedure

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 4-16 Wi-Fi AP



Wi-Fi AP

Enable: on

SSID

Security: None

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

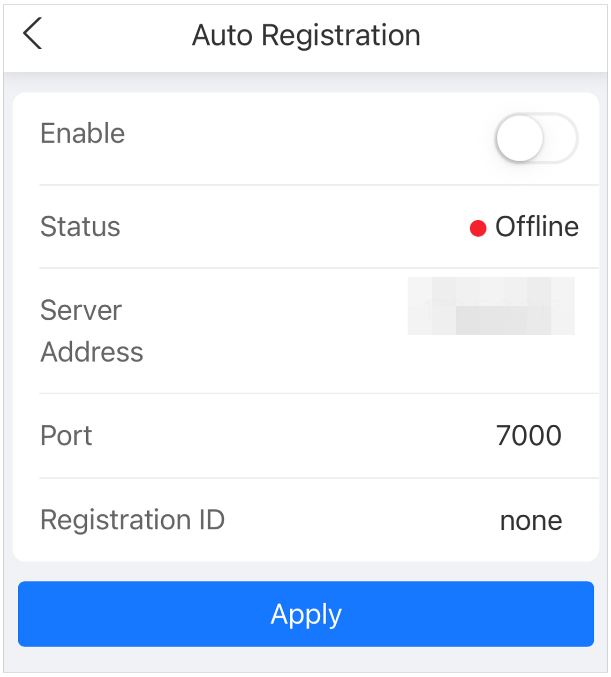
Procedure

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 4-17 Auto registration



Auto Registration

Enable ○

Status ● Offline

Server Address

Port 7000

Registration ID none

Table 4-8 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.

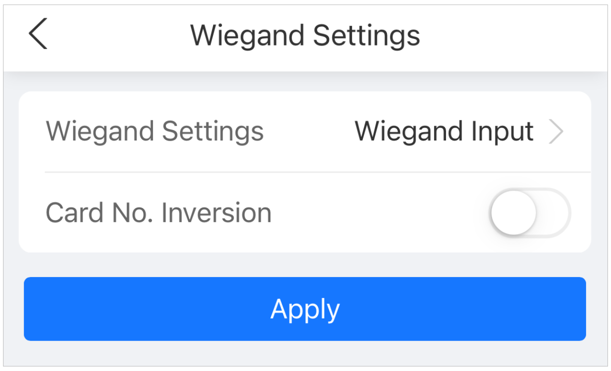
Step 2 Select **More** > **Communication Settings** > **Wiegand**.

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 4-18 Wiegand input

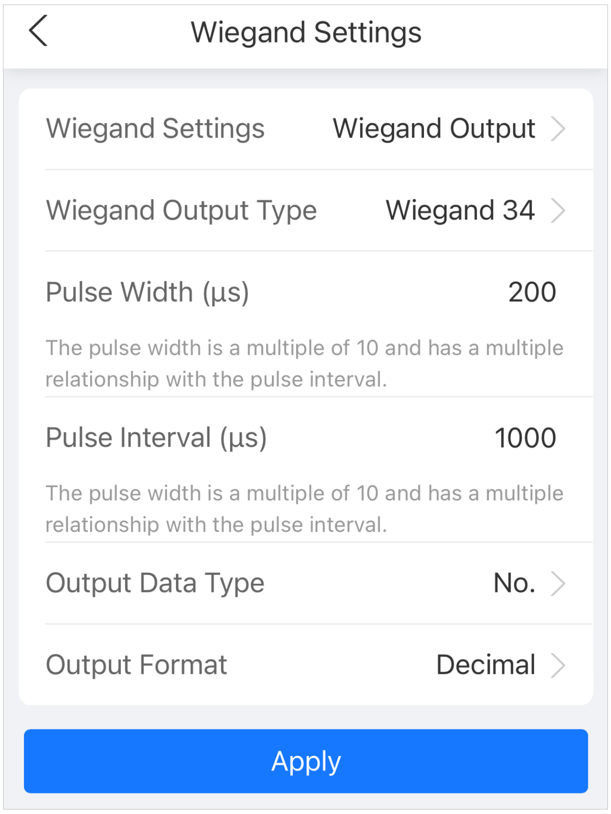


Wiegand Settings: Wiegand Input

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 4-19 Wiegand output



Wiegand Settings

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 4-9 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.

4.7.7 Configuring RS-485

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

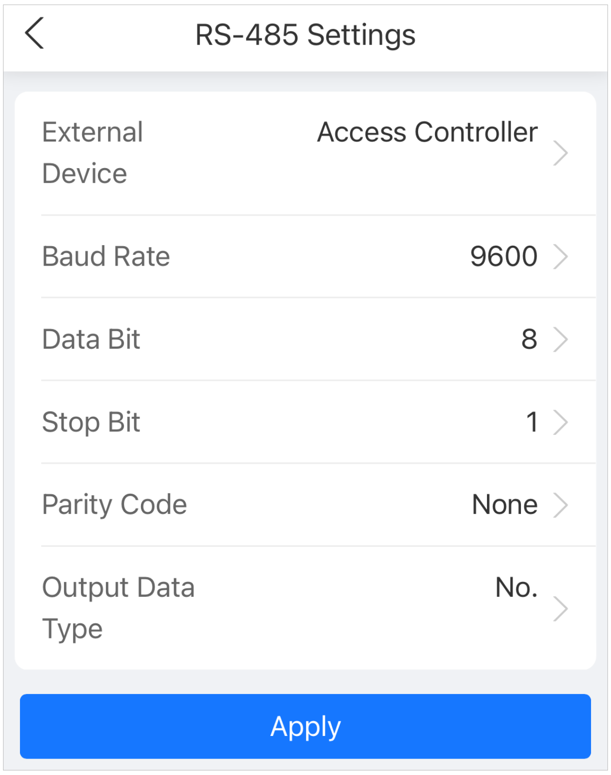
Procedure

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 4-20 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 4-10 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. ◇ **Authentication by Local Device** : The identity is verified on both the Device and the controller. ◇ **Authentication by Controller** : The identity is verified only on the controller. ● 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.

Parameter	Description
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 Viewing Logs

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

4.8.1 System Logs

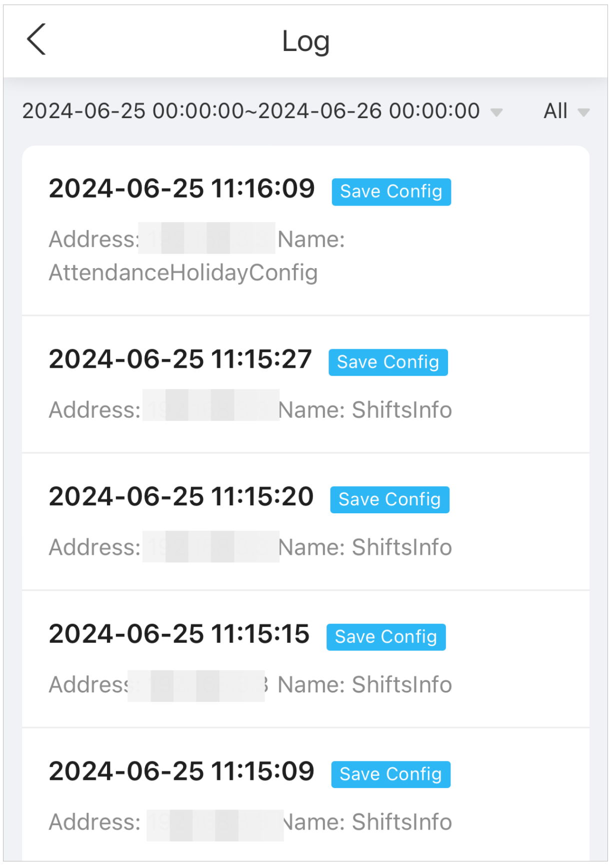
View and search for system logs.

Procedure

Step 1 Log in to the webpage.

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

Figure 4-21 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

4.8.2 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.

4.8.3 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 Installation

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

5.2 Initialization

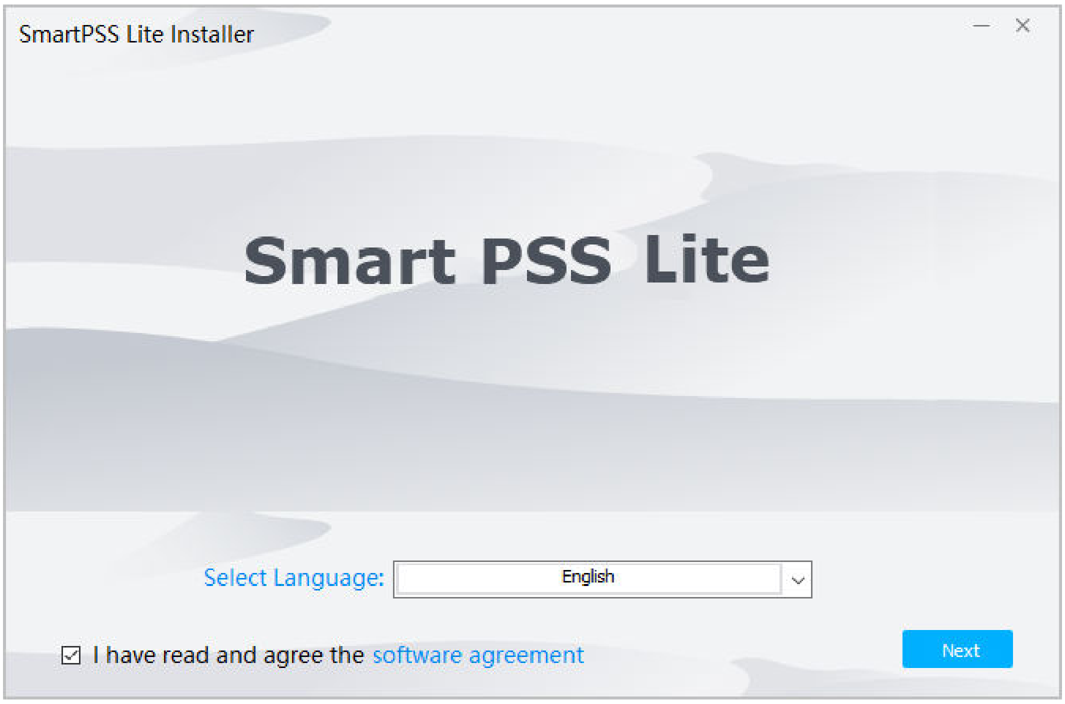
Initialize SmartPSS Lite when you log in for the first time, including setting a password for login and security questions for resetting password.

Procedure

Step 1 Double-click SmartPSSLite.exe.

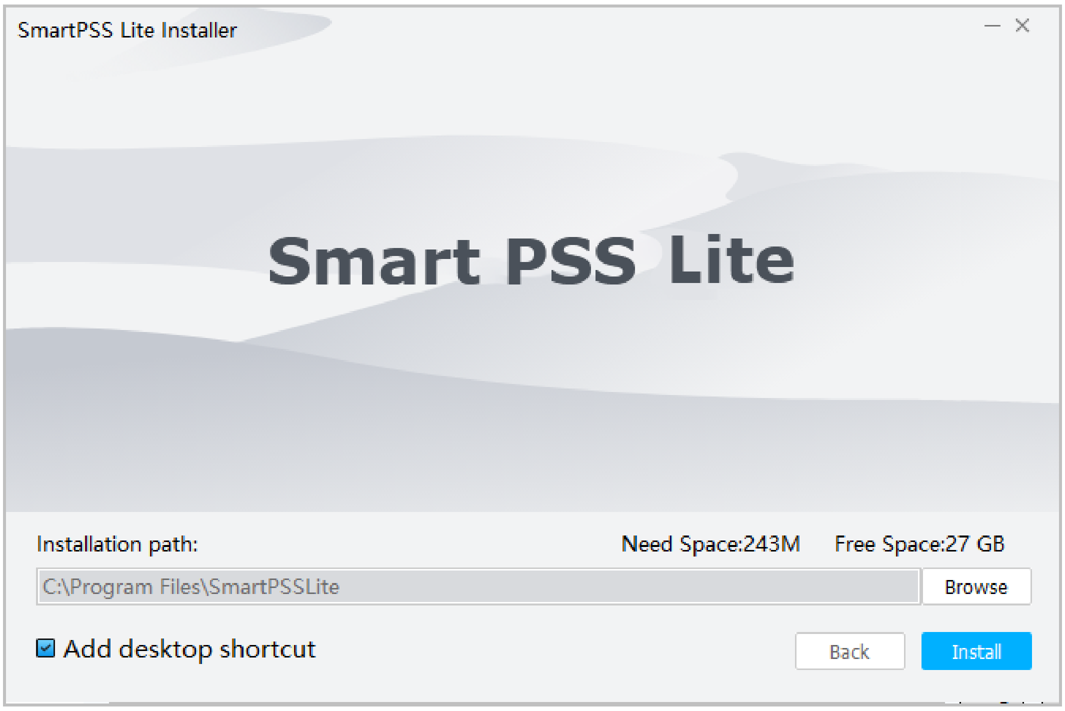
Step 2 Select the language from the drop-down list, select **I have read and agree the software agreement** , and then click **Next**.

Figure 5-1 Select language



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

Figure 5-2 Select installation path



Installation path: C:\Program Files\SmartPSSLite

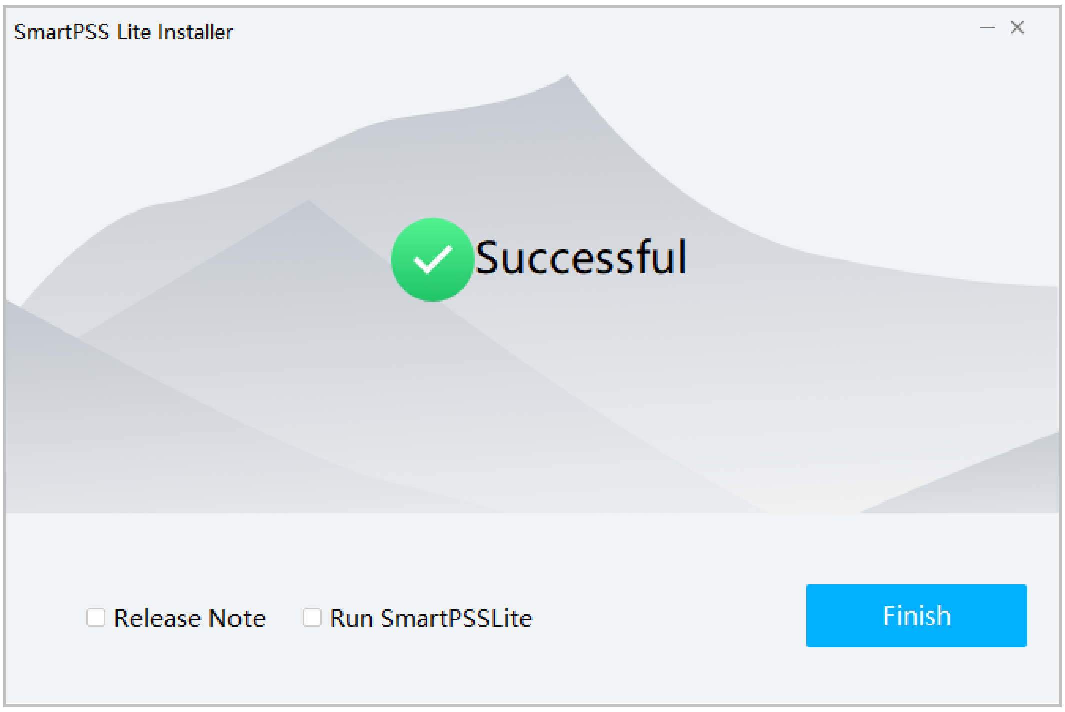
☑ Add desktop shortcut

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

📖

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

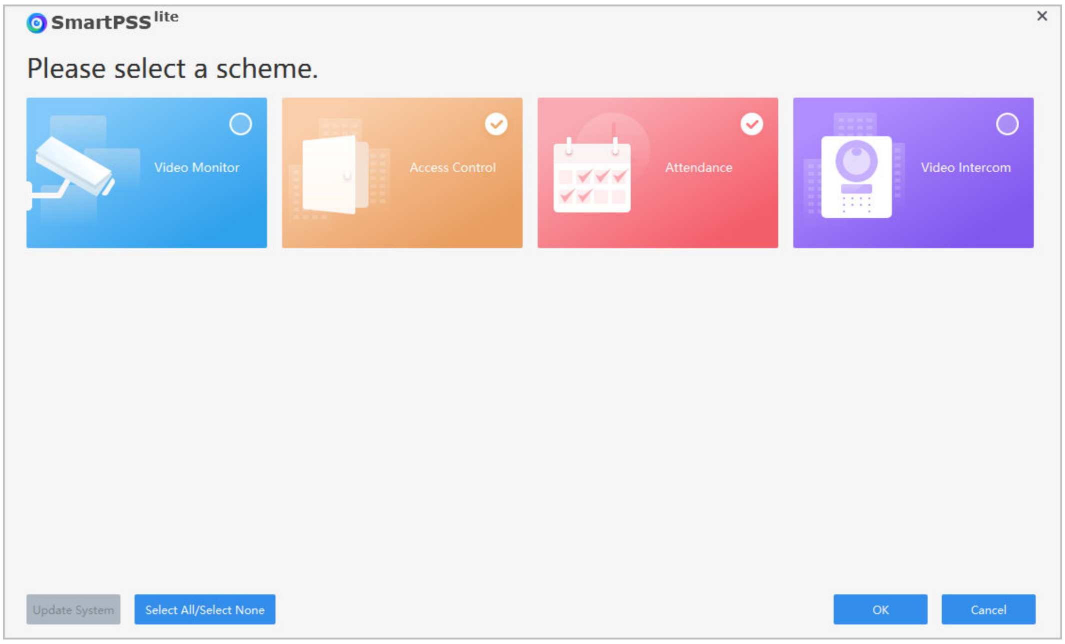
Figure 5-3 Install complete



□ Release Note □ Run SmartPSSLite

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

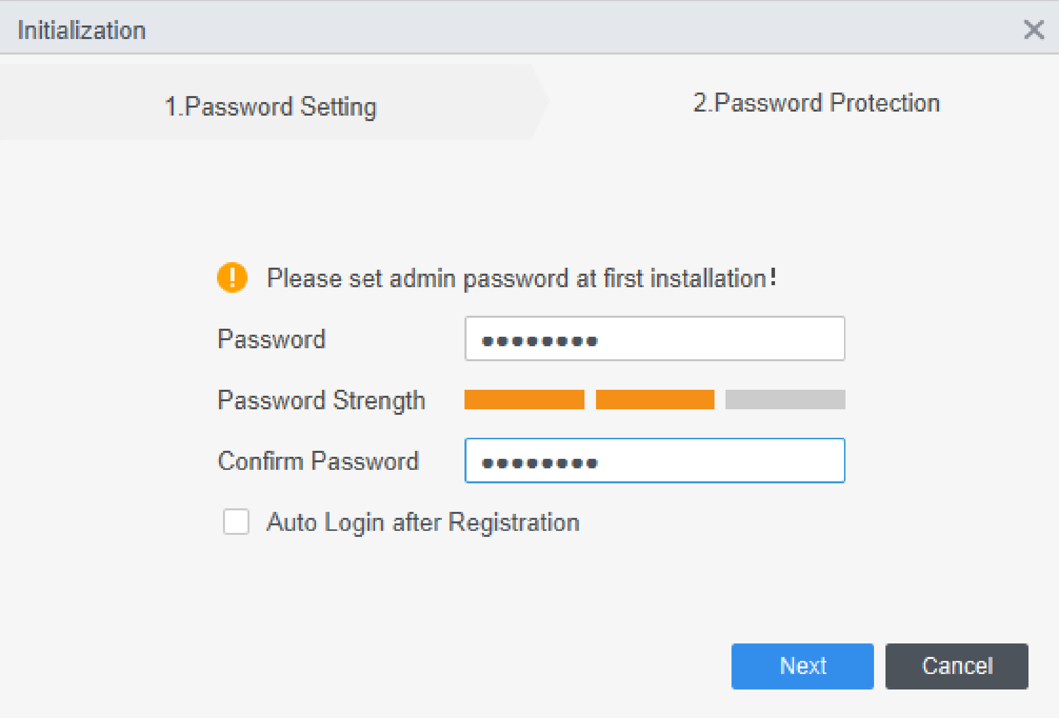
Figure 5-4 Select application scenes



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

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

Figure 5-5 Set password



Please set admin password at first installation!

Password ●●●●●●●●

Password Strength

Confirm Password ●●●●●●●●

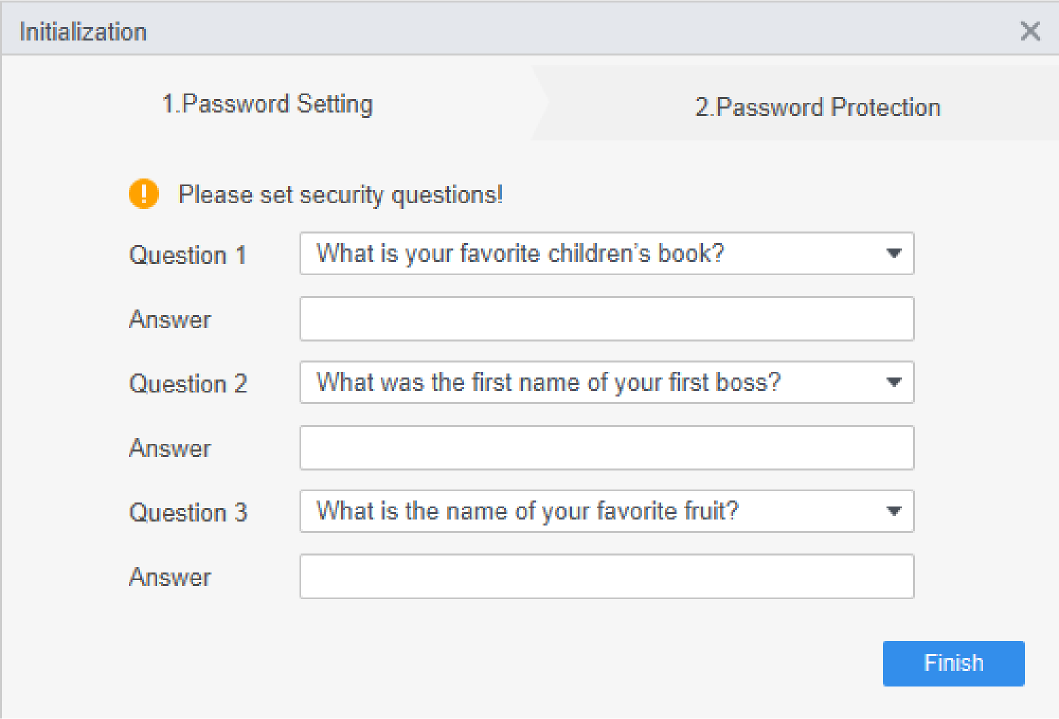
□ Auto Login after Registration

Table 5-1 Initialization parameters

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

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

Figure 5-6 Set security questions



Initialization

1.Password Setting

2.Password Protection

Please set security questions!

Question 1: What is your favorite children's book?

Answer:

Question 2: What was the first name of your first boss?

Answer:

Question 3: What is the name of your favorite fruit?

Answer:

5.3 Adding Devices

There are several methods available to add devices.

- Automatically search
- Manually adding
- Import in batches

5.3.1 Adding Device by Searching

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

Background Information

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

Procedure

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

Step 2 Select a search method.

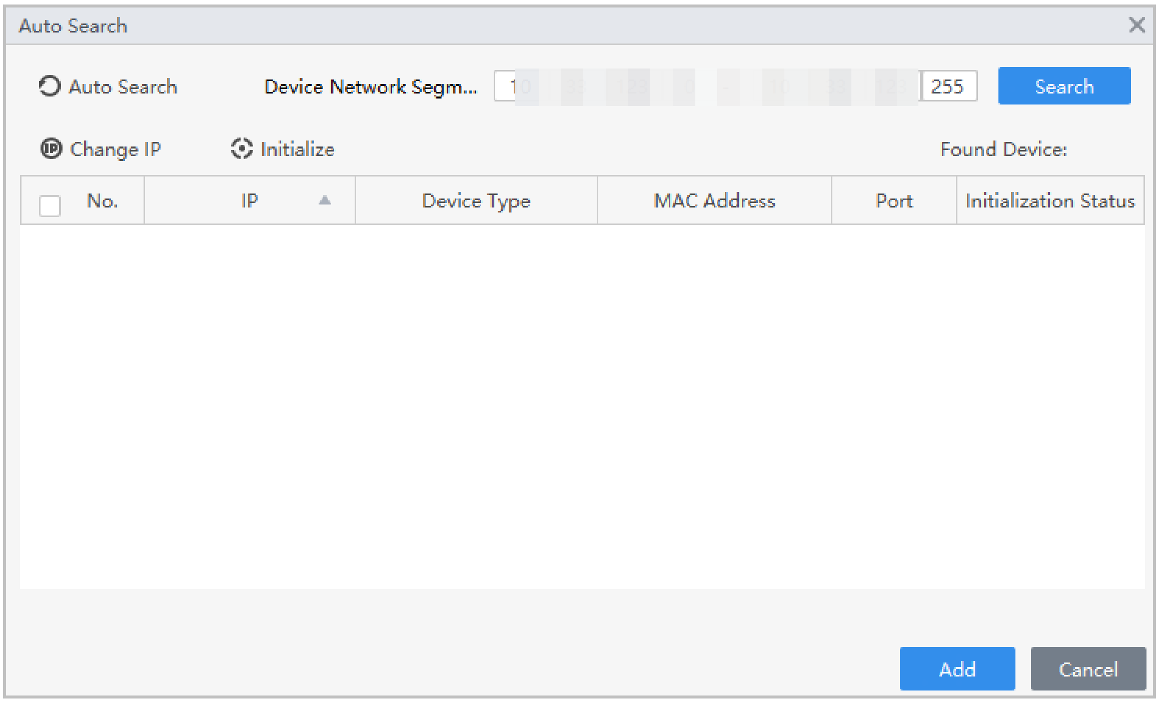
- Auto Search: Enter the username and the password of the device. The system will automatically search for devices that are on the same network to your computer.
- Device Network Segment: Enter the username and the password of the device, and then define the start IP and the end IP. The system will automatically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

Step 3 Click **Auto Search**.

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

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

Figure 5-7 Search for devices



□ No.	IP	Device Type	MAC Address	Port	Initialization Status

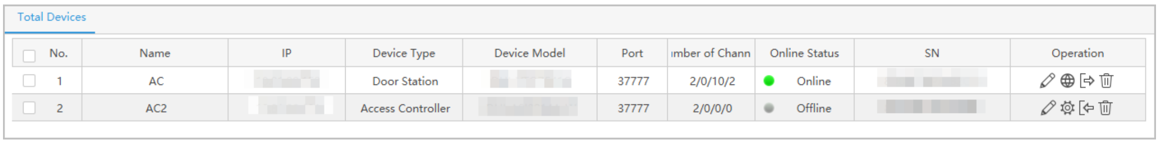
Step 5 Select devices, and then click **Add**.

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

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

The devices will be added to the platform.

Figure 5-8 Added devices



Total Devices

□ No.	Name	IP	Device Type	Device Model	Port	ımber of Chann	Online Status	SN	Operation
□ 1	AC	[redacted]	Door Station	[redacted]	37777	2/0/10/2	● Online	[redacted]	✎ 🌐 ⇨ 🗑
□ 2	AC2	[redacted]	Access Controller	[redacted]	37777	2/0/0/0	● Offline	[redacted]	✎ ⚙ ⇦ 🗑

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

Related Operations

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

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

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

5.3.2 Adding Device One by One

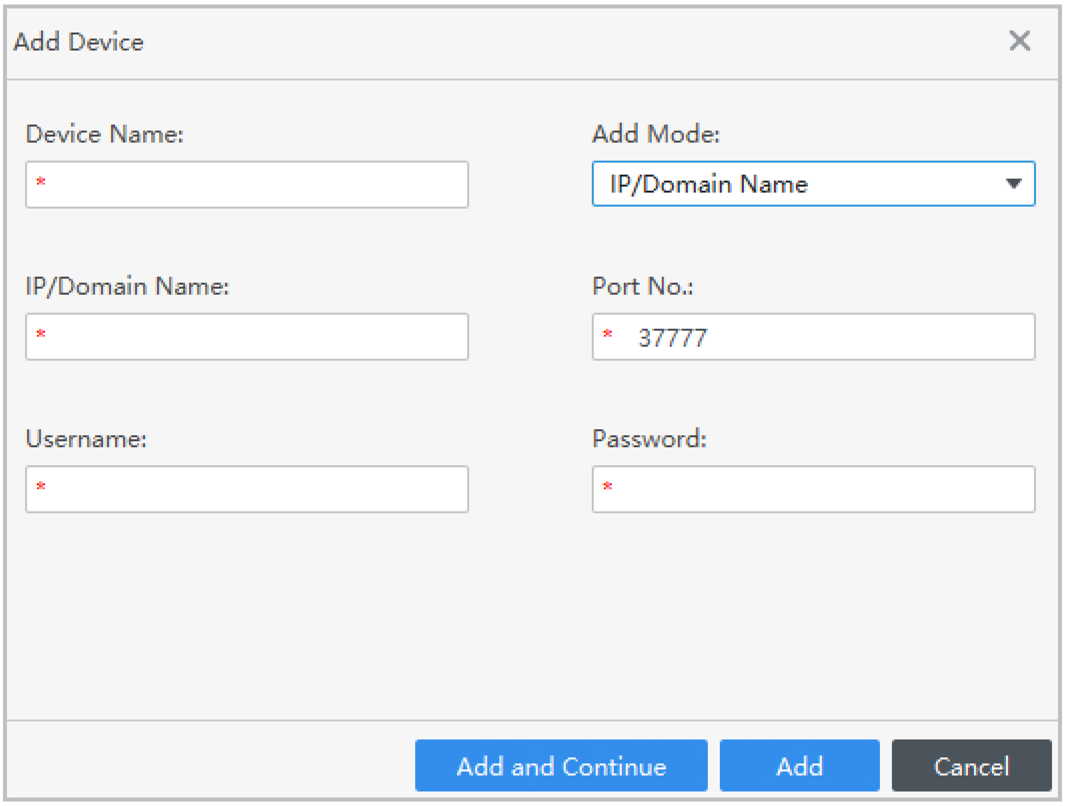
If you already know the IP address of a device, you can manually add it to the platform.

Procedure

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

Step 2 Click **Add**, and then enter the device information.

Figure 5-9 Add devices



Add Device

Device Name: *

Add Mode: IP/Domain Name

IP/Domain Name: *

Port No.: * 37777

Username: *

Password: *

Table 5-2 Parameters of IP adding

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

Step 3 Click **Add**.

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

5.3.3 Importing Device in Batches

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

Prerequisites

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

Procedure

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

Step 2 Click **Import** to import the file the platform.

Devices will be logged in automatically after adding.

5.4 User Management

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

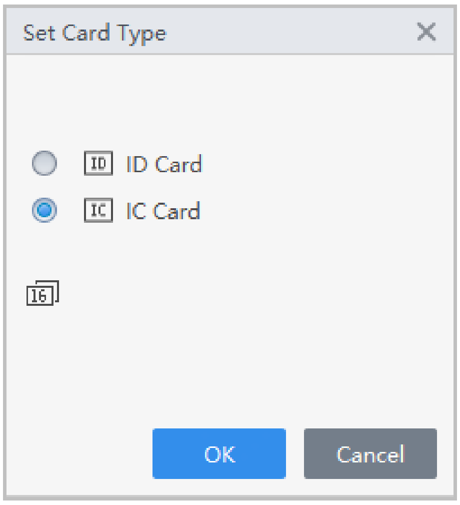
5.4.1 Setting Card Type

Select **Person** > **Person Management**, and then **Card Type**.

Before issuing card, set card type first. For example, if the issued card is ID card, select type as ID card.

The system uses hexadecimal card number by default. Click 16 to change it to decimal card number.

Figure 5-10 Set card type



○ ID ID Card

● IC IC Card

5.4.2 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**.

5.4.3 Adding Users

5.4.3.1 Adding Personnel One by One

Procedure

Step 1 Select **Person** > **Person Management**, and then click **Add**.

Step 2 Enter basic information of person.

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

- Set password

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

- Configure card

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

  📖

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

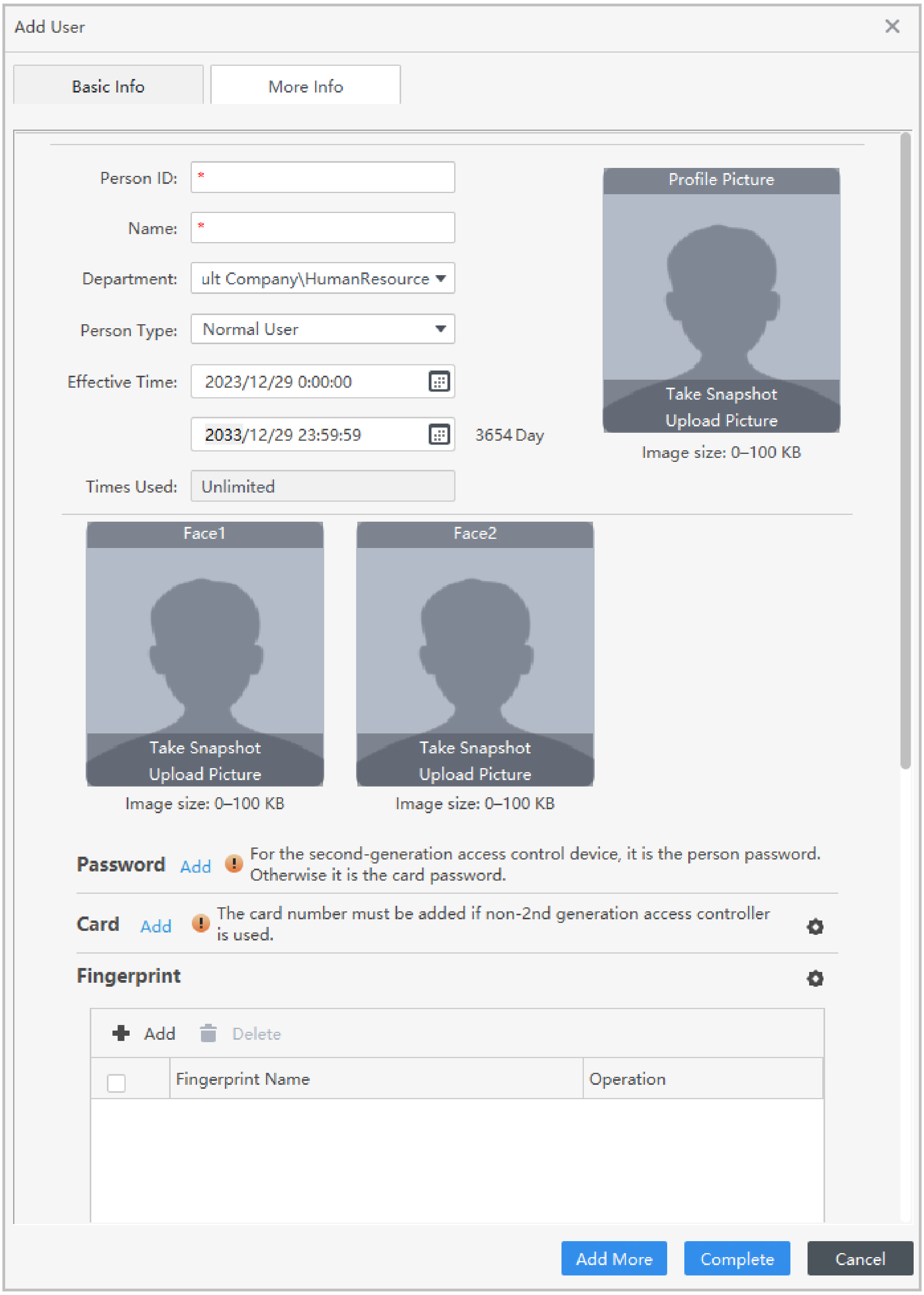
- Configure fingerprint

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

- Configure feature codes

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

Figure 5-11 Add basic information



Add User ✕

Basic Info | More Info

Person ID: *

Name: *

Department: ult Company\HumanResource ▾

Person Type: Normal User ▾

Effective Time: 2023/12/29 0:00:00

2033/12/29 23:59:59 3654 Day

Times Used: Unlimited

Image size: 0–100 KB

Image size: 0–100 KB

Image size: 0–100 KB

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

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

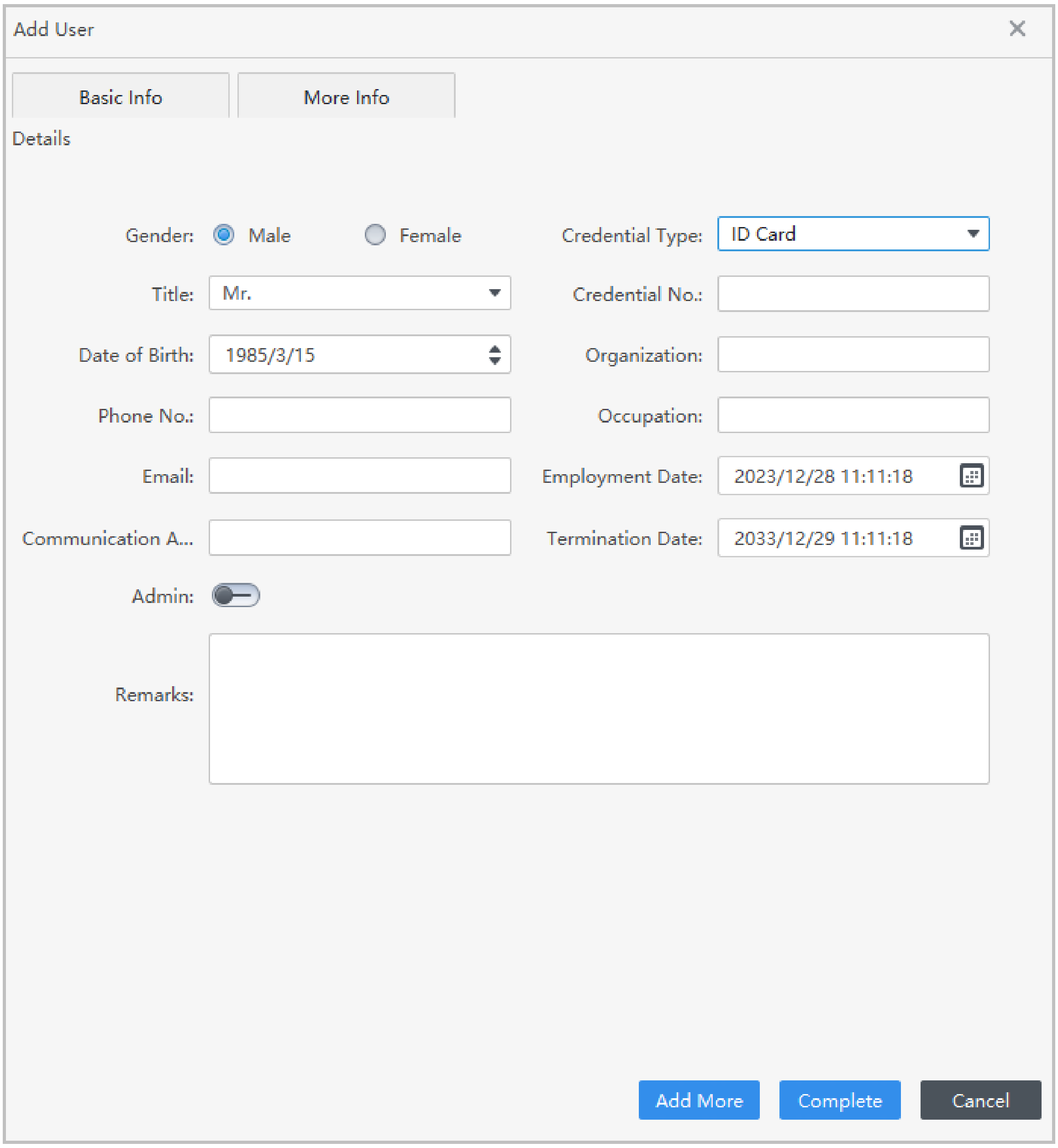
Fingerprint

➕ Add 🗑 Delete

□	Fingerprint Name	Operation

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

Figure 5-12 Add more information



Add User

Basic Info | More Info

Details

Gender:	● Male ○ Female	Credential Type:	ID Card
Title:	Mr.	Credential No.:	
Date of Birth:	1985/3/15	Organization:	
Phone No.:		Occupation:	
Email:		Employment Date:	2023/12/28 11:11:18
Communication A...		Termination Date:	2033/12/29 11:11:18
Admin:			
Remarks:			

Step 4 Click **Complete**.

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

Related Operations

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

5.4.3.2 Adding Personnel in Batches

Procedure

Step 1 Select **Person** > **Person Management**, and then click **Batch Add**.

Step 2 Select the device type, set the start number, number of card.

Step 3 Set the department, and the effective time and expiration time of card.

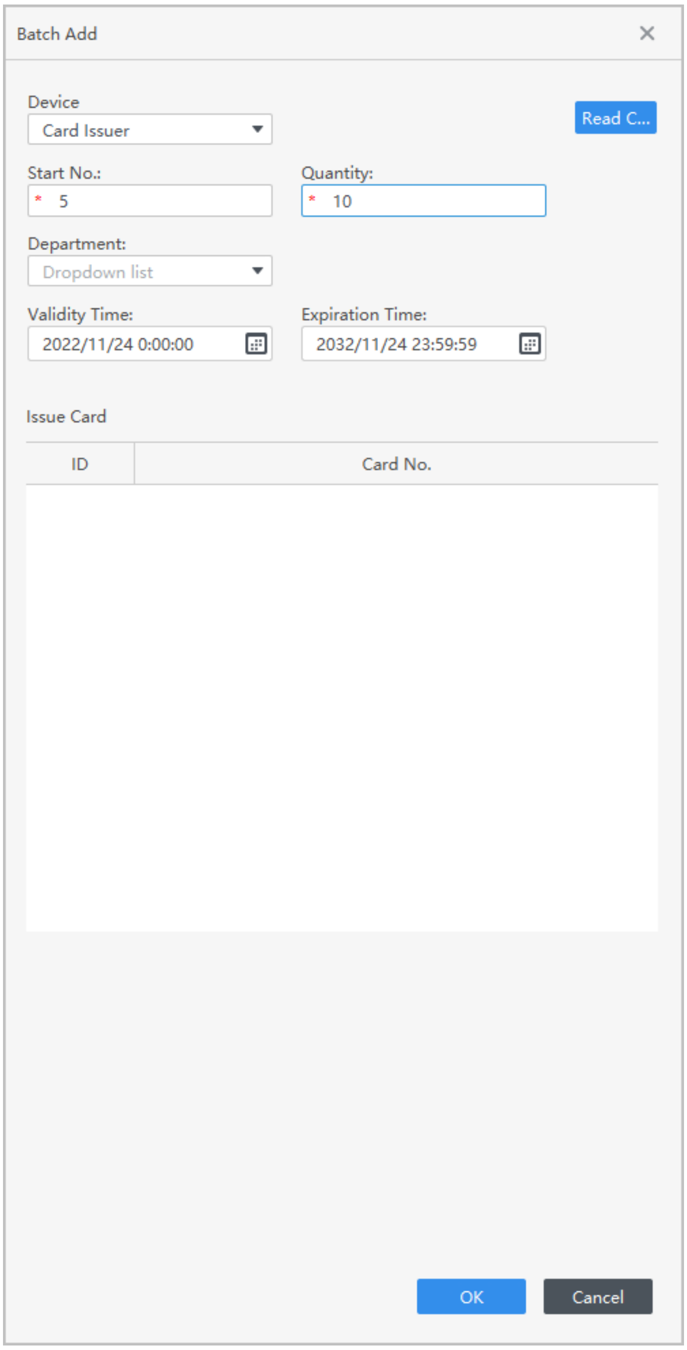
Step 4 Click **Read Card No.**.

Step 5 Place cards on the card issuer or the card reader.

The card number will be read automatically or filled in automatically.

Step 6 Click **OK**.

Figure 5-13 Add personnel in batches



Device: Card Issuer

Start No.: * 5

Quantity: * 10

Department: Dropdown list

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

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

5.4.4 Assigning Access Permissions

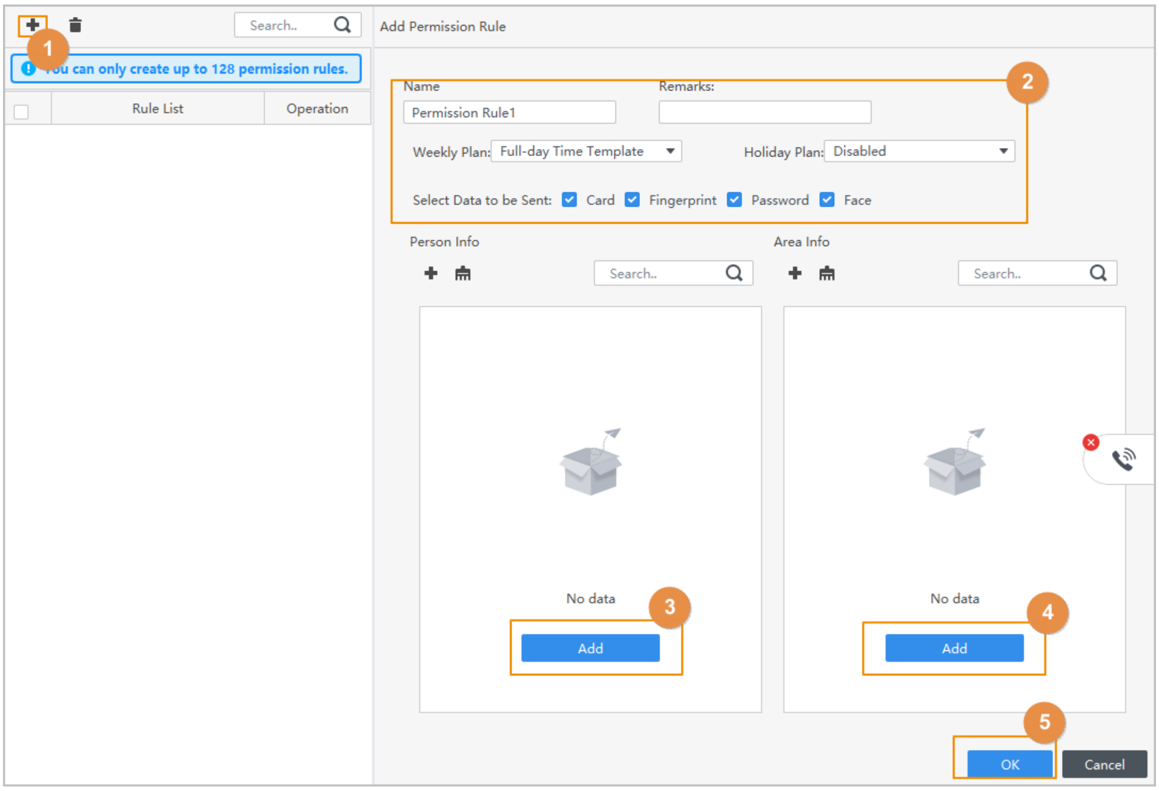
The method to configure permission for department and for personnel is similar, and here uses department as an example.

Procedure

Step 1 Select **Access Control Config** > **Permission Settings**.

Step 2 Click ✚ to add a permission rule.

Figure 5-14 Assign permissions rules



You can only create up to 128 permission rules.

Name: Permission Rule1

Remarks:

Weekly Plan: Full-day Time Template

Holiday Plan: Disabled

Select Data to be Sent: ☑ Card ☑ Fingerprint ☑ Password ☑ Face

Step 3 Enter the name of the permission rule, select the time plan and unlock methods.

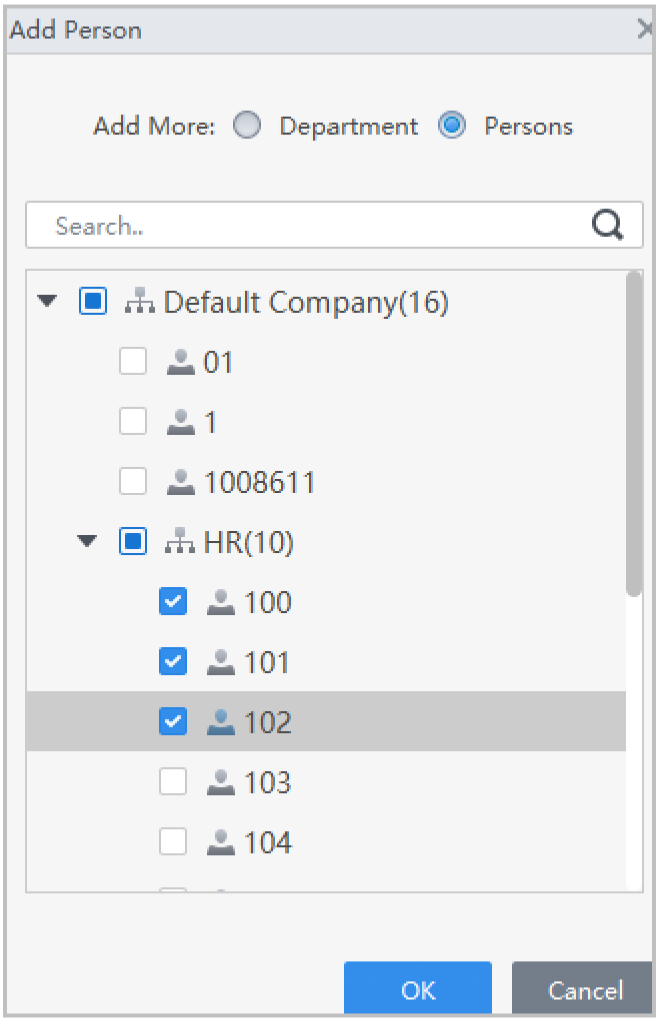
Step 4 In the **Person Info** area, click **Add** to select personnel, and then click **OK**.

You can select personnel on the department or individual users.

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

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

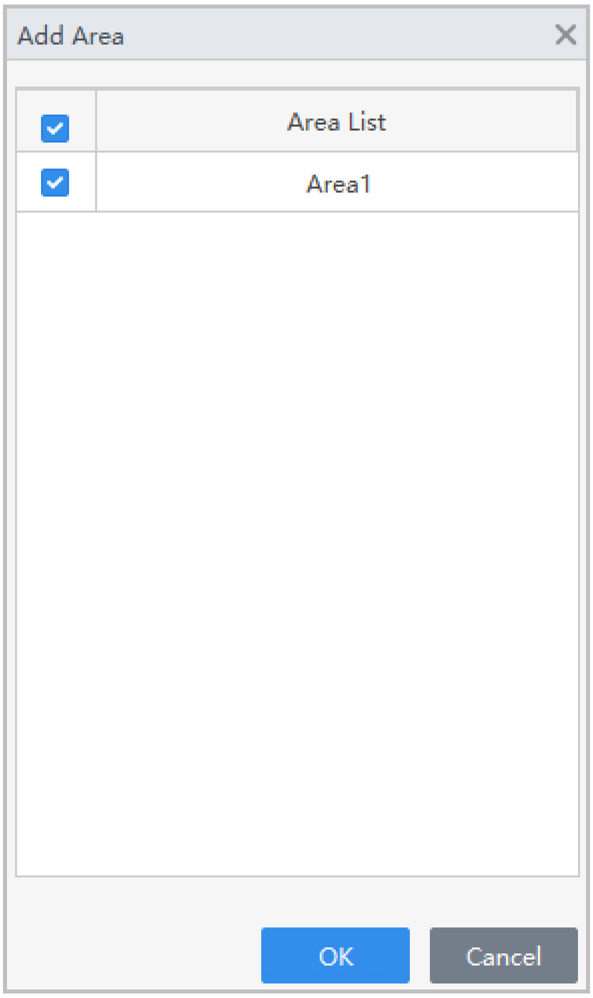
Figure 5-15 Add users



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

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

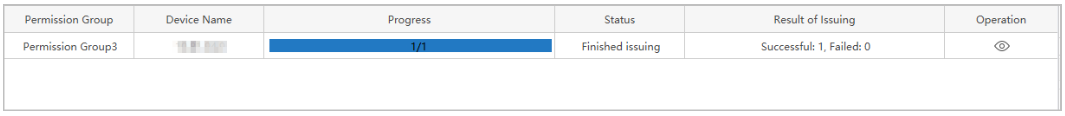
Figure 5-16 Add area



Step 6 Click **OK**.

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

Figure 5-17 Authorization progress



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

5.4.5 Assigning Attendance Permissions

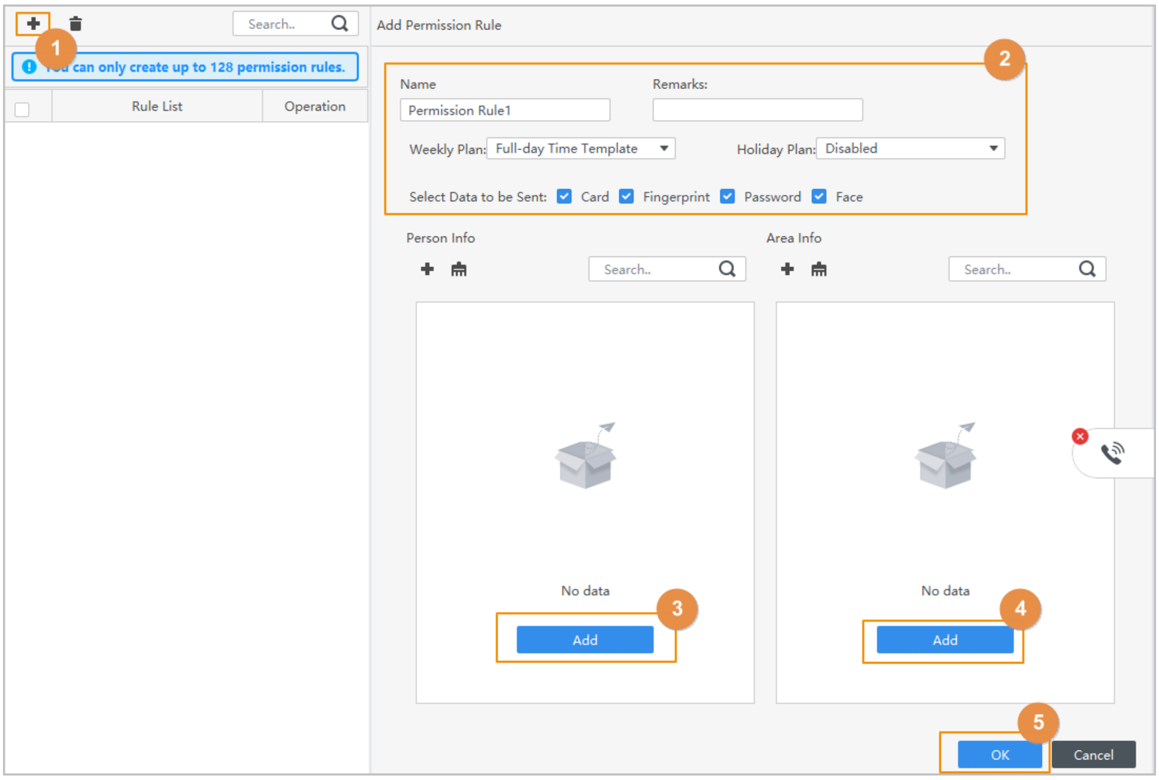
The method to configure permission for department and for personnel is similar, and here uses department as an example.

Procedure

Step 1 Select **Access Control Config** > **Permission Settings**.

Step 2 Click + to add a permission rule.

Figure 5-18 Assign permissions rules



You can only create up to 128 permission rules.

Name: Permission Rule1

Remarks:

Weekly Plan: Full-day Time Template

Holiday Plan: Disabled

Select Data to be Sent: ☑ Card ☑ Fingerprint ☑ Password ☑ Face

Step 3 Enter the name of the permission rule, select the time plan and unlock methods.

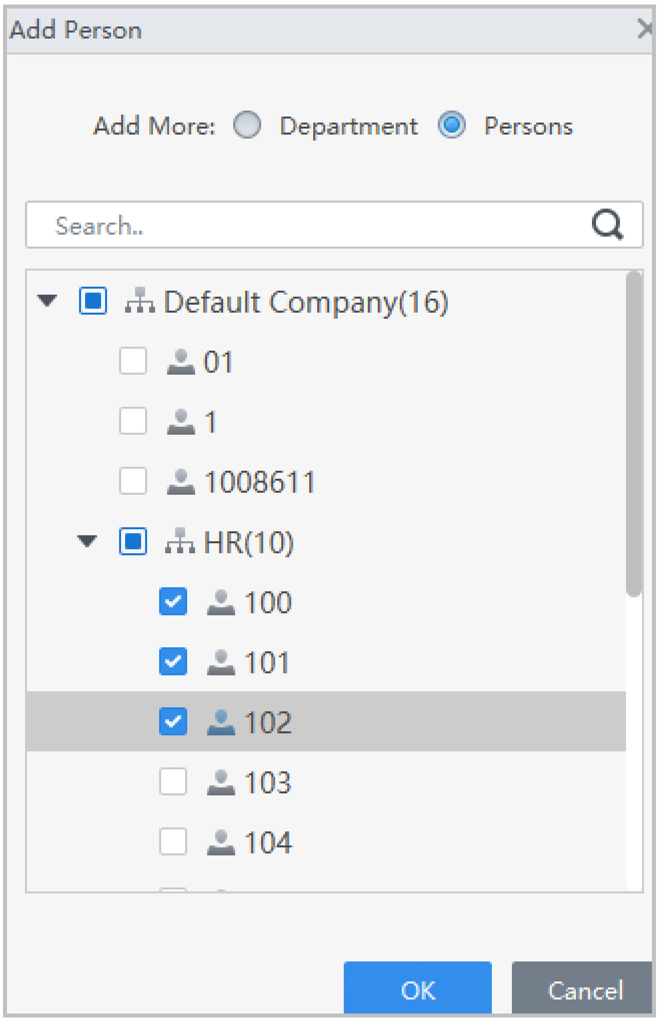
Step 4 In the **Person Info** area, click **Add** to select personnel, and then click **OK**.

You can select personnel on the department or individual users.

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

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

Figure 5-19 Add users



Add Person

Add More: ○ Department ● Persons

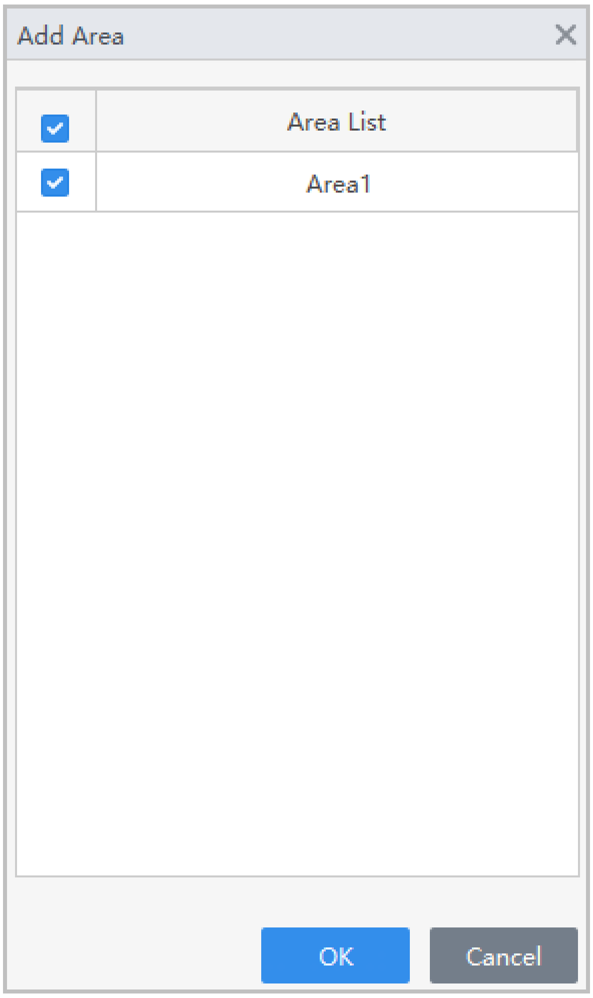
Search..

- □ Default Company(16)
  - □ 01
  - □ 1
  - □ 1008611
  - □ HR(10)
    - ☑ 100
    - ☑ 101
    - ☑ 102
    - □ 103
    - □ 104

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

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

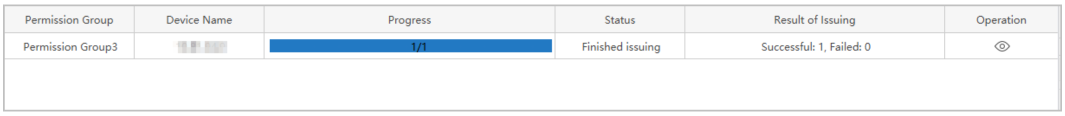
Figure 5-20 Add area



Step 6 Click **OK**.

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

Figure 5-21 Authorization progress



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

5.5 Access Control Monitoring

Procedure

Step 1 Click **Access Control Monitoring** on the home page.

Step 2 Manage the door.

Figure 5-22 Monitor the door

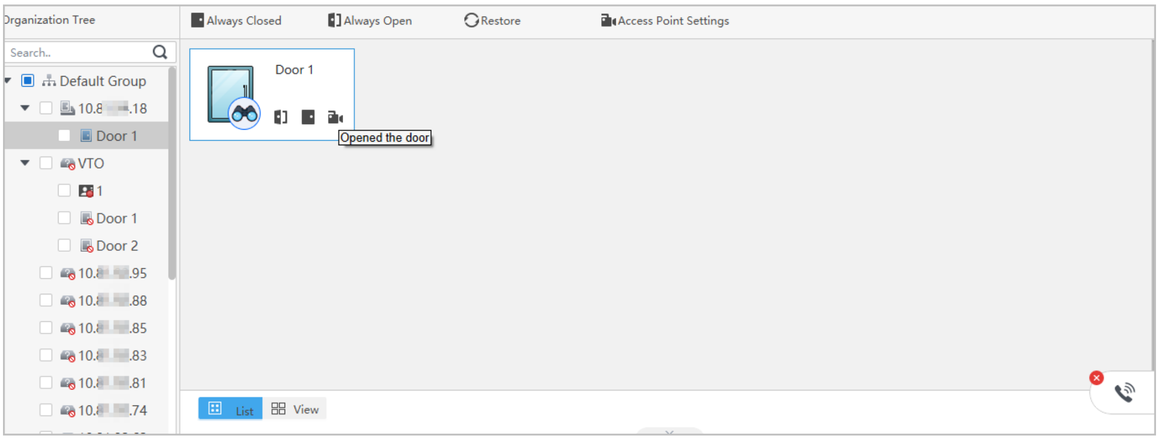


Table 5-3 Parameters description

Function	Description
Remotely control the door	Remotely control the door. ● Method 1: Right-click a door, and then select **Open** or **Close**. ● Method 2: Click ◧ or ■ to open or close the door.
📹	View the video captured by the camera of the access controller or the linked external camera. 📖 If you cannot view real-time video, it means that the access control device has no camera and is not connected to an external camera. Please configure an external camera for access controller. For details, see the corresponding user's manual.. If you want to view multiple live videos at the same time, click ⊞ View, and then drag the access control device in the organization tree to windows, or double-click the access control device in the organization tree.
Always Open	After setting always open or always closed, the door is open or closed all the time and cannot be controlled manually. If you want to manually control the door again, click **Normal** to reset the door status.
Always Closed	
Restore	
Access Point Settings	Set devices (NVR, IPC, IVSS and more) that support target recognition as the access control point. After setting, the door unlock records will be uploaded to the platform.

Step 3 Right-click a access control device to manage the device.

Figure 5-23 Manage the device

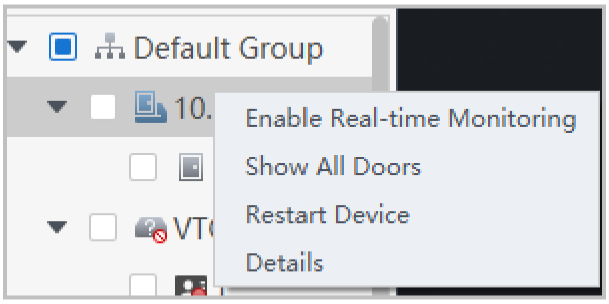


Table 5-4 Parameters description

Parameter	Description
Enable Real-time Monitoring	Start real-time event monitoring.
Show all Doors	Show all doors connected to the access control device.
Restart Device	Restart the access control device.
Details	View the device information, such as version, and more.

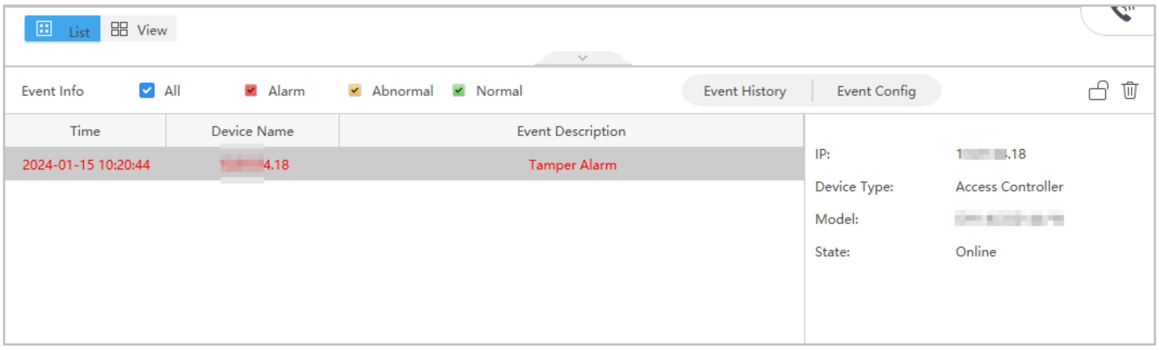
Step 4 View door status on **Event Info** list. For details, see the corresponding user's manual.

Related Operations

Click ^ to open the **Event Info** list.

- View access control information: You can view real-time access information in the **Event Info** list. The information will be cleared after the platform restarts.
- Filter events: Select the event type in the **Event Info** , and the event list displays events of the selected types. For example, select **Alarm**, and the event list only displays alarm events.
- Lock or unlock the event list: Click 🔓 on the right side of **Event Info** to lock or unlock the event list, and then the real-time events cannot be viewed.
- Delete events: Click 🗑 on the right side of **Event Info** to clear all events in the event list.
- Click **Event History** to jump to the **Access Control Record** page, and click **Event Config** to jump to the **Event Config** page.

Figure 5-24 Event information



Time	Device Name	Event Description
2024-01-15 10:20:44	[redacted]4.18	Tamper Alarm

IP: 1[redacted].18

Device Type: Access Controller

Model: [redacted]

State: Online

Appendix 1 Important Points of Fingerprint Registration Instructions

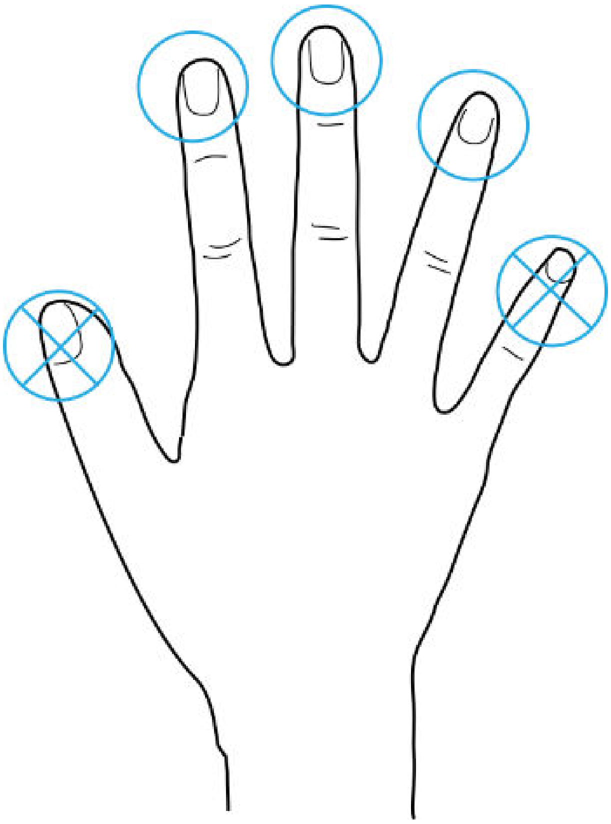
When you register the fingerprint, pay attention to the following points:

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

Fingers Recommended

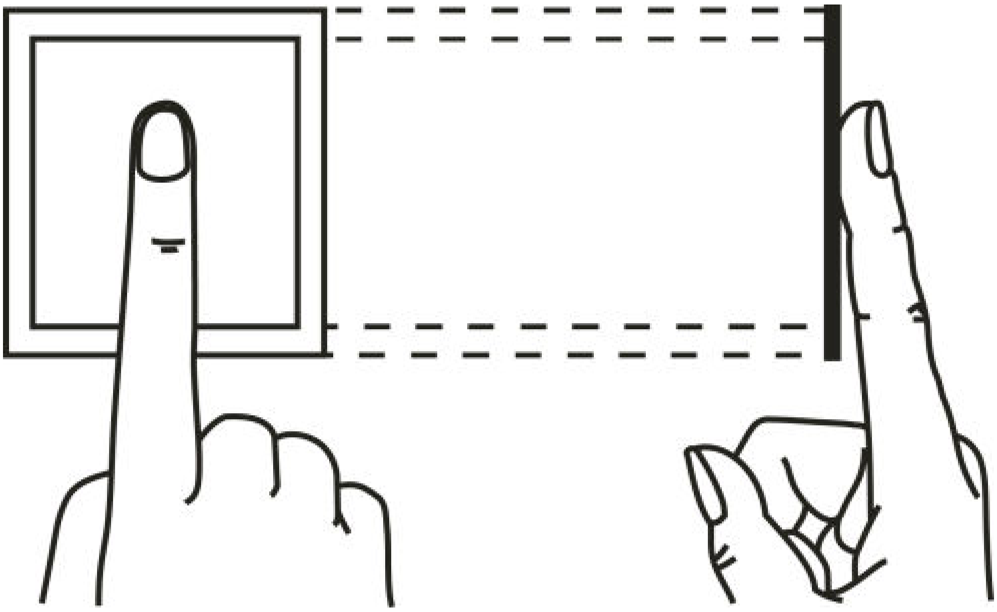
Forefingers, middle fingers, and ring fingers are recommended. Thumbs and little fingers cannot be put at the recording center easily.

Appendix Figure 1-1 Recommended fingers

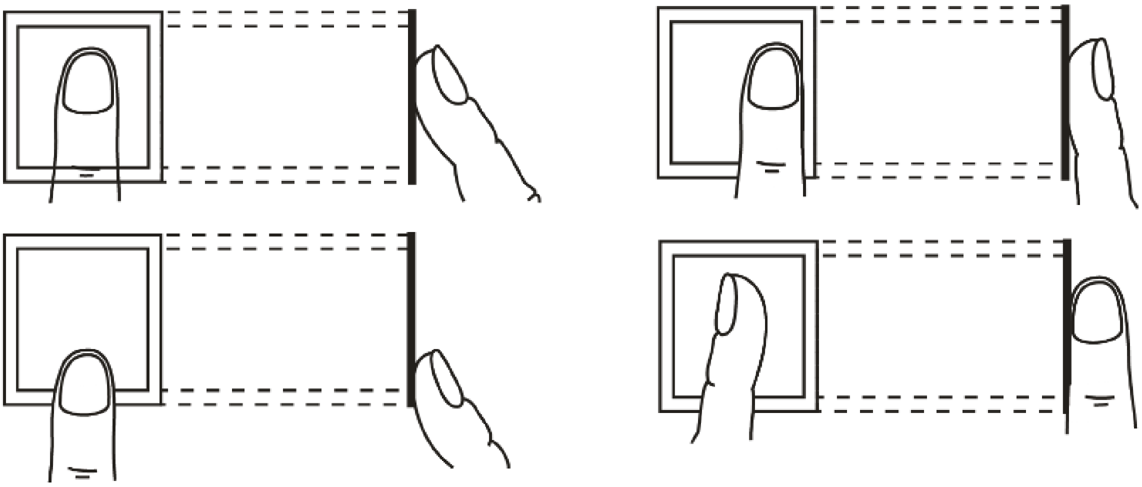


How to Press Your Fingerprint on the Scanner

Appendix Figure 1-2 Correct placement



Appendix Figure 1-3 Wrong placement



Appendix 2 Security Recommendation

Account Management

1. **Use complex passwords**

   Please refer to the following suggestions to set passwords:

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

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

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

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

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

Service Configuration

1. **Enable HTTPS**

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

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

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

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

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

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

Network Configuration

1. **Enable 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).