Access Controller

User Manual



V1.0.0

Foreword

General

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

Symbols

The following symbols might appear in the manual.

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

Revision History

Version	Revision Content	Release Time
V1.0.0	First Release.	July 2026

Privacy Protection Notice

As the device user, you might collect the personal data of individuals such as their names, email addresses, face images, audio and fingerprints. You shall be fully responsible for any activities associated with processing personal data. You commit to comply with your local privacy protection laws and regulations to protect the legitimate rights and interests of individuals, and shall implement measures which are required by applicable law, including but not limited to, providing clear and comprehensive information to individuals before processing their personal data, obtaining consent from individuals when necessary, informing individuals of the existence of the surveillance area, and providing required contact information.

Intelligent Product Usage Statement

Intelligent products utilize AI technology to effectively enhance security. The intelligent recognition and alarm functions of the product might be affected by factors such as environmental lighting, camera angles, object obstructions, and network delays, potentially leading to false alarms, missed alerts, or response delays. This intelligent product is solely intended to be used as a security assistance tool. The results from performing identification are for reference only and do not

constitute absolute guarantee of personal or property safety. Users need to combine these products with necessary physical security measures to enhance overall protection. Except as otherwise provided by laws or in the event of intentional or gross negligence on the part of the company, the company shall not be liable for any losses caused by the aforementioned factors not attributable to the company.

Interface Declaration

This manual mainly introduces the relevant functions of the device. The interfaces used in its manufacture, the procedures for returning the device to the factory for inspection and for locating its faults are not described in this manual. Please contact technical support if you need information on these interfaces.

About the Manual

- This manual is provided for general reference only. Discrepancies might exist between the product and this manual, including but not limited to printed, electronic, or any other editions.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. Specifications and documentation are subject to change without prior notice. For the latest versions, as well as legal notices, consult the printed manual, the product webpage, our official website, or scan the QR code to access the electronic edition.
- The manual will be updated as necessary to reflect product changes and applicable legal requirements. These updates will not diminish your statutory rights, nor will they remove or weaken the safety information or essential instructions provided at the time of purchase.
- Although we make every effort to ensure accuracy, errors or deviations in descriptions of functions, operations, or technical data might occur. If there is any uncertainty or controversy, we reserve the right of final explanation.
- All trademarks, registered trademarks and company names referenced in this manual are the property of their respective owners.

Table of Contents

Foreword I
1 Overview 1
2 Web Operations 2
2.1 Initialization 2
2.2 Logging In 2
2.3 Resetting the Password 3
2.4 Home Page 4
2.5 Person Management 4
2.5.1 Adding Person 4
2.5.2 Verification Mode 7
2.6 Configuring Access Control 9
2.6.1 Configuring General Plans 9
2.6.2 Configuring Holiday Plans 10
2.6.3 Configuring Door Parameters 12
2.6.4 Configuring Alarm 17
2.6.5 Configuring Advanced Parameters 22
2.6.6 Configuring Unlock Methods 28
2.6.7 Card Settings 29
2.6.8 Configuring QR Code 32
2.6.9 Configuring Back-end Comparison 33
2.7 Access Monitoring 33
2.8 Network Settings 34
2.8.1 Configuring TCP/IP 35
2.8.2 Configuring Port 36
2.8.3 Configuring Basic Services 37
2.8.4 Configuring Cloud Service 39
2.8.5 Configuring Auto Registration 40
2.8.6 Configuring CGI Auto Registration 41
2.8.7 Configuring Auto Upload 43
2.9 Configuring the System 43
2.9.1 User Management 44
2.9.2 Viewing Online Users 47
2.9.3 Configuring Time 47
2.10 Security Settings(Optional) 48
2.10.1 Security Status 48
2.10.2 Configuring HTTPS 49
2.10.3 Attack Defense 50

2.10.4 Installing Device Certificate..... 53
2.10.5 Installing the Trusted CA Certificate.....56
2.10.6 Security Warning.....57
2.10.7 Security Authentication.....58
2.11 Maintenance Center..... 58
2.11.1 One-click Diagnosis.....58
2.11.2 System Information..... 59
2.11.3 Data Capacity.....59
2.11.4 Viewing Logs..... 59
2.11.5 Maintenance Management..... 60
2.11.6 Updating the System..... 63
2.11.7 Advanced Maintenance.....64
Appendix 1 Important Points of Fingerprint Registration Instructions.....66
Appendix 2 Security Recommendation..... 68

1 Overview

Flexible and convenient, the Access Controller has a user friendly system that allows you to manage access permissions on the webpage through IP address of the Device when used with card reader. It supports functions of multi-person unlock, anti-passback and first-card unlock.

It is widely used in communities, business centers, properties of the group and commercial buildings.

2 Web Operations

On the webpage, you can configure and operate the Device, including configuring network parameters, access parameters and other operations. You can also maintain and update the Device.

This chapter uses access controller (four doors) as the example.

Web configurations differ depending on models of the Device.

2.1 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.

Step 3 (Optional) Read and accept the agreement and statement.

Step 4 Configure the time zone.

Step 5 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.
- If you need to reset the password, the email address is required. You can receive the security code through the email address.

Step 6 (Optional) Select **Auto Check for Updates**.

After you select the function, there will be notification when a version update is detected.

Step 7 Click **Completed** to finish the initialization.

2.2 Logging In

Procedure

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

Step 2 Enter the user name and password.

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

Step 3 Click **Login**.

2.3 Resetting the Password

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

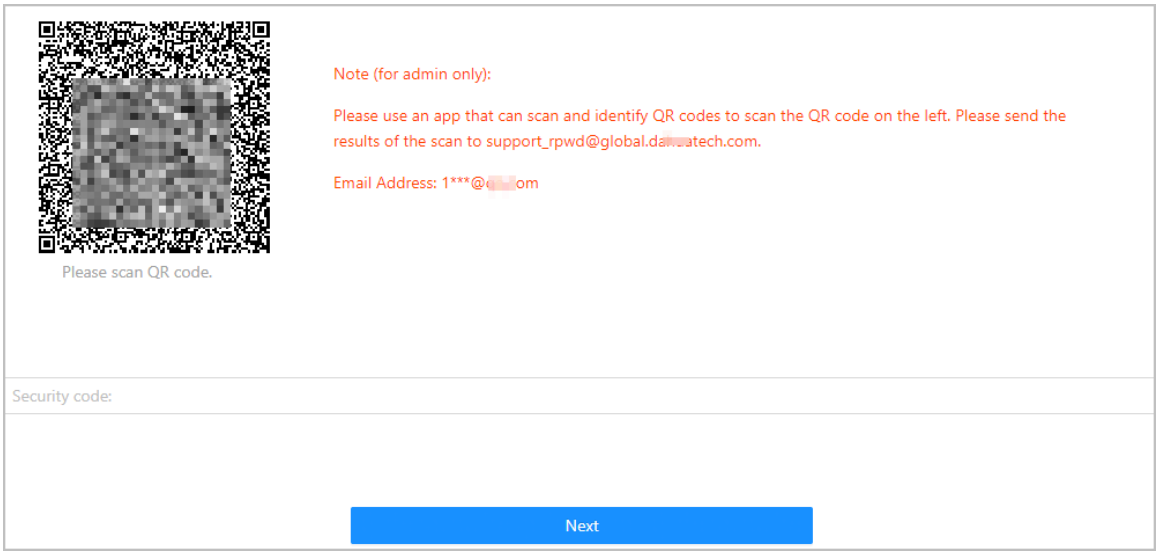
Procedure

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 2-1 Reset password



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

Step 4 Enter the security code.

Step 5 Click **Next**.

Step 6 Reset and confirm the password.

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

Step 7 Click **OK**.

2.4 Home Page

The home page is displayed after you successfully log in.

Figure 2-2 Home page

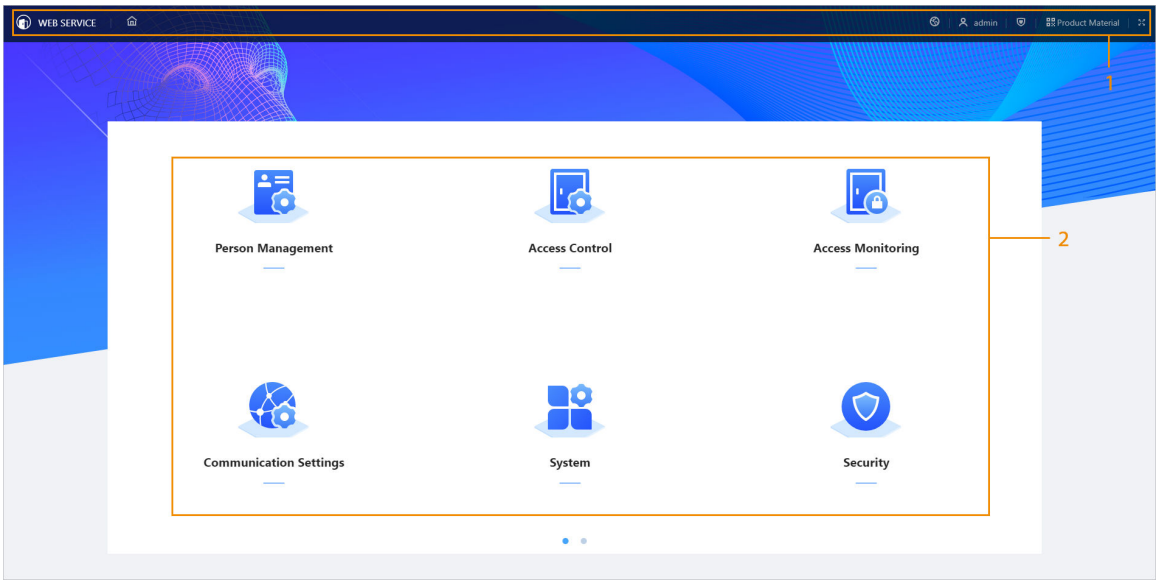


Table 2-1 Home page description

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 with your phone to view the product documents. This function is only available on select models. • : Display in full screen.
2	Main menu.

2.5 Person Management

2.5.1 Adding Person

Procedure

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

Step 2 Configure user information.

Figure 2-3 Add users

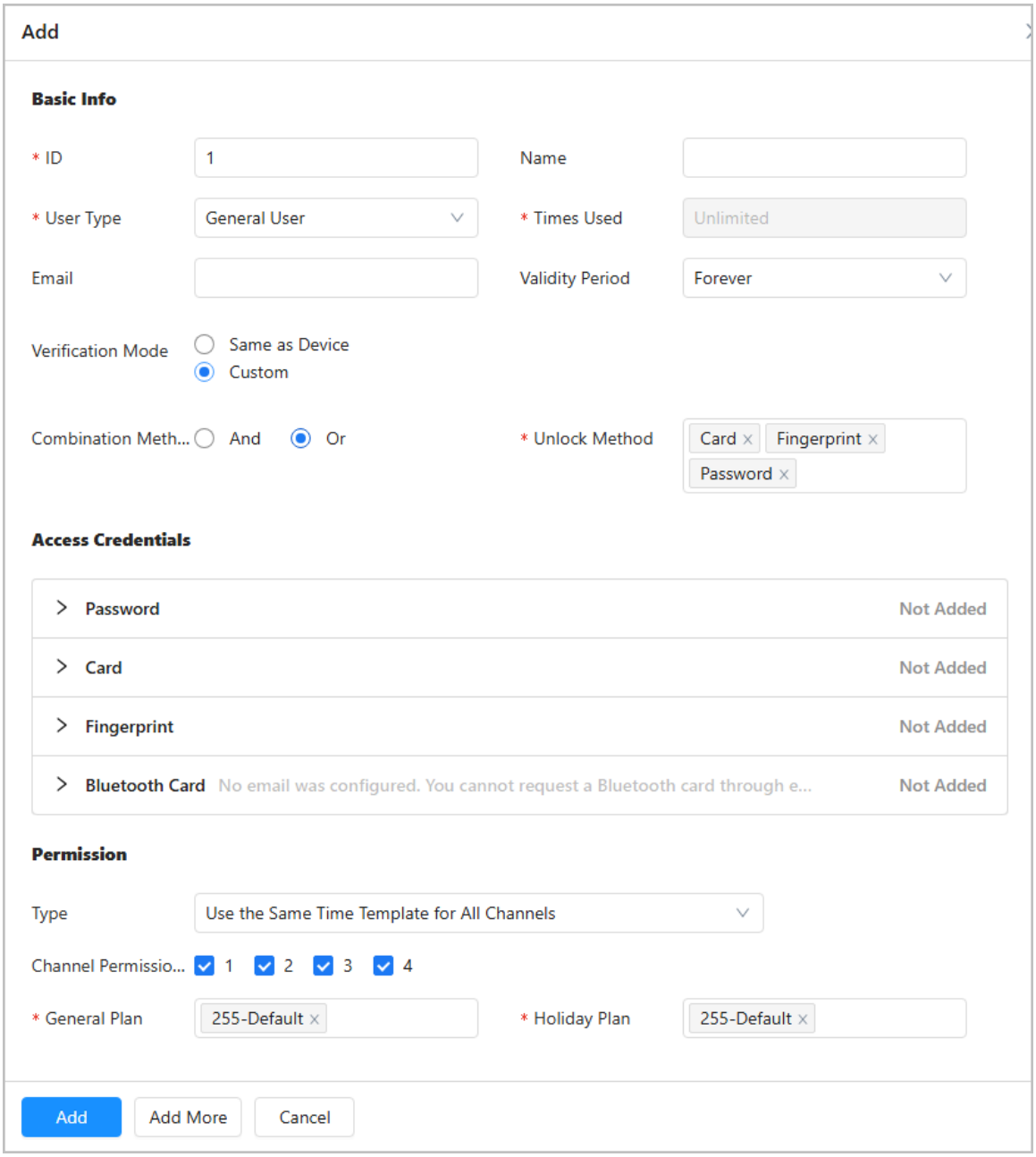


Table 2-2 Parameters description

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

Parameter		Description
	User Type	• **General User** : General users can verify the identifications according to the configured unlock methods. • **VIP User** : VIP users can unlock the door regardless of the configurations of unlock methods, unlock periods and multi-user unlock. • **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. • **Blocklist User** : When users in the blocklist attempt to unlock the door, they cannot open the door, and the alarm will be reported. • **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.
	Times Used	Set an unlock limit for guest users. After the unlock times run out, they cannot unlock the door.
	Email	Set the email address of the user.
	Validity Period	Set a date on which the door access permissions of the person will be expired. • **Custom** : The person has the corresponding access control permissions until the set custom time. • **Forever** : The person permanently has the corresponding access control permissions.
	Verification Mode	Configure the verification mode for the person. You can use the mode that is the same as the device or customize the mode. • **Same as Device** : The mode is the same as the device. • **Custom** : After you select **Custom**, **Combination Method** and **Unlock Method** are displayed. Select the combination method and unlock methods as needed. ◇ Or: Use one of the selected unlock methods to open the door. ◇ And: Use all the selected unlock methods to open the door.
Access Credentials	Password	For details, see "2.5.2 Verification Mode".
	Card	
	Fingerprint	
	Bluetooth Card	
Permission	Type	• Use the same time template for all channels: Configure the same general plan and holiday plan for all the channels. • Use different time templates for different channels: Configure different general plan and holiday for different channels. The parameter is not displayed for the access controller (single door).

Parameter		Description
	Channel Permissions	The number refer to the corresponding door. For example, 1 refers to door1. Select the channel to have the access permissions of the channel. • The parameter is not displayed for the access controller (single door). • The number might differ according to the actual device model.
	General Plan	People can unlock the door during the defined time period.
	Holiday Plan	People can unlock the door during the defined holiday. There is no holiday by default.

Step 3 Click **Add**.

Related Operations

- Import user information: Click **Export Template**, and download the template and enter user information in it.

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

2.5.2 Verification Mode

Password

Configure the user password. The maximum length of the password is 8 digits.

Enter **user No. + password** to unlock the door.

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.

1. Click **Add**.
2. Enter the password and confirm the password.
3. Click **OK**.

Card

Collect the card information through the external devices or enter the card number manually.

- Enter the card number manually.
  1. Click **Add**.
  2. Enter the card number, and then click **Add**.
- Read the number automatically through the enrollment readers (IC card or ID card).

1. Click **Add** , and then click **Modify** to select an enrollment reader that is connected to the access controller. Select from **IC Card** and **ID Card**.
2. Click **Read Card**, and then swipe cards on the enrollment 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**.

- Read the number automatically through the enrollment readers (Desfire card).

1. Click **Add** , and then click **Modify** to select **Desfire Card** that is connected to the access controller.
2. Place the card on the enrollment reader, and then click **Read Card**.

   If the Desfire card has been written with the card number, it will be read and displayed here. If the card is empty, then the card number needs to be written first. The card number will be automatically generated on the computer, and be written to the card.
3. Click **Add**.

- Read the number automatically through the card reader that is connected to the Device.

1. Click **Add** , and then click **Modify** to select the card reader. Select **Device**, and then select the specific reader.
2. Click **Read Card**, and then swipe cards on the external device.

   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.

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 the enrollment reader that is connected to the computer or the external card reader that is connected to the access controller.

1. Click **Add** , and then click **Modify** to select an enrollment reader or the card reader that is connected to the access controller.
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.

Bluetooth Card

- Bluetooth is only available on select models.
- Bluetooth must be used with card readers supporting Bluetooth.

You can select **Request through Email** or **Request through Registration Code**.

- **Request through Email** : Suitable for the first time a Bluetooth card is requested. You can request up to 5 Bluetooth cards, and have to use the email that is registered to DMSS.

  You must have entered your reserved Email before you use the function.

  1. Configure the Email that is registered to DMSS.
  2. Click **Request through Email**, and then the Bluetooth cards can be requested.
- **Request through Registration Code** : Suitable when you already have a Bluetooth card and want to reuse it on another access controller supporting Bluetooth function.

  1. Copy the Bluetooth registration code from the DMSS.
  2. Click **Request through Registration Code**, and then enter the code.
  3. Click **OK**.

2.6 Configuring Access Control

2.6.1 Configuring General Plans

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

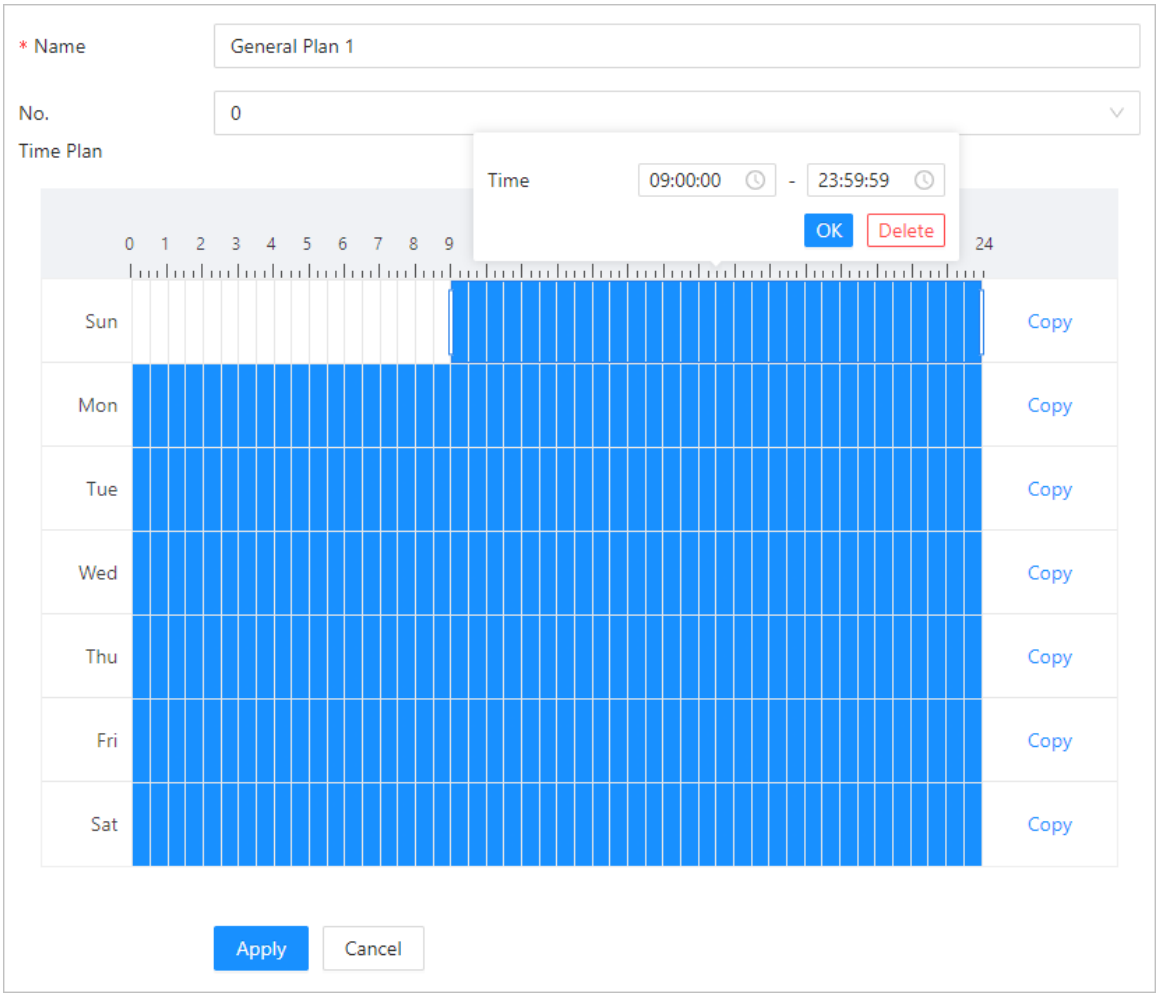
Step 1 Log in to the webpage.

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

Step 3 Click **+**.

1. Configure the plan name and the plan number.
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 2-4 Configure general plan



Step 4 Click **Apply**.

2.6.2 Configuring Holiday Plans

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

Procedure

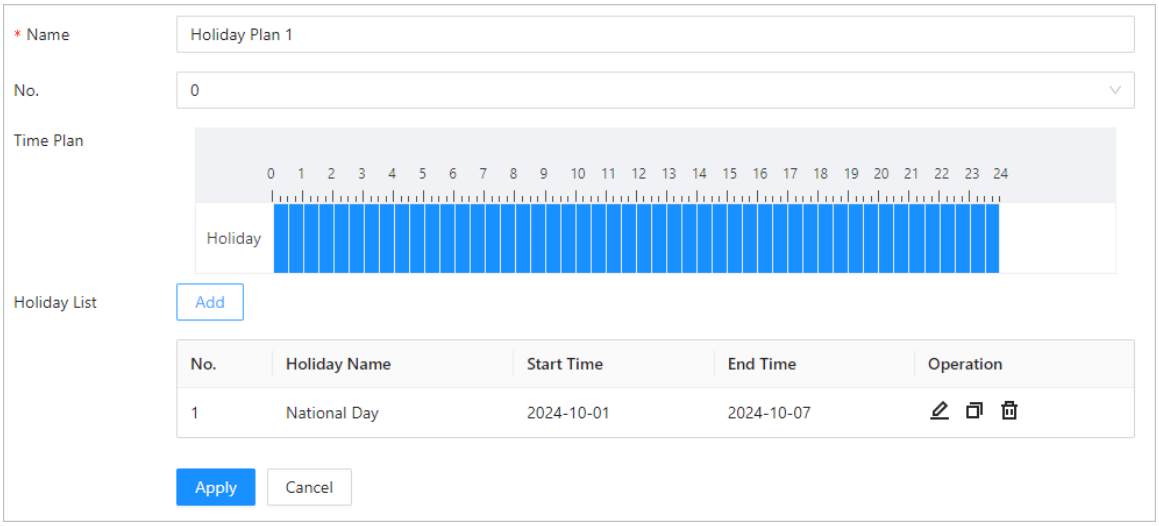
Step 1 Log in to the webpage.

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

Step 3 Click **+**.

1. Configure the plan name and the plan number.

Figure 2-5 Add a holiday plan

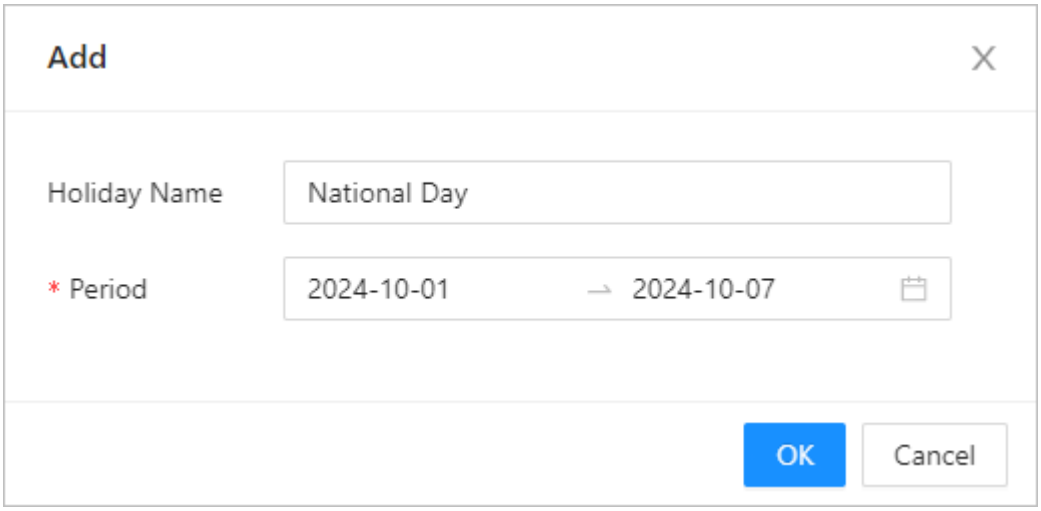


2. Drag the time slider to configure time for the holiday.

   You can configure up to 4 periods.

3. Click **Add** , configure the name and the period, and then click **OK** to add a holiday to the holiday list.

Figure 2-6 Add a holiday



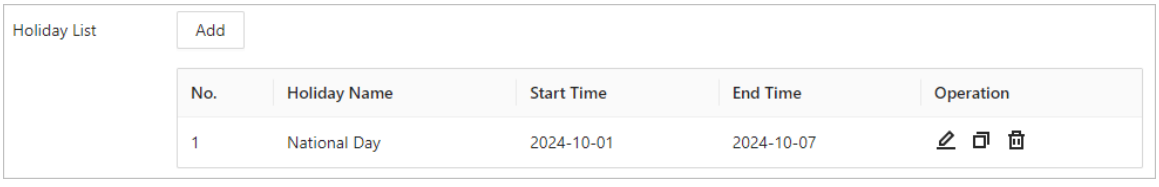
4. Click **OK**.

Step 4 Click **Apply**.

Related Operations

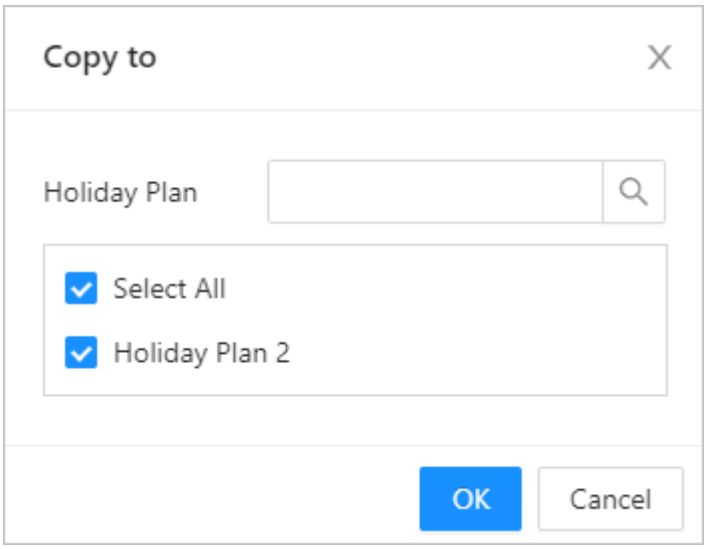
Copy the configured holiday to other holiday plans.

Figure 2-7 Holiday list



1. Click , select the added holiday plan, and then click **OK**.

Figure 2-8 Copy the holiday



2. Click **Apply**.

2.6.3 Configuring Door Parameters

Configure door status, unlock methods and other door parameters.

Procedure

Step 1 Log in to the webpage.

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

Step 3 In **Basic Settings**, configure basic parameters for the access control.

Figure 2-9 Basic parameters

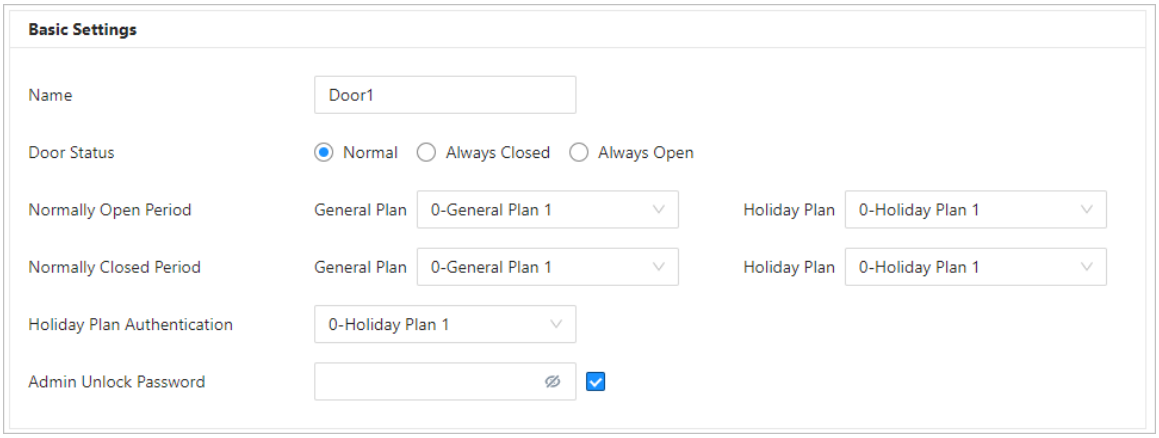


Table 2-3 Basic parameters description

Parameter	Description
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 Closed: The door remains locked all the time. ● Always Open: The door remains unlocked all the time.
Normally Open Period	When you select **Normal**, you can select a time template from the drop-down list. The door remains open or closed during the defined time. You need to configure the general plan and holiday plan first. ● 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	
Holiday Plan Authentication	Authorized access is allowed for always closed door in the defined holiday plan.
Admin Unlock Password	After the function is enabled, you can unlock the door through admin password. Enter **admin password** directly without entering user ID to unlock the door regardless of the user type, unlock method, general plan, holiday plan and anti-passback permissions. Only when the door is in the normally closed status, the admin password cannot be used to unlock the door.

Step 4 In **Unlock Settings**, configure unlock method and corresponding parameters.

- 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 2-10 Unlock settings

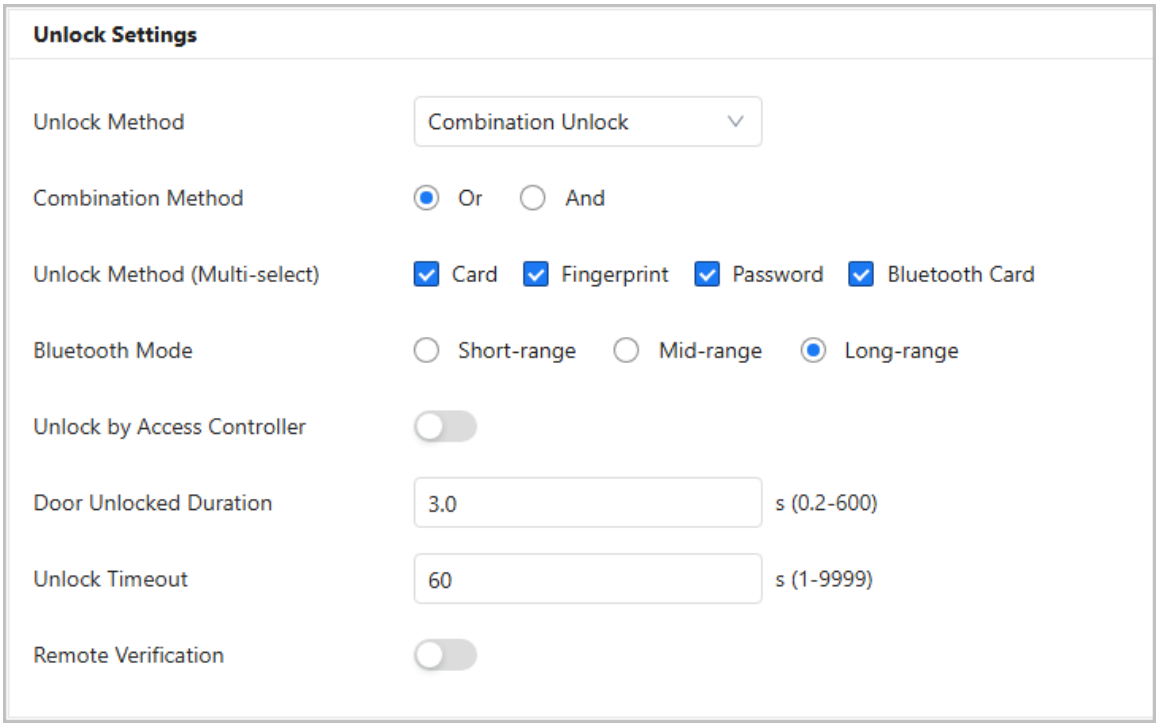


Table 2-4 Unlock settings description

Parameter	Description
Unlock Method (Multi-select)	Unlock methods might differ depending on the models of product.
Door Unlocked Duration	After a person is granted access, the door will remain unlocked for a defined time for them to pass through. It ranges from 0.2 to 600 seconds.
Bluetooth Mode	Select the range for Bluetooth. You can select from **Long-range** , **Mid-range** and **Short-range**. It is only available for devices with Bluetooth function.
Unlock by Access Controller	When the device is connected to an access controller via RS-485, and the external device in the RS-485 settings of the access controller is set to **Access Controller**, this parameter must be configured based on the output data type set on the access controller. • If the output data type is **Card Number**, no need to enable this function. • If the output data type is **ID**, this function must be enabled.
Door Unlock Duration	After a person is granted access, the door will remain unlocked for a defined time for the person to pass through. It ranges from 0.2 to 600 seconds.
Unlock Timeout	When the door detector and the unlock timeout alarm are enabled, a timeout alarm will be triggered if the door remains unlocked longer than the defined unlock time.

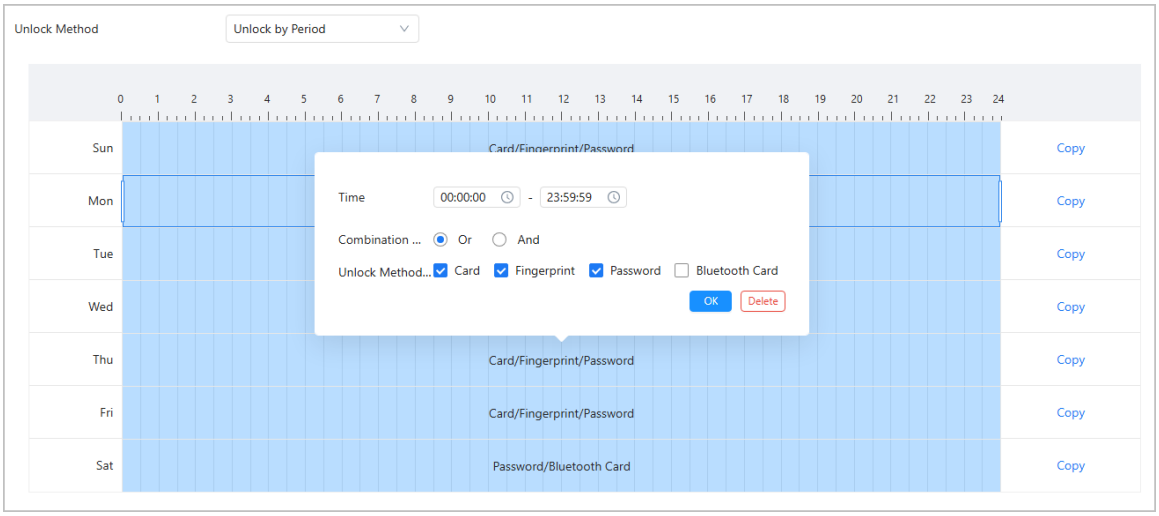
Parameter	Description
Remote Verification	If this function is enabled, you can control the door on the corresponding platform.

- 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 the combination method and the unlock method for the time period, and then configure other parameters.

Figure 2-11 Unlock by period



- Unlock by multiple users.

1. In the **Unlock Method** list, select **Unlocked by multiple users**.
2. Click **Add** to add groups.
3. Select unlock method, valid number and users.
   - If only one group is added, the door unlocks only after the number of people in the group who grant access equals the defined valid number.
   - If more than one groups are added, the door unlocks only after the number of people in each group who grant access equals the defined valid number.
4. Configure the verification of multi-person unlock timeout duration.

- You can add up to 4 groups.
- The valid number indicates the number of people in each group who need to verify their identities on the Device before the door unlocks. For example, if the valid number is set to 3 for a group, any 3 people in the group need to verify their identities to unlock the door.
- If you configure the first-card unlock, and the first-card user is in the user group, the first-card user need to verify the identification first.

Step 5 In the **Alarm**, configure alarm parameters.

Figure 2-12 Alarm settings

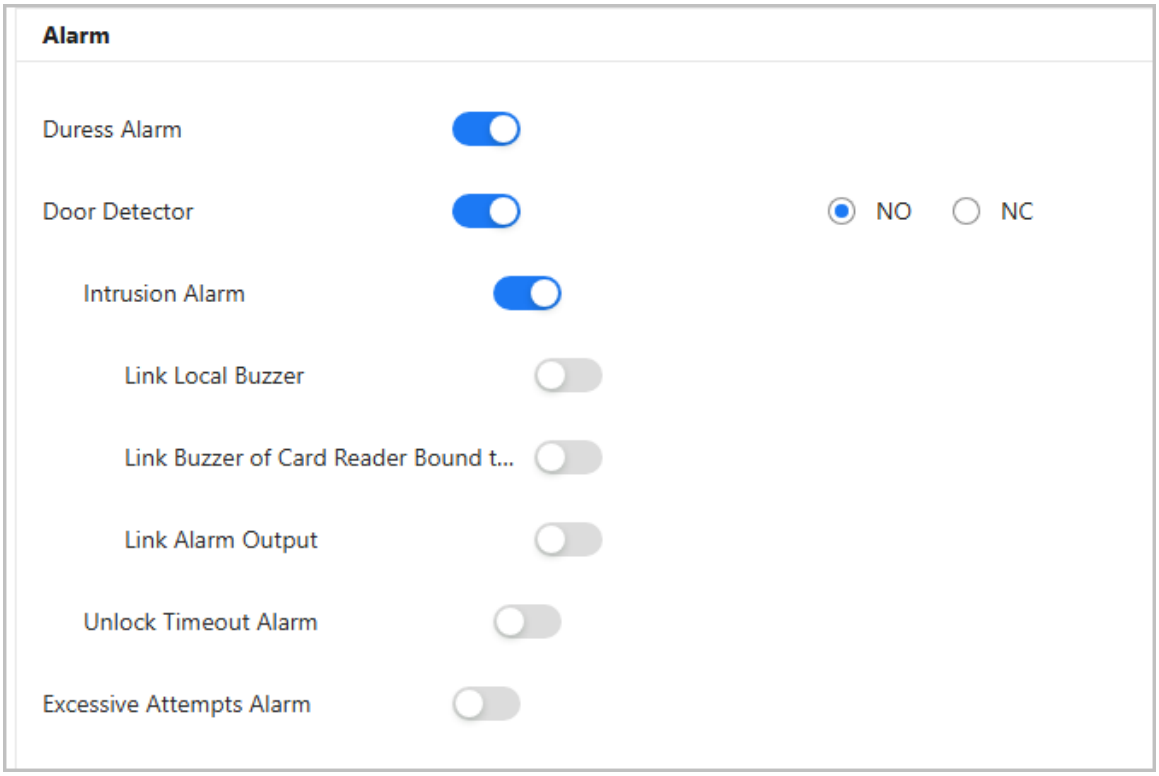


Table 2-5 Description of alarm parameters

Parameter	Description
Duress Alarm	An alarm will be triggered when a duress card, duress password or duress fingerprint is used to unlock the door.
Door Detector	With the door detector wired to your device, alarm can be triggered when doors are opened or closed abnormally. The door detector includes 2 types, including NC detector and NO detector. • NO: An open circuit is created when the door is actually closed. • NC: The sensor is in a shorted position when the door is closed.
Intrusion Alarm	After both the door detector and intrusion alarm are enabled, if the door is opened abnormally, an intrusion alarm will be triggered and last for a defined time. • **Link Local Buzzer** : When the alarm is triggered, the device beeps, and the duration is 15 seconds by default. • **Link Buzzer of Card Reader Bound to This Channel** : When the alarm is triggered, the RS-485 card reader that is bound to this channel beeps, and the duration is 15 seconds by default. • **Link Alarm Output** : Select the linked alarm output channel. When the alarm is triggered, the linked channel beeps, and the duration is 15 seconds by default.

Parameter	Description
Unlock Timeout Alarm	After both the door detector and unlock timeout alarm are enabled, if the door remains unlocked for longer than the defined timeout duration, the door timeout alarm will be triggered and last for the defined time. • **Link Local Buzzer** : When the alarm is triggered, the Device beeps. You can configure the buzzing mode and the duration. • **Link Buzzer of Card Reader Bound to This Channel** : When the alarm is triggered, the RS-485 card reader that is bound to this channel beeps. You can configure the buzzing mode and the duration. This function is available on select models. • **Link Alarm Output** : Select the linked alarm output channel. When the alarm is triggered, the linked channel beeps, and the duration is 15 seconds by default. Buzzing mode supports 2 methods. • Custom time: When the time exceeds the configured duration, the Device stops beeping. • Until door locks: When the door closes, the Device stops beeping.
Excessive Attempts Alarm	An alarm triggered when the number of failed attempts exceeds a preset limit within a specified time period. • **Link Local Buzzer** : When the alarm is triggered, the device beeps, and the duration is 15 seconds by default. • **Link Buzzer of Card Reader Bound to This Channel** : When the alarm is triggered, the RS-485 card reader that is bound to this channel beeps, and the duration is 15 seconds by default. • **Link Alarm Output** : Select the linked alarm output channel. When the alarm is triggered, the linked channel beeps, and the duration is 15 seconds by default.

Step 6 Click **Apply**.

Related Operations

The device supports tamper alarm by default, and it can be enabled simply by connecting the case wire.

2.6.4 Configuring Alarm

- 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.

2.6.4.1 Configuring Alarm Input Channel

You can configure alarm linkages.

Procedure

Step 1 Log in to the webpage.

Step 2 Select **Access Control** > **Alarm** > **Alarm Linkage Setting** > **Alarm**.

Step 3 Click  next to the alarm input channel to configure the parameters.

Figure 2-13 Alarm linkage

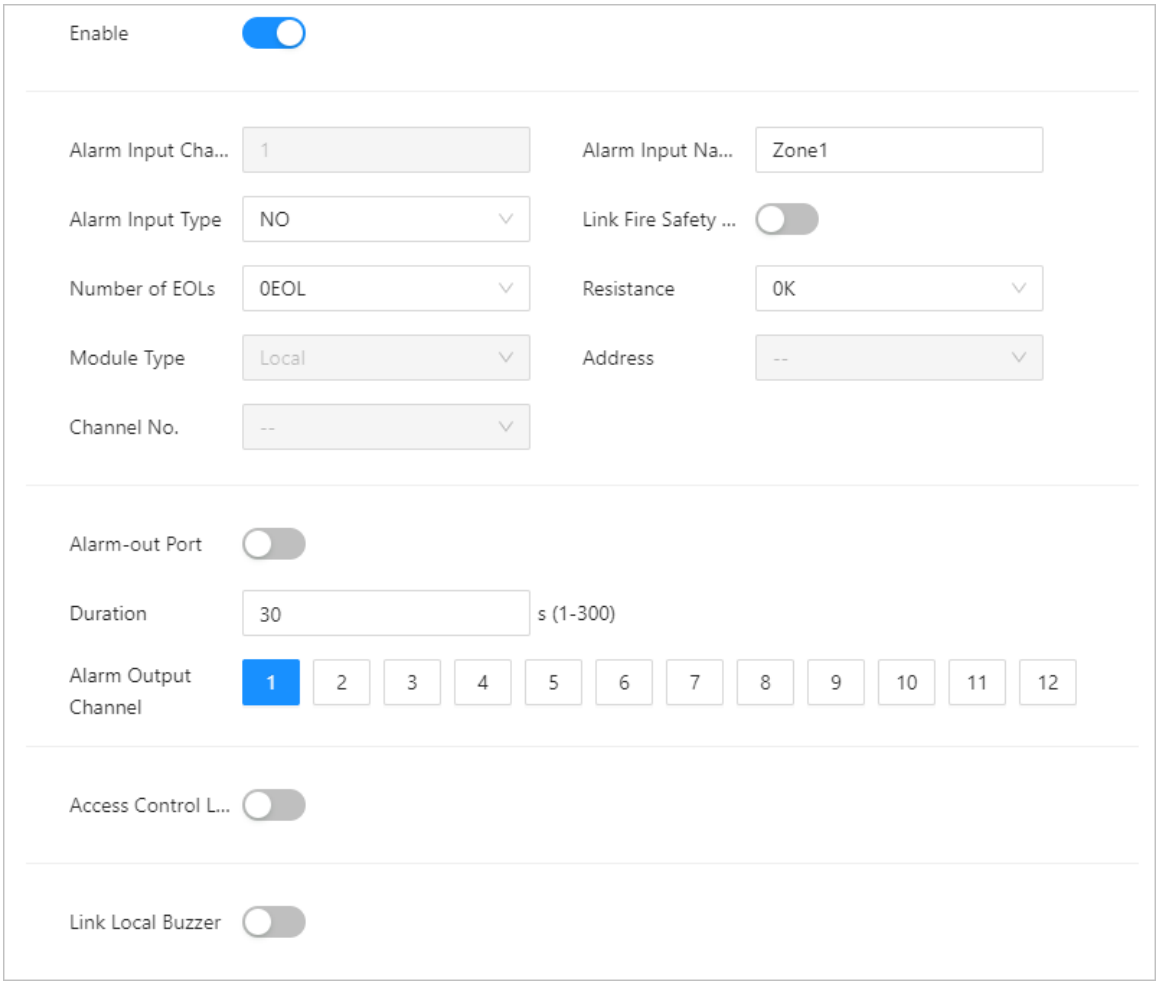


Table 2-6 Description of alarm input

Parameter	Description
Alarm Input Name	Customize the name.
Alarm Input Type	Select **No** or **NC** according to the external alarm input device type. • NO: The alarm input device is in a normally open (NO) circuit state when the alarm has not been triggered. Closing the circuit sets off the alarm. • NC: The alarm input is in a normally closed (NC) circuit state when the alarm has not been triggered. Opening a normally closed circuit sets off the alarm.

Parameter	Description
Link Fire Safety Control	After the function is enabled, all the alarm output channels and access control channels open by default.
Number of EOLs	• Local alarm input: You can select from **0EOL** (alarm and normal), **1EOL** (alarm, normal and open circuit) and **2EOL** (alarm, normal, open circuit and short circuit). • External expansion module: You can select from **0EOL** (alarm and normal), **1EOL NC** (alarm, normal and short circuit), **1EOL NO** (alarm, normal and open circuit), **2EOL** (alarm, normal, open circuit and short circuit), and **3EOL** (normal, alarm, open circuit, short circuit and block). When connecting external alarm input devices, 0EOL does not require resistor configuration, while 1EOL, 2EOL, and 3EOL require the configuration of 1, 2, and 3 resistors, respectively. The voltage values for each alarm state vary with different combinations of the number of resistors and their resistance values, so you should choose flexibly based on the actual external alarm devices used. • The model C access controller supports polymorphic alarm for only the first two alarm input channels. • The model B access controller does not support polymorphic alarm.
Resistance	• You do not need to configure this parameter for local alarm input. • Select the resistance according to the actual connected alarm device.
Module Type	Supports connecting ARM708-RS and ARM808-RS modules.
Address	Select the type, address and channel number according to the actual connected modules.
Channel No.	-- is invalid channel number. You do not need to configure this parameter for local alarm input.
Alarm-out Port	Enable **Alarm-out Port**, and then select alarm output channels. When the alarm is triggered, the selected alarm output alarms, and the duration is 30 seconds by default.
Duration	
Alarm Output Channel	

Parameter	Description
Access Control Linkage	After the function is enabled, when the alarm is triggered, the door becomes the configured status. • Auto: The door maintains the status before the alarm. If the door status is normal (authorized unlock) before the alarm, after the alarm is triggered, the door is still normal status. • NO: The door automatically opens when fire alarm is triggered. • NC: The door automatically closes when fire alarm is triggered. Linkage mode: When you select **NO** or **NC** as the door status, configure the linkage mode. • Strong Execution: When the fire alarm signal disappears, the door remains the current status. Please manually changes to its previous door status settings if you want to. • Weak Execution: When the fire alarm signal disappears, the door automatically returns to its previous door status.
Link Local Buzzer	After the function is enabled, when the alarm is triggered, the Device beeps, and the duration is 15 seconds by default.

Step 4 Click **OK**.

2.6.4.2 Configuring Alarm Output Channel

Configure the address, channel number and other parameters when external alarm output expansion modules are connected.

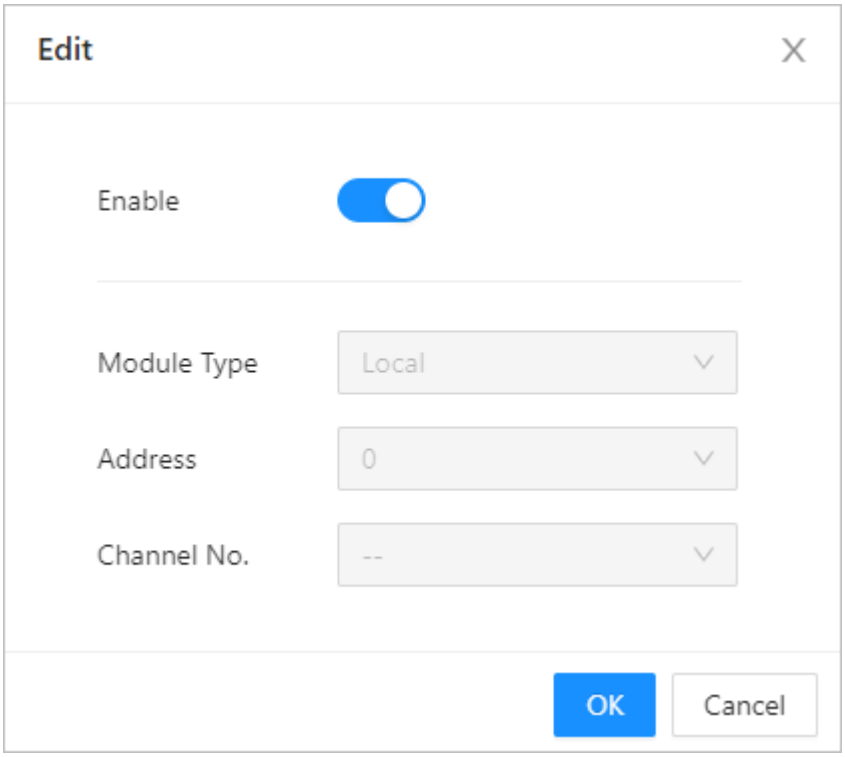
Procedure

Step 1 Log in to the webpage.

Step 2 Select **Access Control** > **Alarm** > **Alarm Linkage Setting** > **Alarm Output Channel**.

Step 3 Click  next to the alarm output channel to configure the parameters.

Figure 2-14 Alarm output channel



Step 4 Click **OK**.

2.6.4.3 Configuring Alarm Linkage

Procedure

Step 1 Log in to the webpage.

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

Step 3 Configure alarm event linkages, and then click **Apply**.

Table 2-7 Alarm event linkage

Parameter	Description
Tamper Alarm	The tamper alarm is triggered when someone has tried to physically damage the device. ● Buzzer: The buzzer sounds when the tamper alarm is triggered. You can configure the alarm duration. ● Link Alarm Output: The external alarm device generates alarms when the tamper alarm is triggered. You can configure the alarm duration.

Parameter	Description
Mains Electricity Power Failure Alarm	The alarm is triggered when the device loses its primary power supply from the mains. • Buzzer: The buzzer sounds when the mains electricity power failure alarm is triggered. You can configure the alarm duration. • Link Alarm Output: The external alarm device generates alarms when the mains electricity power failure alarm is triggered. You can configure the alarm duration. This function is only available for model C series units where the battery has been purchased as an optional accessory.
Battery Failure Alarm	The alarm is triggered when the device detects that its backup battery is malfunctioning, depleted, or unable to provide sufficient power. • Buzzer: The buzzer sounds when the battery failure alarm is triggered. You can configure the alarm duration. • Link Alarm Output: The external alarm device generates alarms when the battery failure alarm is triggered. You can configure the alarm duration. This function is only available for model C series units where the battery has been purchased as an optional accessory.
Battery Undervoltage Alarm	The alarm is triggered when the voltage of the backup battery drops below a predefined threshold. • Buzzer: The buzzer sounds when the battery under-voltage alarm is triggered. You can configure the alarm duration. • Link Alarm Output: The external alarm device generates alarms when the battery under-voltage alarm is triggered. You can configure the alarm duration. This function is only available for model C series units where the battery has been purchased as an optional accessory.

2.6.5 Configuring Advanced Parameters

2.6.5.1 Configuring First Card Unlock

Define certain people as the first-card holders, other users can verify their identities to unlock the door only after the first-card holders verify their identities first.

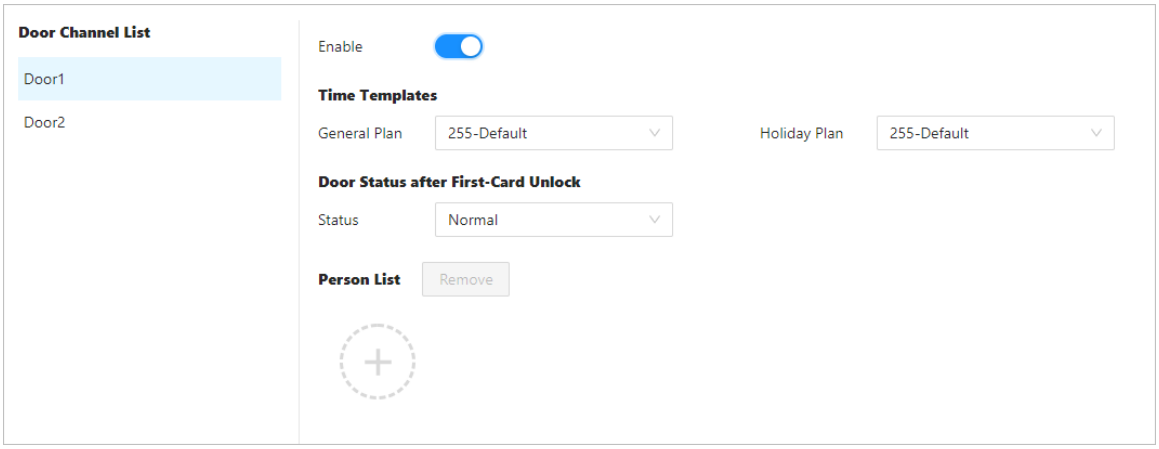
Procedure

Step 1 Log in to the webpage.

Step 2 Select **Access Control** > **Access Control Advanced Settings** > **First-card Unlock**.

Step 3 Select the door, and then click .

Figure 2-15 Assign first-card permission to users



Step 4 Select the general plan and the holiday plan.

First-card is valid only during the defined time. In each period of the plan, after the first-card holders verify their identities first, other users can verify their identifications.

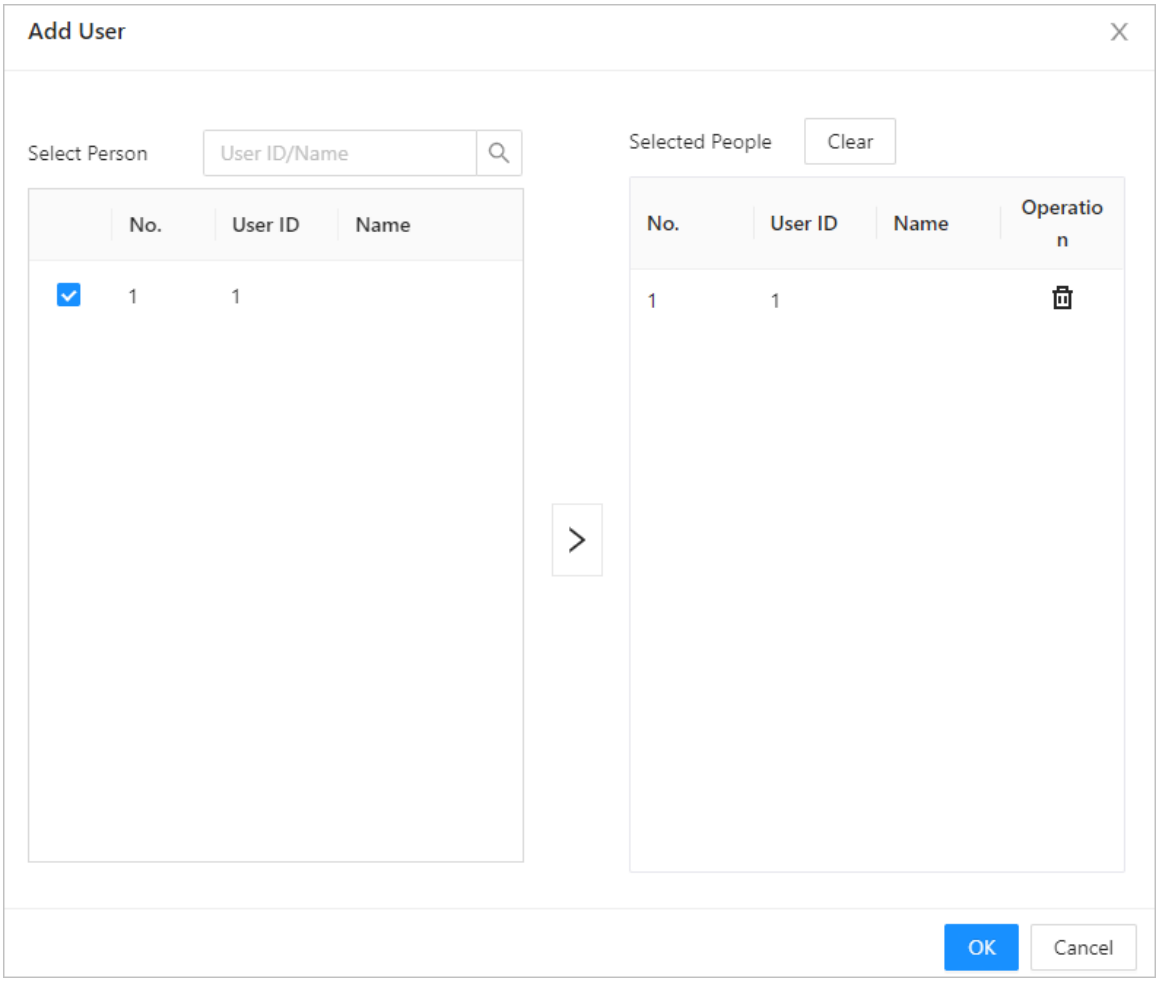
Step 5 Select the door status.

- Normal: Non-first cards users must verify their identities to unlock the door after first-card users grant access on the Access Controller.
- Always Open: The door stays open after first-card users grant access on the Access Controller.

Step 6 Click to add first-card users, and then click **OK**.

You can only select the user whose user type is **General User**.

Figure 2-16 Add first-card users



Step 7 Click **Apply**.

2.6.5.2 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.

Background Information

- If a person is authorized to enter, but exits without verification, an alarm will be triggered when they attempt to enter again, and access is denied at the same time.
- If a person enters by following someone else without verification, an alarm will be triggered when the they attempt to exit, and access is denied at the same time.

Procedure

Step 1 Log in to the webpage.

Step 2 Select **Access Control** > **Access Control Advanced Settings** > **Anti-passback Group Config**.

Step 3 Click **+** , configure the parameters and then click **Apply**.

Figure 2-17 Anti-passback

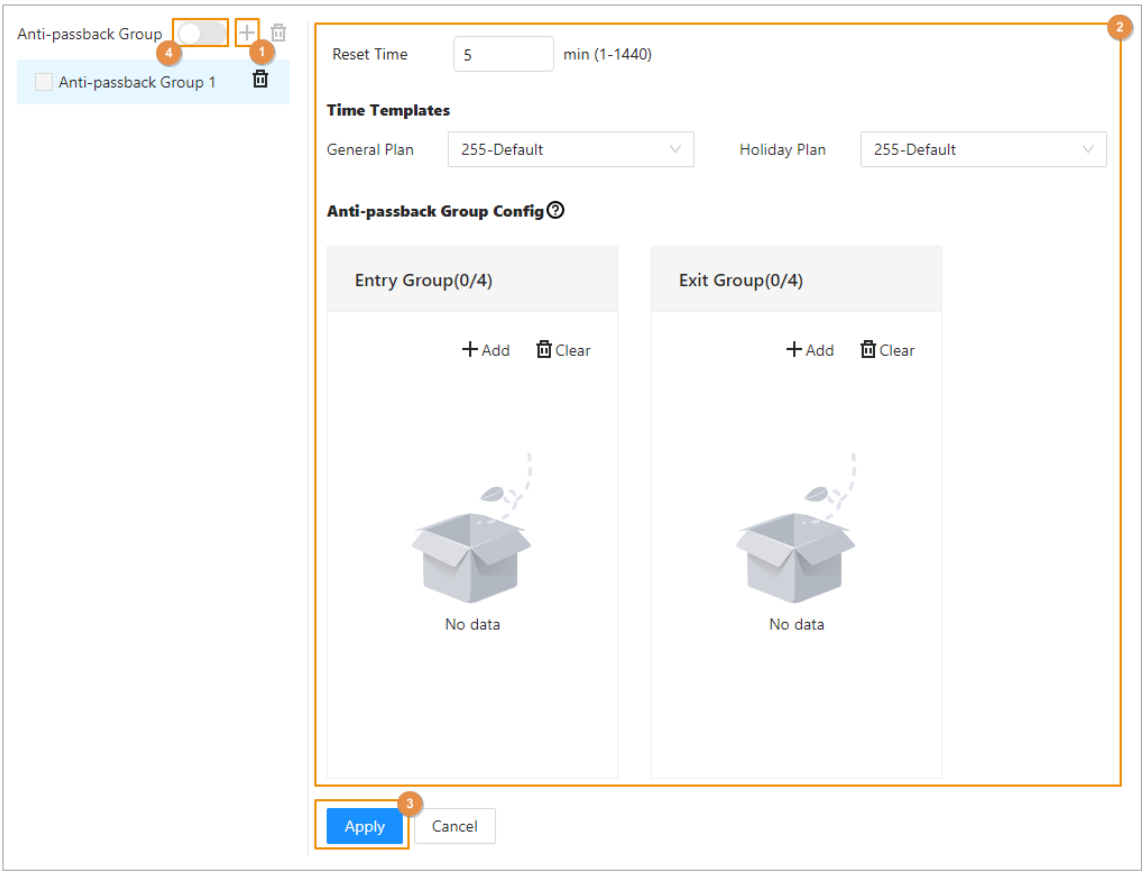


Table 2-8 Description of anti-passback group parameters

Parameter	Description
Reset Time	The reset time starts counting after the anti-passback is triggered. Once the reset time elapses, the person's anti-passback status is cleared, and they can enter or exit the door again. For example: If a person verifies entry but does not verify exit, and they verify entry again within 30 minutes, anti-passback is triggered. If they verify entry again after 30 minutes, anti-passback is also triggered.
General Plan	Select the weekly plan and the holiday plan. Anti-passback is effective during the defined time.
Holiday Plan	
Entry Group	Click **Add**, and then select card readers for entry and exit. At least 2 groups must be added.
Exit Group	

Step 4 Click **Apply**.

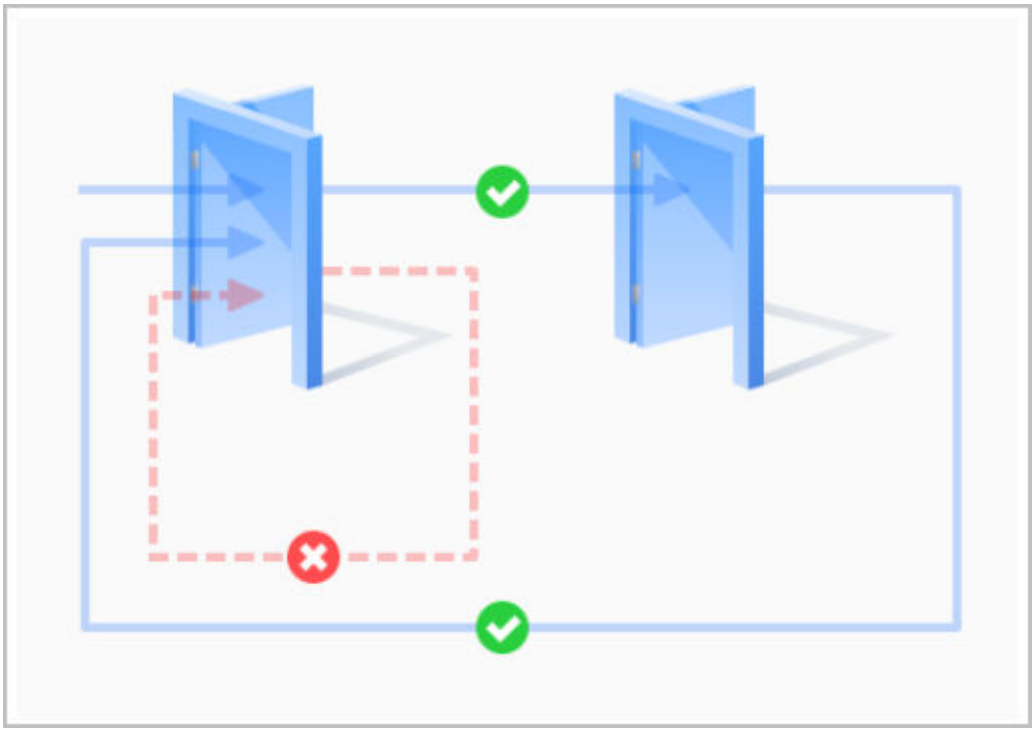
Step 5 Click to enable the function.

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 group 1, and then at a

reader for group 2, and then at a reader in group 3, etc. As long as you swipe card following the established sequence, the system works fine.

Figure 2-18 Anti-passback function



2.6.5.3 Configuring Interlock within Group

Each interlock group contains only one door group, with the maximum number of doors matching the controller's door capacity, and doors are selected within the device. If one door in the group is in an open status, the other doors in the group cannot be opened.

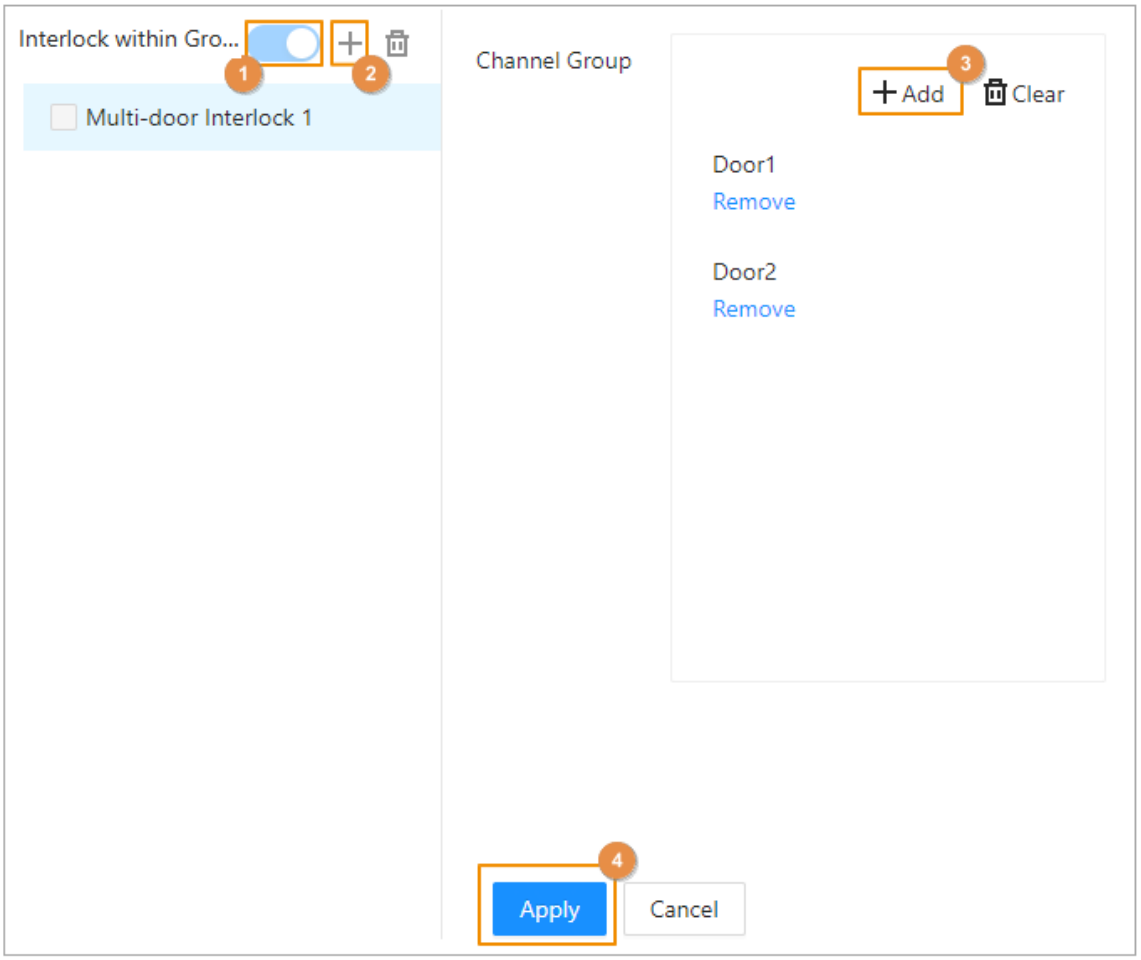
Procedure

Step 1 Log in to the webpage.

Step 2 Select **Access Control** > **Access Control Advanced Settings** > **Multi-door Interlock** > **Interlock within Group**.

Step 3 Click to enable the function, and then click **+**.

Figure 2-19 Interlock within group



Step 4 Click **Add** , select the door, and then click **OK**.

Step 5 Click **Apply**.

2.6.5.4 Configuring Interlock between Groups

Each interlock group consists of 2 door groups, with the maximum number of doors matching the controller's door capacity, and doors are selected within the device. If a door in one group is open, the doors in the other group cannot be opened. Intra-group interlock and inter-group interlock do not conflict with each other. After inter-group interlock is configured, intra-group interlock can still be enabled through settings

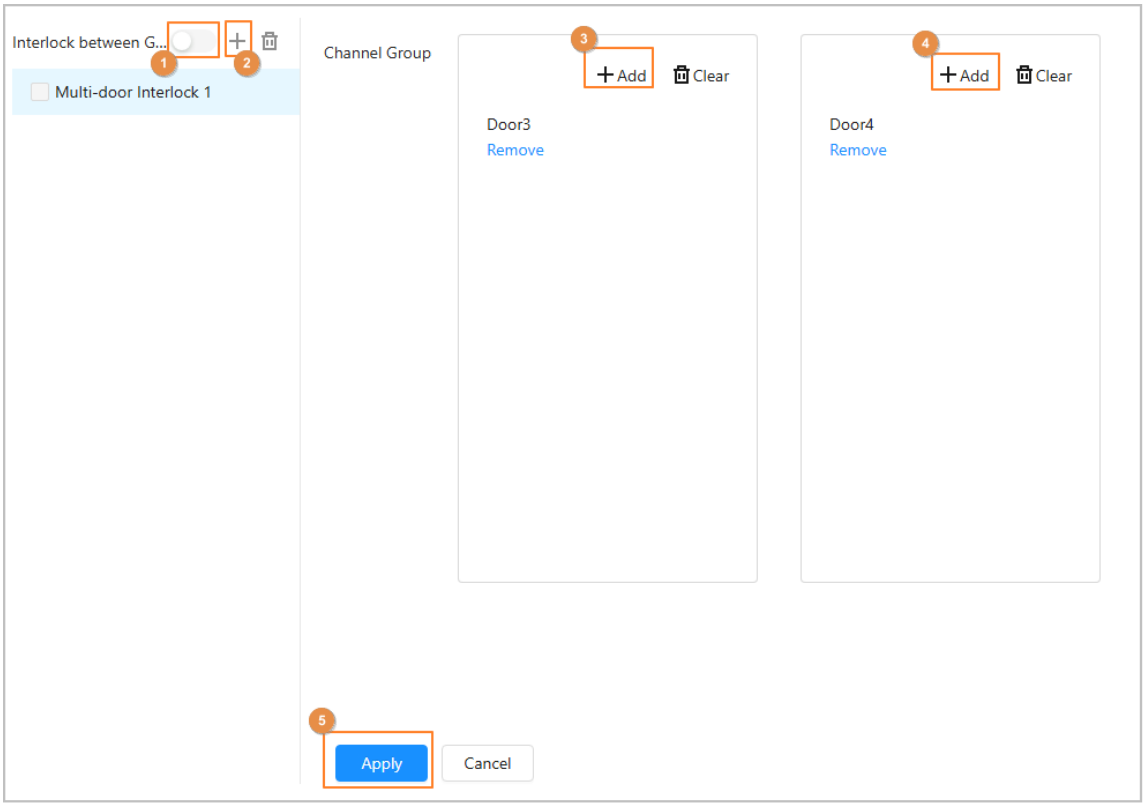
Procedure

Step 1 Log in to the webpage.

Step 2 Select **Access Control** > **Access Control Advanced Settings** > **Multi-door Interlock** > **Interlock between Groups**.

Step 3 Click to enable the function, and then click **+**.

Figure 2-20 Interlock within group



Step 4 Click **Add** , select the door, and then click **OK**.

Step 5 Click **Apply**.

2.6.6 Configuring Unlock Methods

Procedure

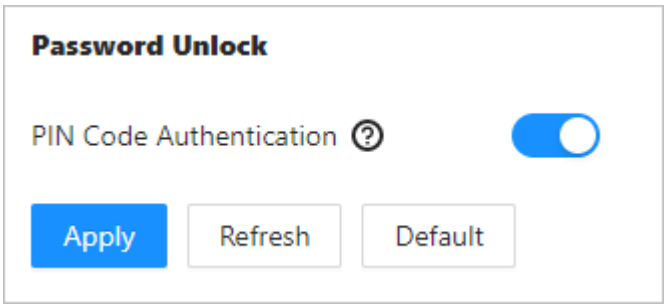
Step 1 Log in to the webpage.

Step 2 Select **Access Control** > **Unlock Method Config**.

Step 3 Turn on or turn off **PIN Code Authentication**.

When PIN code authentication is enabled, you can open the door with just the password.

Figure 2-21 PIN code authentication



Step 4 Click **Apply**.

2.6.7 Card Settings

2.6.7.1 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 2-22 Card parameters

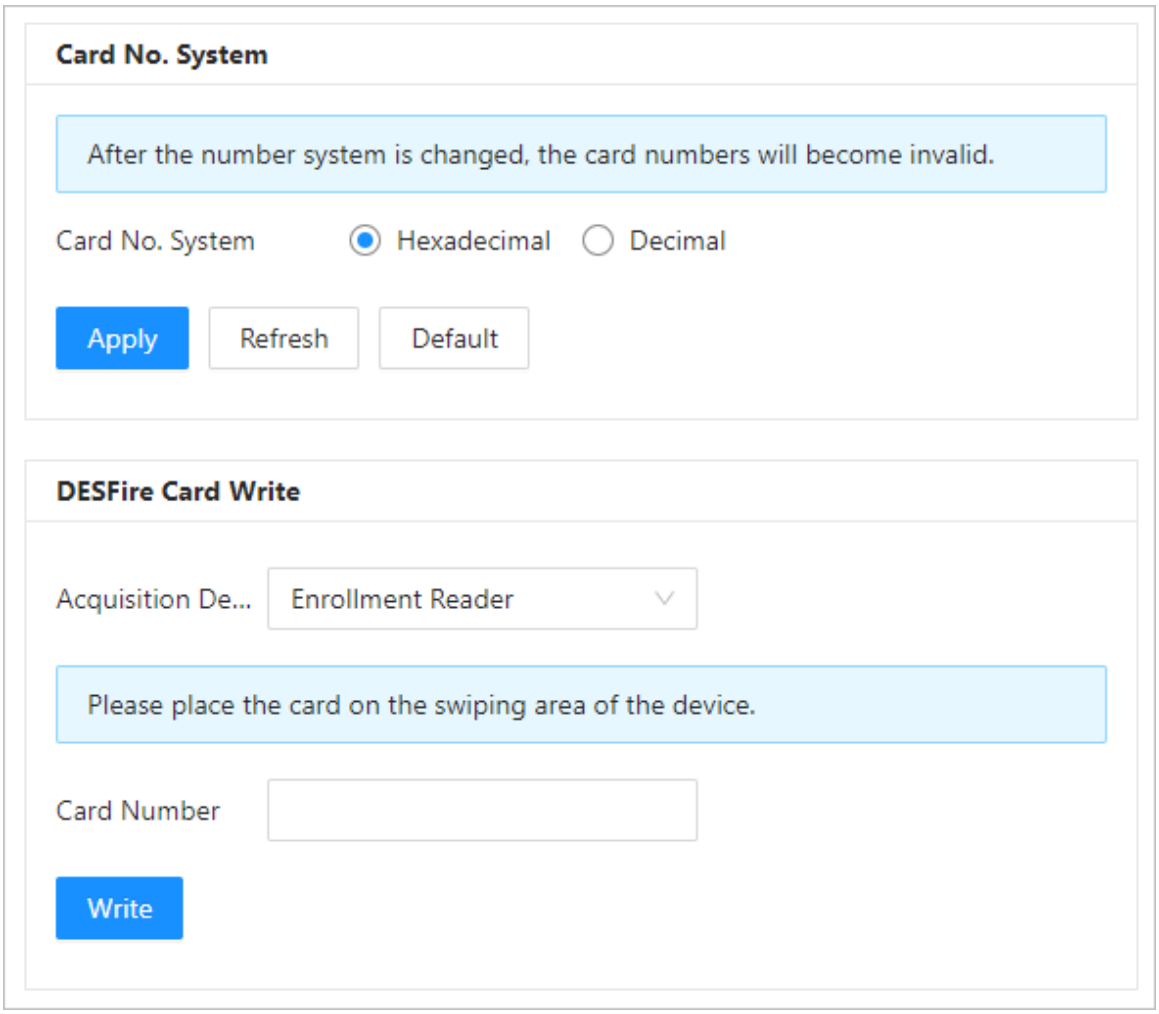


Table 2-9 Card parameters description

Item	Parameter	Description
Card No. System	Card No. System	Select decimal format or hexadecimal format for the card number when Wiegand card reader is connected. The card No. system is the same for both card number input and output.
DESFire Card Write	Acquisition Device	Select the device, place the card on the reader, enter the card number, and then click **Write** to write card number to the card. ● Only supports hexadecimal format. ● Supports up to 8 characters.
	Card Number	

2.6.7.2 Configuring Access Card Rule Parameters

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

Procedure

Step 1 Log in to the webpage.

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

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

Figure 2-23 Add new Wiegand formats

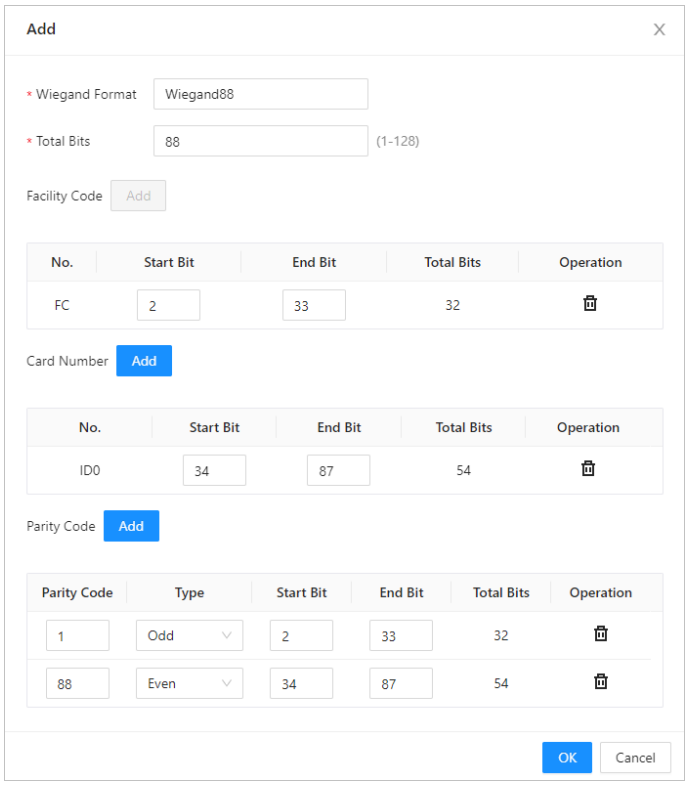


Table 2-10 Wiegand format description

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

Step 4 Click **OK**.

Related Operations

- You can also click **Add Protocol** to import a Wiegand file to the platform.
- Facility Code: If the function is enabled, and you have set **Card No. System** to decimal format on the **Person Management** page, the facility code and the card number are transformed into decimal format separately, and then combine together.
- HID26: If the function is turned on:
  - Only Wiegand 26 is supported.
  - The platform only supports displaying card in decimal format.
  - The card number must have 5 characters and the facility code must have 3 characters at most. When you manually entering card, the system will automatically add leading zero to fixed number length. For example, if the card number you enter is less than 5 characters, like 56, leading zero is added to fix the number length to 5 characters, like 00056, and another 0 is added to function as a facility code. Therefore, the final card No. will be 000056.

2.6.7.3 Configuring Custom Conversion

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

Procedure

Step 1 Log in to the webpage.

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

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

- Auto match: Use the built-in conversion rule of the Device to convert the card number.
  1. Select the input type.
     - RS-485 input: Swipe the card on the connected RS-485 card reader to read the card.
     - Wiegand input: Swipe the card on the connected Wiegand card reader to read the card.
  2. Read the card number through the device or enter the card number before conversion, and then enter the card number after conversion.
  3. Click **Auto Match**.

- If the card numbers are successfully matched, you can click **Export** to export the rule and import to another device for quickly switching the match rules.
- If the card numbers failed to match, it indicates that there is no match rule in the system. You need to customize the match rule script, and select **Import Conversion Rule** to import the rule to the device.
- If you need to modify the match rule, click **Change Matching Rule**.

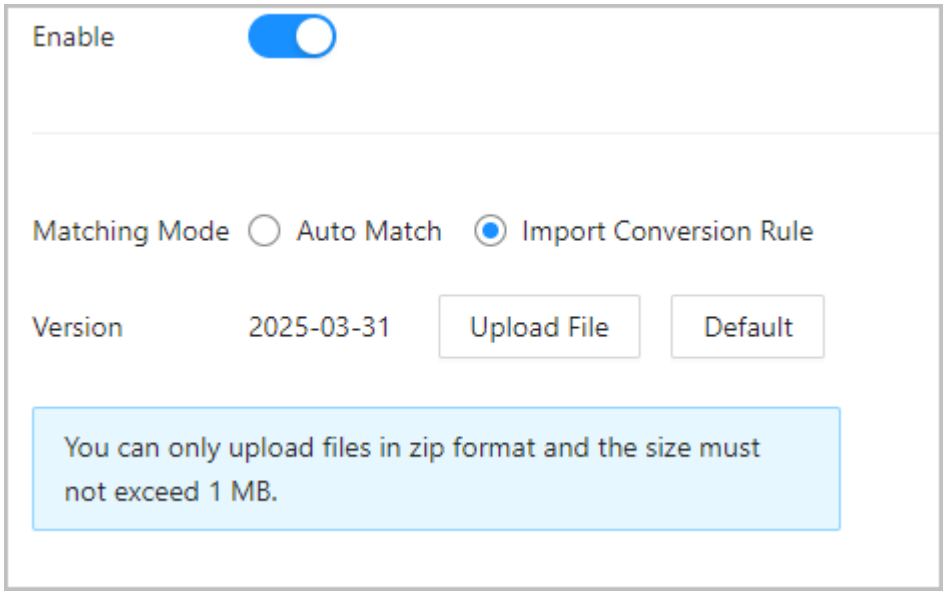
Figure 2-24 Auto match



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

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

Figure 2-25 Import conversion rule



2.6.8 Configuring QR Code

Procedure

Step 1 On the webpage, select **Access Control** > **QR Code**.

Figure 2-26 QR code



Step 2 Configure the parameter, and then click **Apply**.

After the QR code is generated, and the validity of your QR codes will last for a defined time before it expires.

The validity periods of QR codes on QR Code Validity Period, DSS Pro, and Dolynk override each other. This means whichever platform last modified the time will have its latest configuration take precedence, and the original validity period will be invalidated.

2.6.9 Configuring Back-end Comparison

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

Integration with third-party platforms must be achieved through SDK or API.

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

Figure 2-27 Back-end comparison

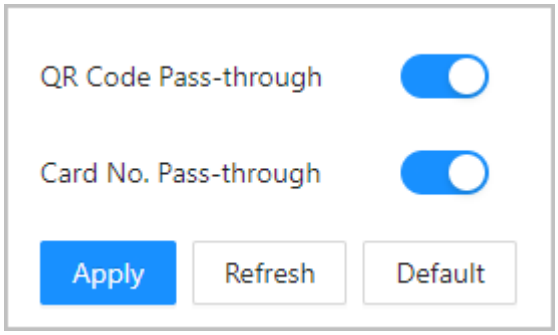


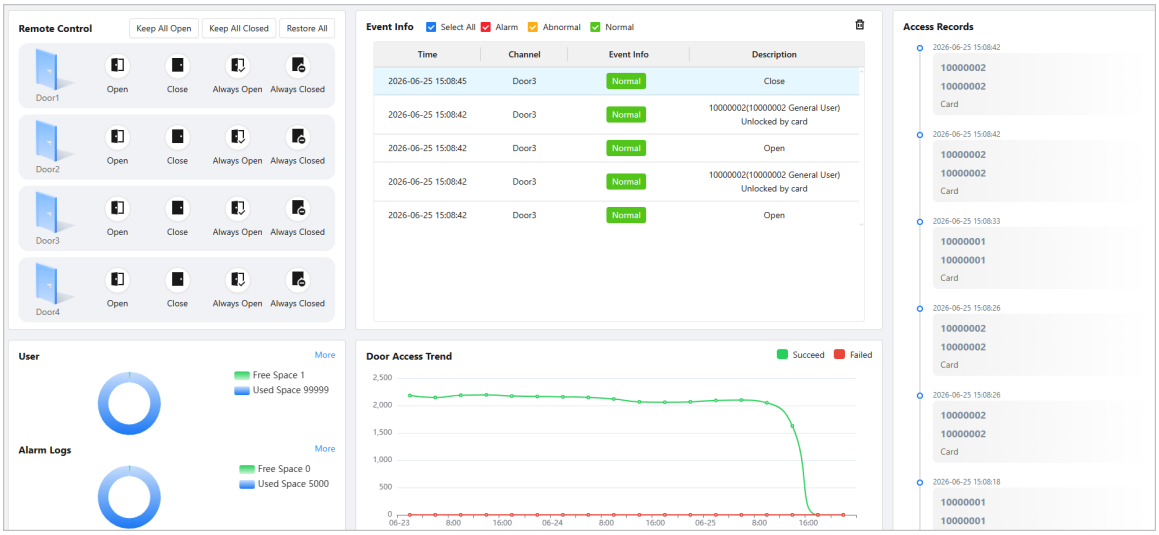
Table 2-11 Back-end comparison

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

2.7 Access Monitoring

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

Figure 2-28 Access monitoring



Remote Control

- Click **Open** or **Close** next to the door to remotely control the door.
- Select the door, and then click **Always Open** or **Always Closed** to remotely control the door.

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

Event Information

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

Access Records

View the access records of the device.

Door Access Trend

View the door access trend, including successful and failed access.

User Information and Alarm Logs

View the users registered on the device, and the alarm logs. Click **More** to view details.

2.8 Network Settings

2.8.1 Configuring TCP/IP

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

Procedure

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

Step 2 Configure the parameters.

Figure 2-29 TCP/IP

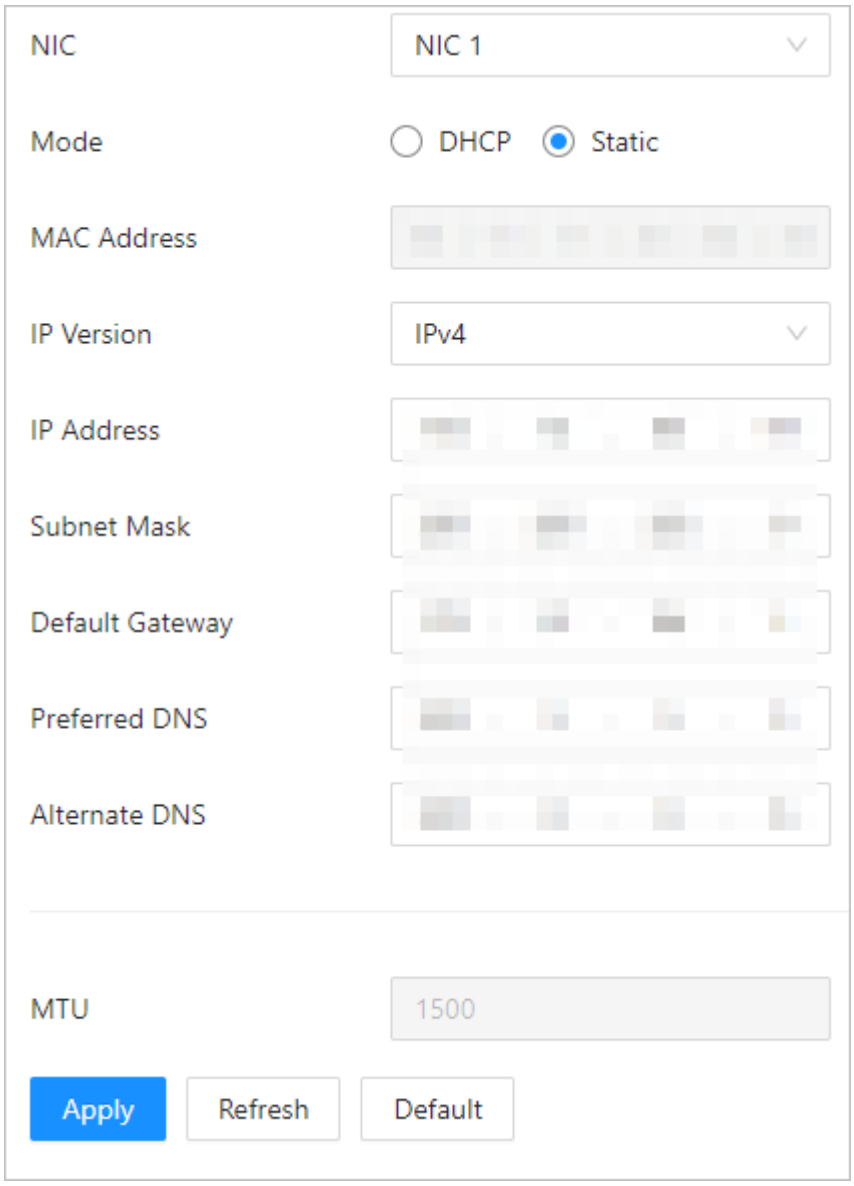


Table 2-12 Description of TCP/IP

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

Parameter	Description
MAC Address	MAC address of the Device.
IP Version	IPv4 or IPv6.
IP Address	If you set the mode to **Static**, configure the IP address, subnet mask and gateway. - IPv6 address is represented in hexadecimal. - IPv6 version does 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 **Apply**.

2.8.2 Configuring Port

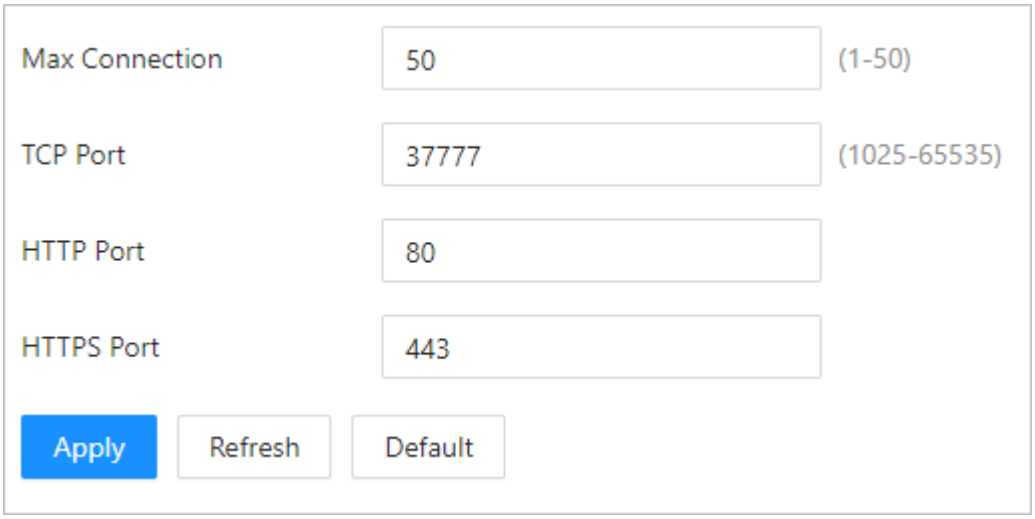
You can limit access to the Device at the same time through webpage, desktop client and mobile client.

Procedure

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

Step 2 Configure the ports.

Figure 2-30 Configure ports



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

Table 2-13 Description of ports

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

Step 3 Click **Apply**.

2.8.3 Configuring Basic Services

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** > **Basic Services**.

Step 2 Configure the basic service.

Figure 2-31 Basic service

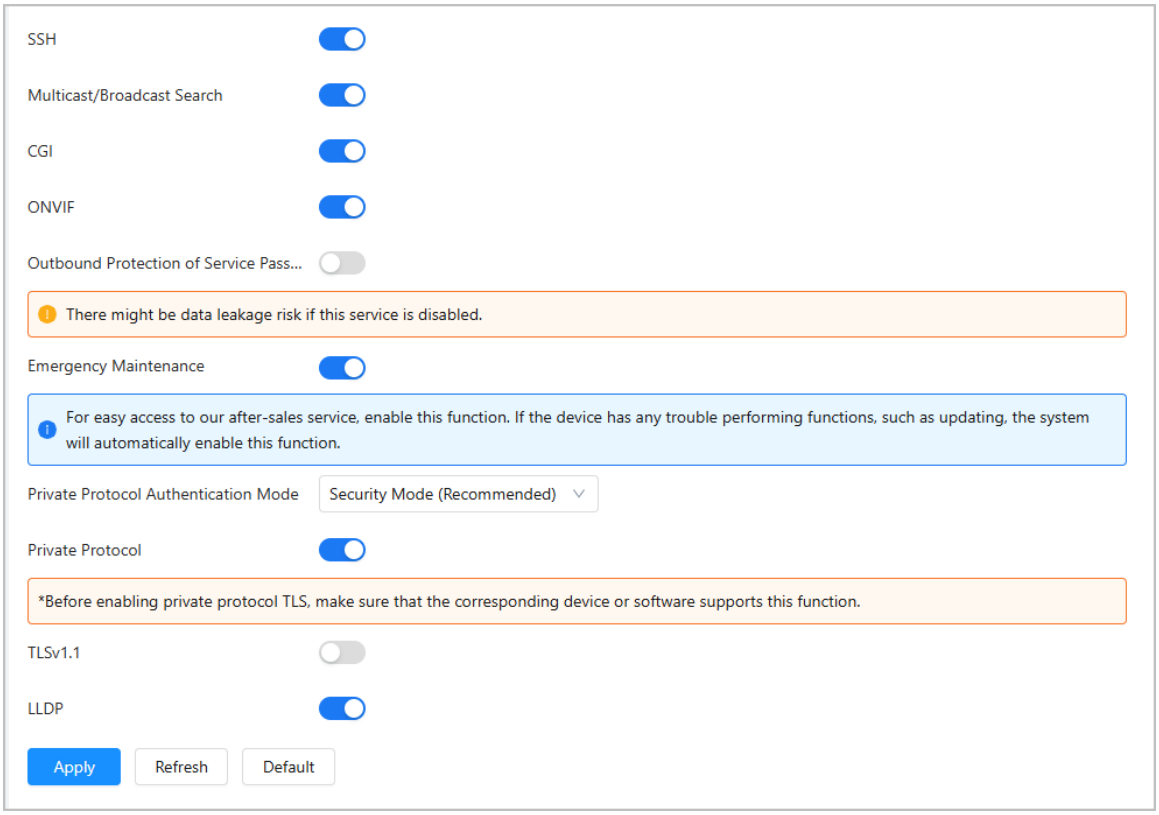


Table 2-14 Basic service parameter description

Parameter	Description
SSH	SSH, or Secure Shell Protocol, is a remote administration protocol that allows users to access, control, and modify their remote servers over the internet.
Multicast/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.
Outbound Protection of Service Password	The device password cannot be obtained through third-generation protocol tools once this function is enabled.
Emergency Maintenance	It is turned on by default.

Parameter	Description
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.
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. TLSv1.1 is disabled by default. In fact, TLSv1.2 is used instead of TLSv1.1.
LLDP	Enable the LLDP (Link Layer Discovery Protocol) function to discover network devices at the link layer. It is disabled by default.

Step 3 Click **Apply**.

2.8.4 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.

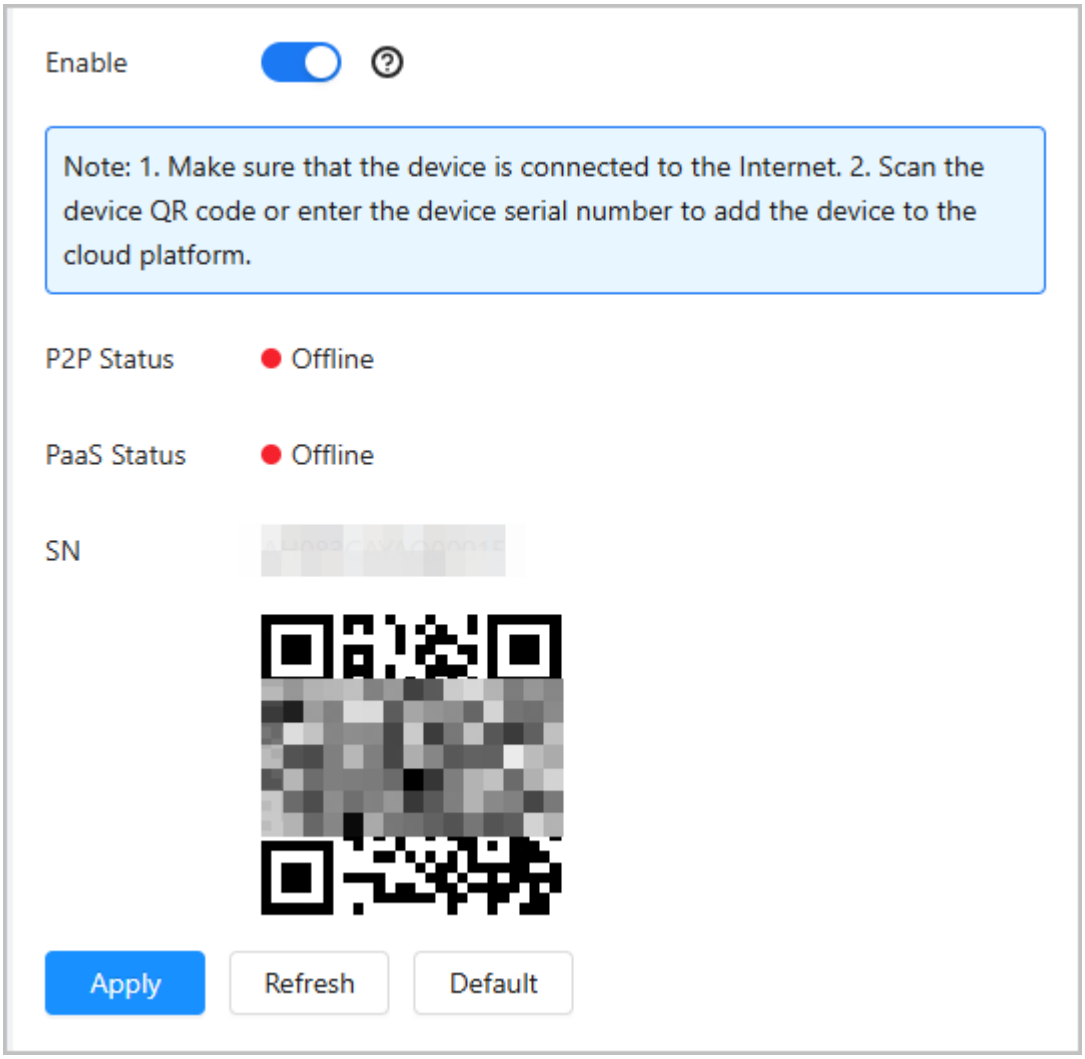
Procedure

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

Step 2 Turn on the cloud service function.

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

Figure 2-32 Cloud service



Step 3 Click **Apply**.

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

2.8.5 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 **Communication Setting** > **Auto Registration**.

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

Figure 2-33 Auto Registration

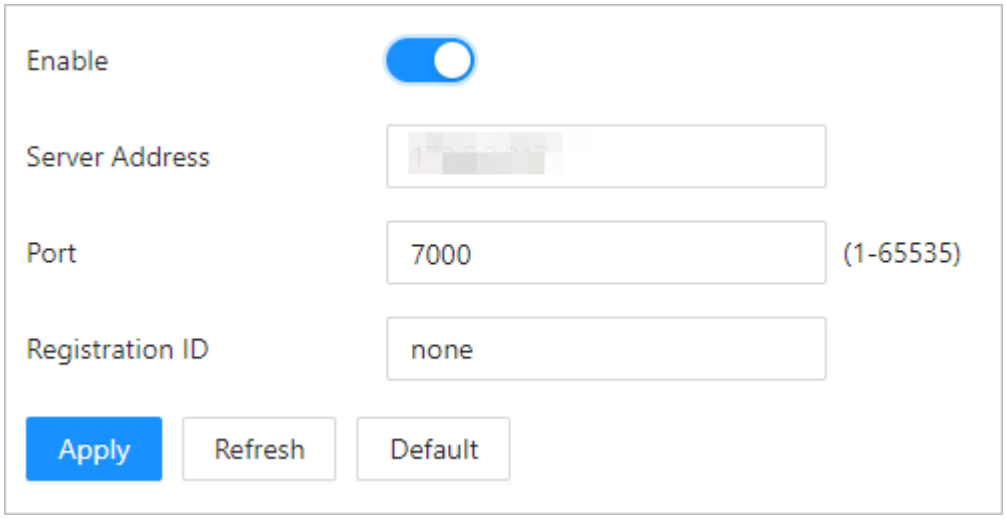


Table 2-15 Automatic registration description

Parameter	Description
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**.

2.8.6 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** > **CGI Auto Registration**.

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

Step 3 Click , and then configure parameters.

Figure 2-34 CGI auto registration

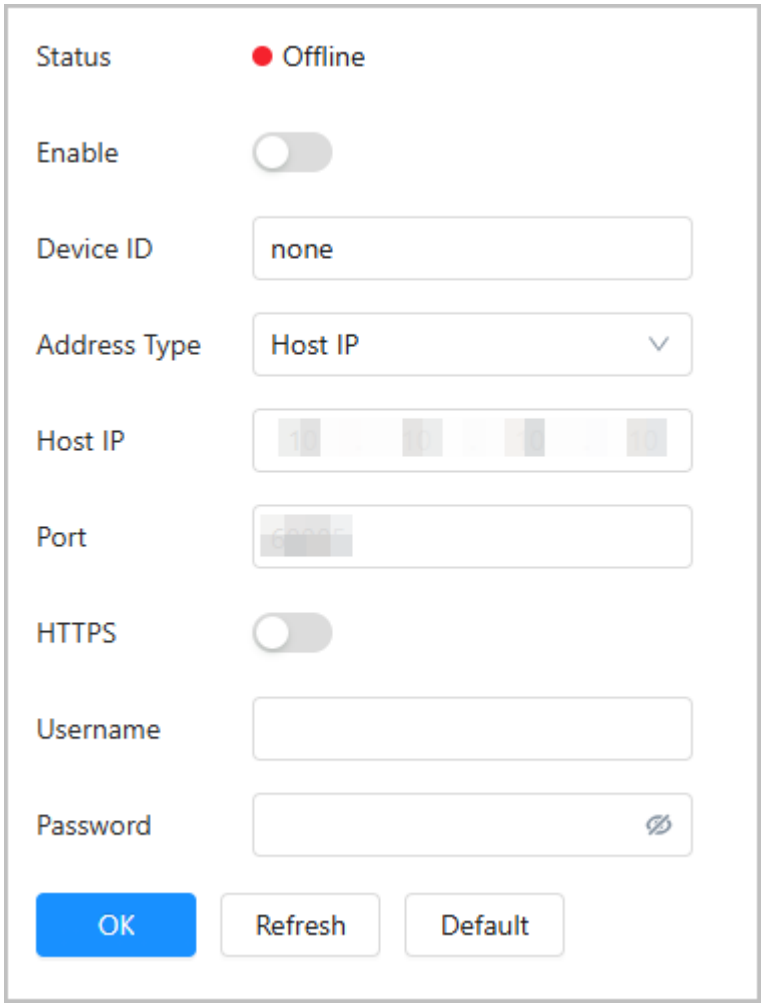


Table 2-16 Automatic registration description

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

Step 4 Click **Apply**.

2.8.7 Configuring Auto Upload

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

Procedure

Step 1 On the home page, select **Communication 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 2-35 Automatic upload

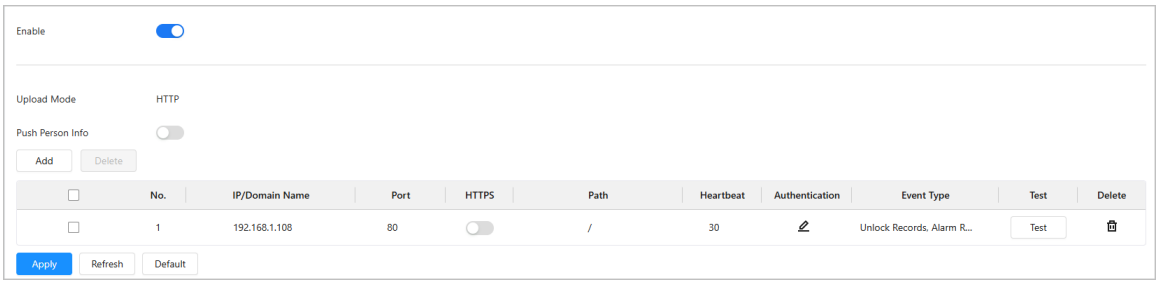


Table 2-17 Parameters description

Parameter	Description
IP/Domain Name	The IP or domain name of the management platform.
Port	The port of the management platform.
HTTPS	Access the management platform through HTTPS. HTTPS secures communication over a computer network.
Authentication	Enable account authentication when you access the management platform. Login username and password are required.
Even Type	Select the type of event (unlock records and alarm records) 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**.

2.9 Configuring the System

2.9.1 User Management

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

2.9.1.1 Adding Administrators

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

Procedure

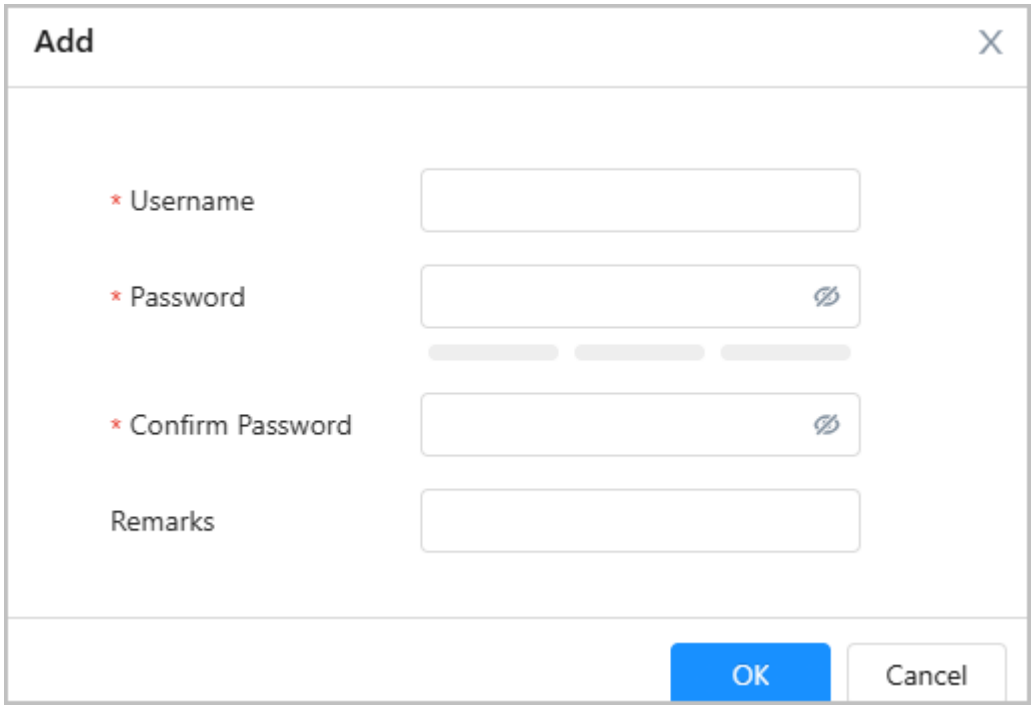
Step 1 On the home page, select **System** > **Account**.

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

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

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

Figure 2-36 Add administrators



Step 3 Click **OK**.

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

2.9.1.2 Resetting the Password

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

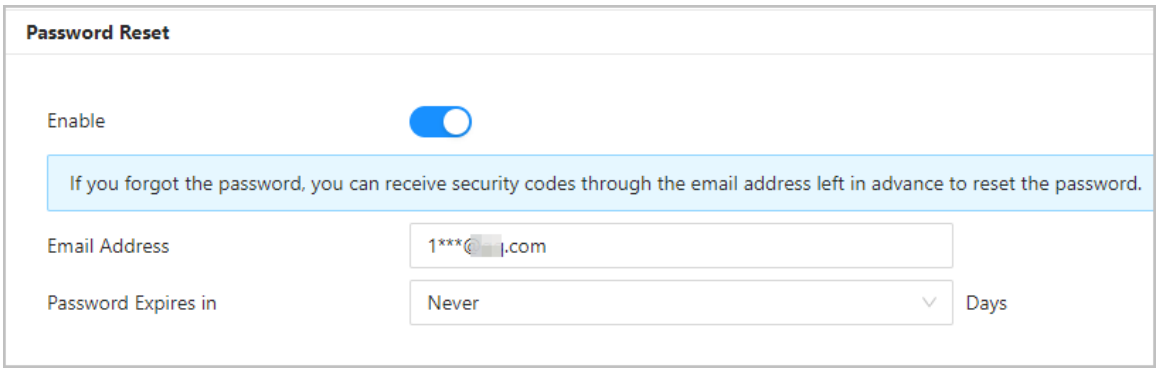
Procedure

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

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

Step 3 Turn on the password reset function.

Figure 2-37 Reset Password



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

Step 4 Click **Apply**.

2.9.1.3 Adding ONVIF Users

Background Information

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

Procedure

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

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

Figure 2-38 Add ONVIF user

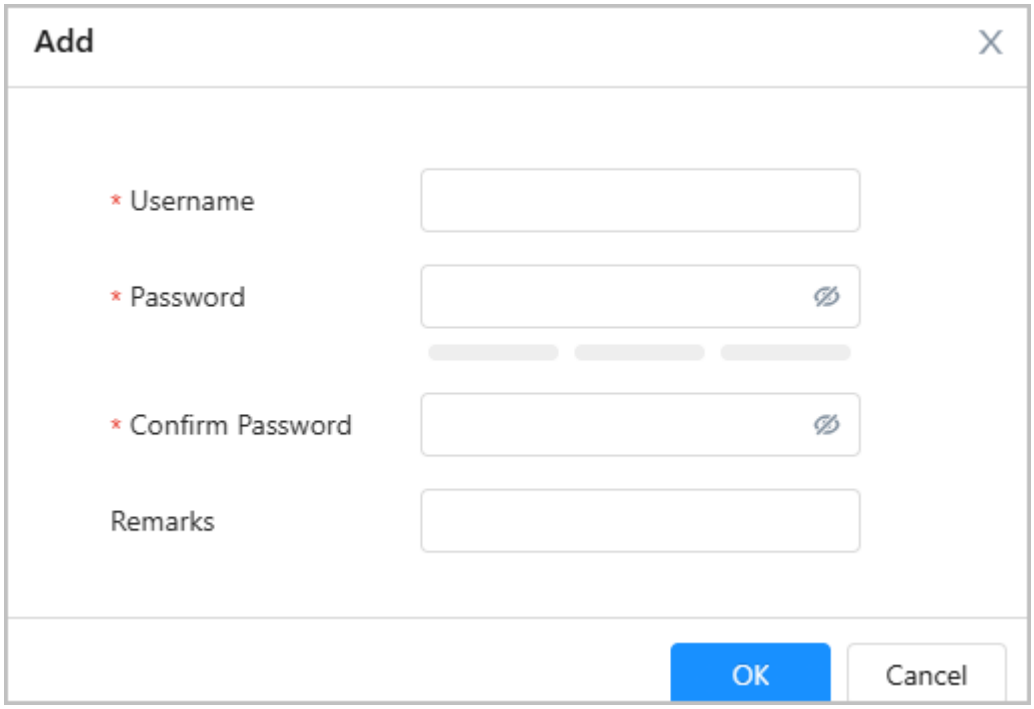


Table 2-18 ONVIF user description

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

Step 3 Click **OK**.

2.9.2 Viewing Online Users

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

2.9.3 Configuring Time

Procedure

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

Step 2 Configure the time of the Platform.

Figure 2-39 Date settings

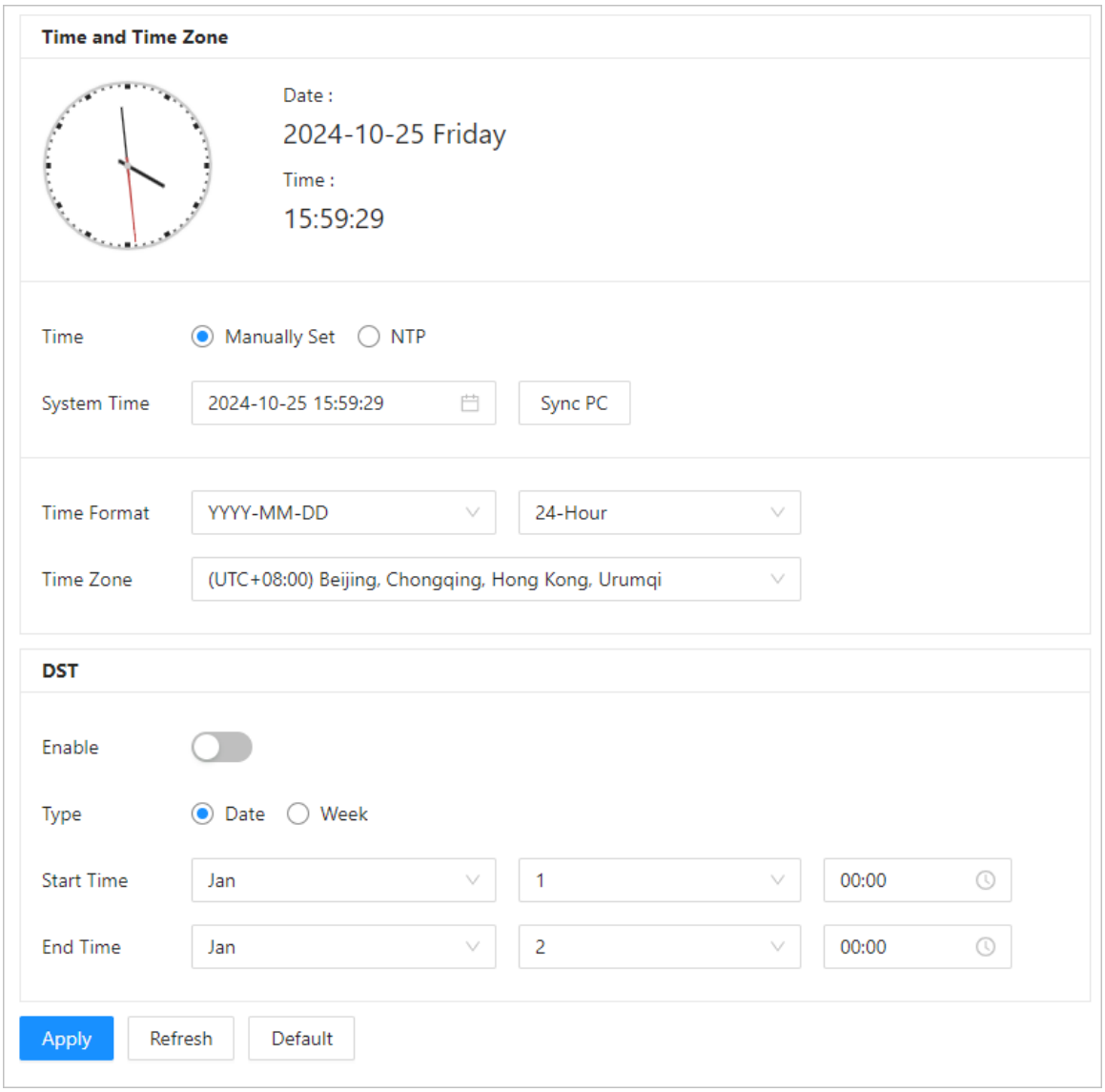


Table 2-19 Time settings description

Parameter	Description
Time	• Manual Set: Manually enter the time or you can click **Sync Time** to sync time with computer. • NTP: The Device will automatically sync the time with the NTP server. ◇ **Server** : Enter the domain of the NTP server. ◇ **Port** : Enter the port of the NTP server. ◇ **Interval** : Enter its time with the synchronization interval.
Time format	Select the time format.
Time Zone	Enter the time zone.
DST	1. (Optional) Enable DST. 2. Select **Date** or **Week** from the **Type**. 3. Configure the start time and end time of the DST.

Step 3 Click **Apply**.

2.10 Security Settings(Optional)

2.10.1 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.

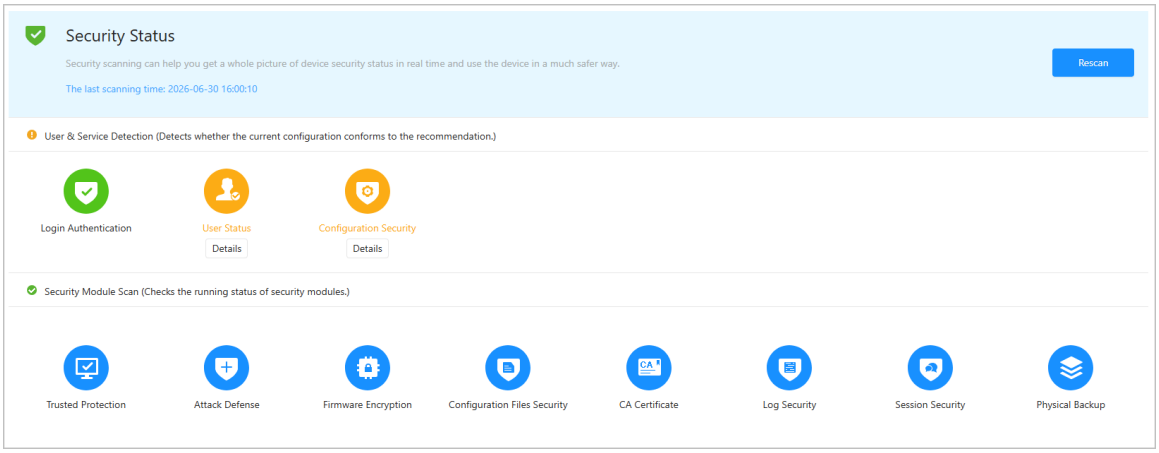
Procedure

Step 1 Select **Security** > **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 2-40 Security Status



Related Operations

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

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

2.10.2 Configuring HTTPS

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

Procedure

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

Step 2 Turn on the HTTPS service.

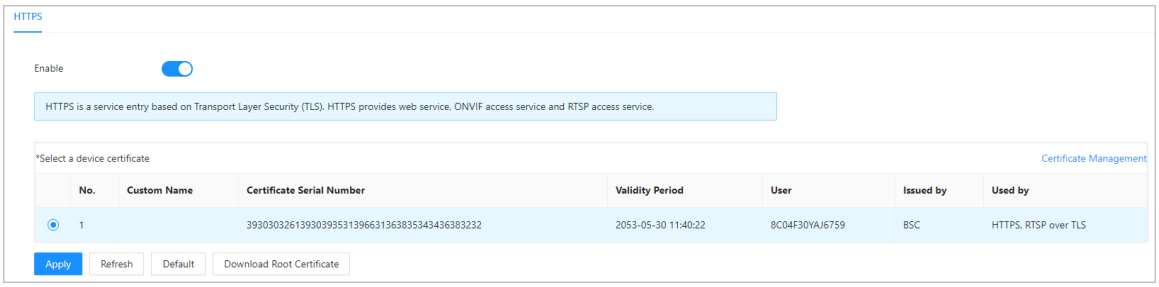
If you turn on the compatible with TLS v1.1 and earlier versions, security risks might occur. Please be advised.

Step 3 Select the certificate.

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

.

Figure 2-41 HTTPS



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.

2.10.3 Attack Defense

2.10.3.1 Configuring Firewall

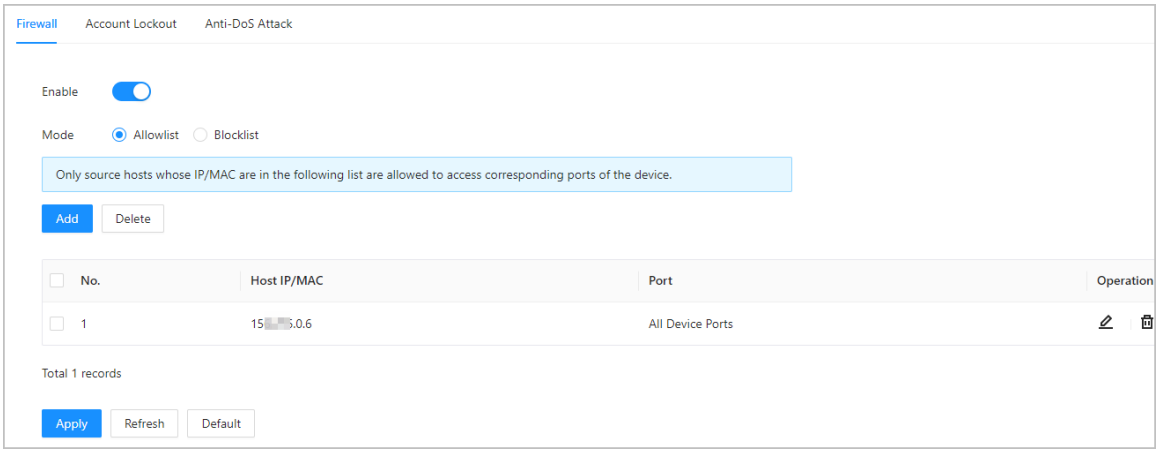
Configure firewall to limit access to the Device.

Procedure

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

Step 2 Click to enable the firewall function.

Figure 2-42 Firewall

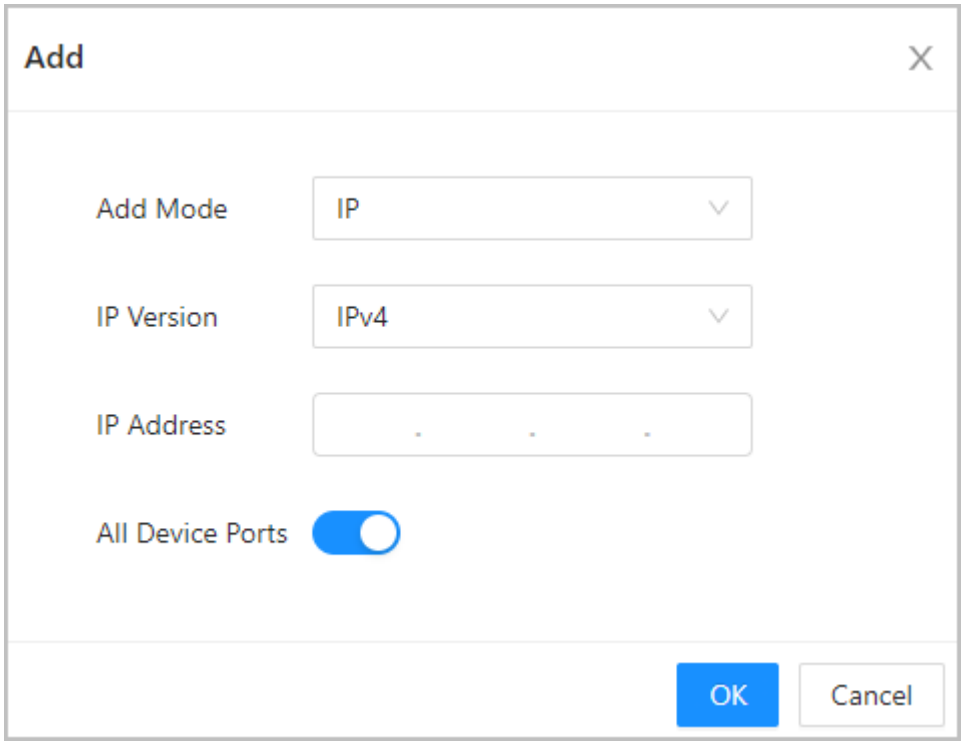


Step 3 Select the mode: **Allowlist** and **Blocklist**.

- **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 2-43 Add IP information



Step 5 Click **OK**.

Related Operations

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

2.10.3.2 Configuring Account Lockout

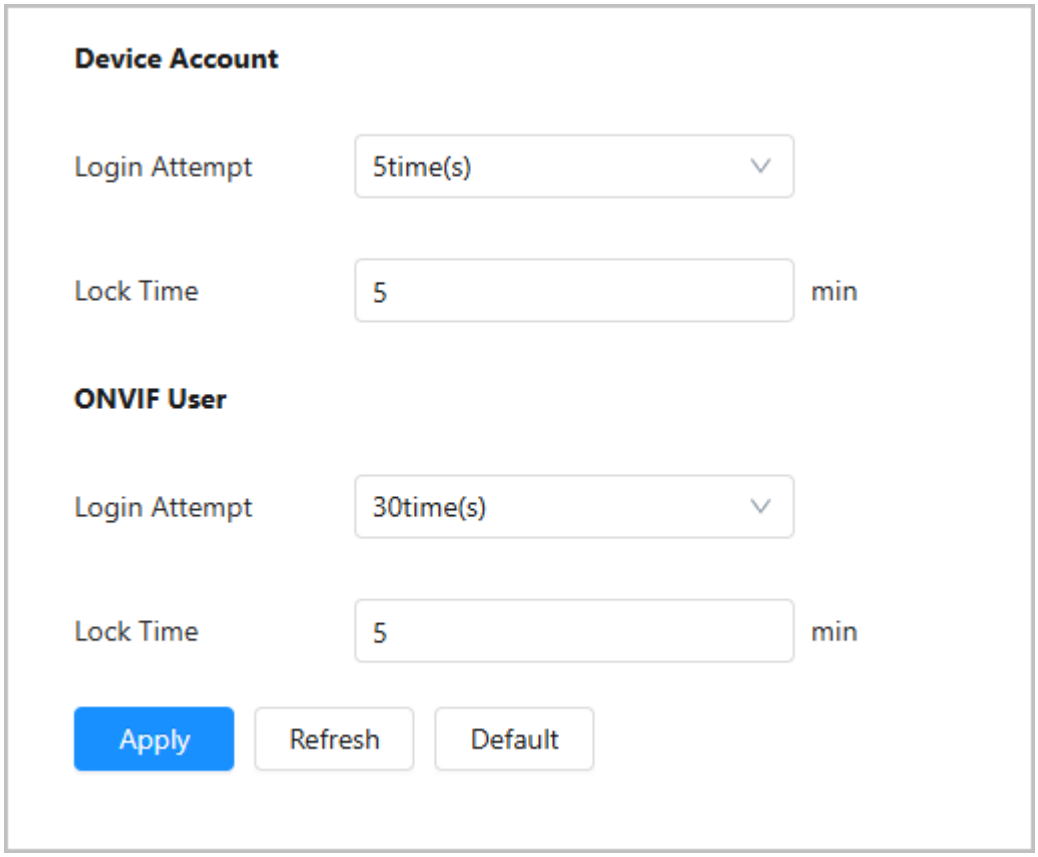
If the incorrect password is entered for a defined number of times, the account will be locked.

Procedure

Step 1 Select **Security** > **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 2-44 Account lockout



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

Step 3 Click **Apply**.

2.10.3.3 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 **Security** > **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 2-45 Anti-DoS attack



Step 3 Click **Apply**.

2.10.4 Installing Device Certificate

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

2.10.4.1 Creating Certificate

Create a certificate for the Device.

Procedure

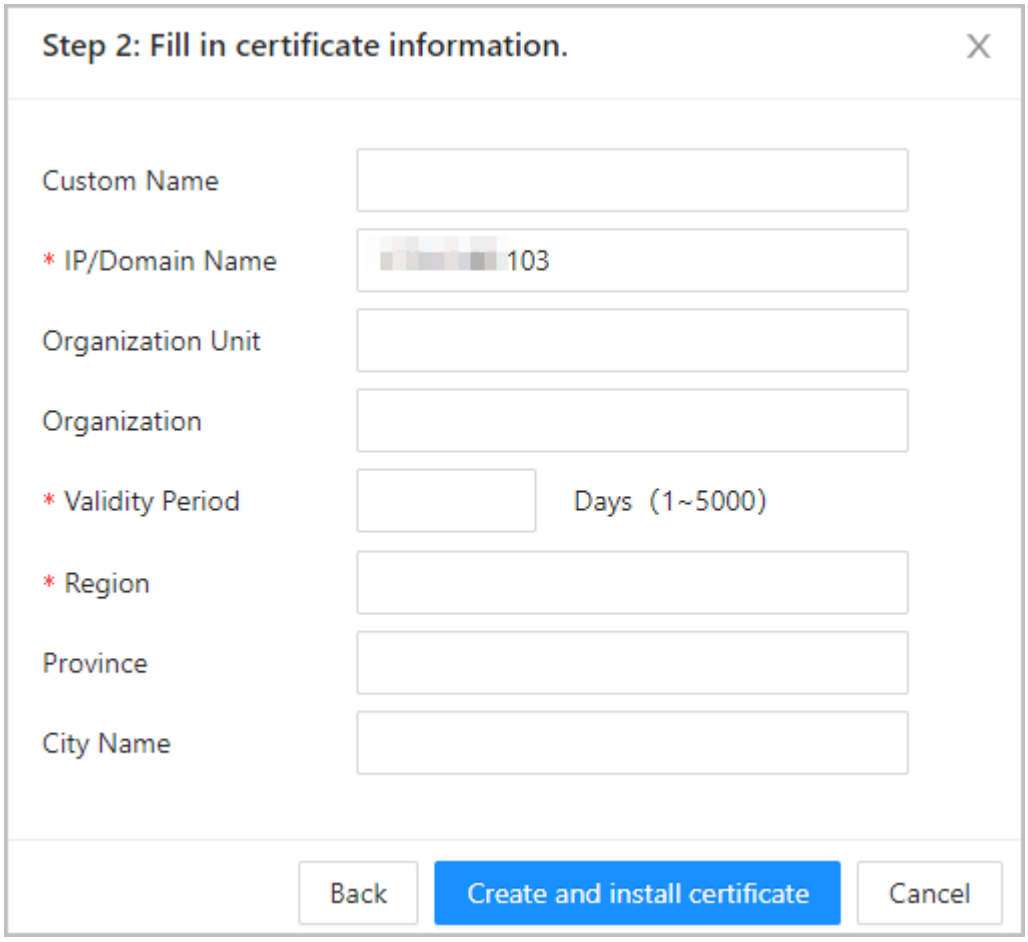
Step 1 Select **Security** > **CA Certificate** > **Device Certificate**.

Step 2 Select **Install Device Certificate**.

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

Step 4 Enter the certificate information.

Figure 2-46 Certificate information



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

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

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

Related Operations

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

2.10.4.2 Applying for and Importing CA Certificate

Import the third-party CA certificate to the Device.

Procedure

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

Step 2 Click **Install Device Certificate**.

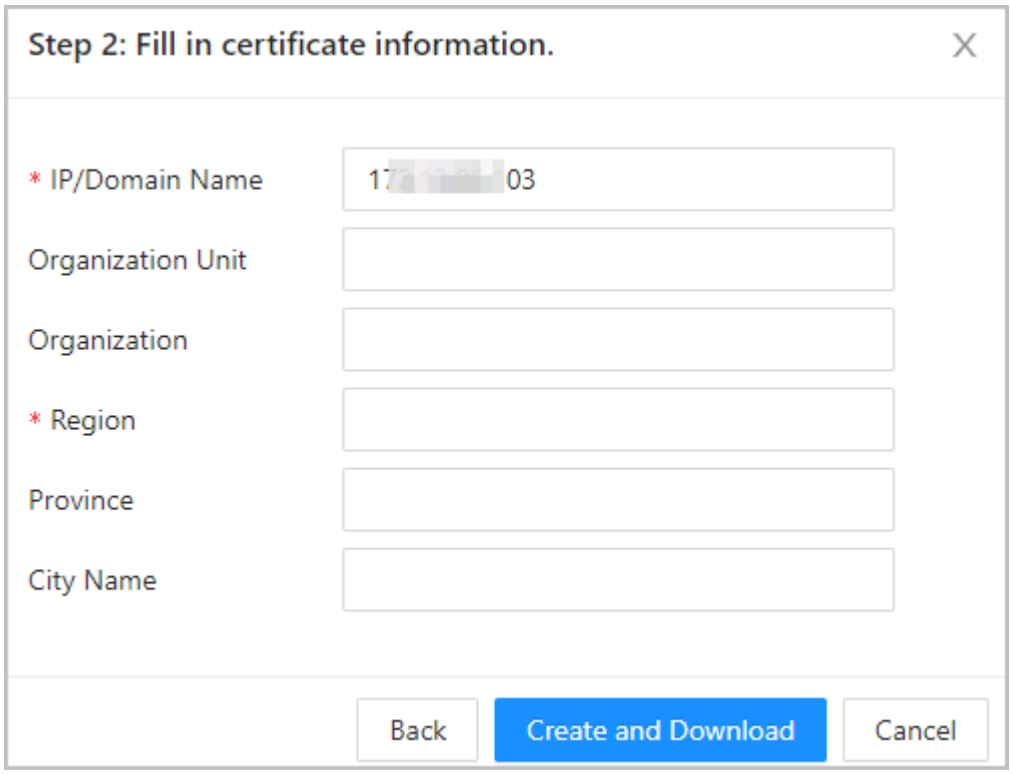
Step 3 Select **Apply for CA Certificate and Import (Recommended)** , and click **Next**.

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 2-47 Certificate information (2)



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.

2.10.4.3 Installing Existing Certificate

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

Procedure

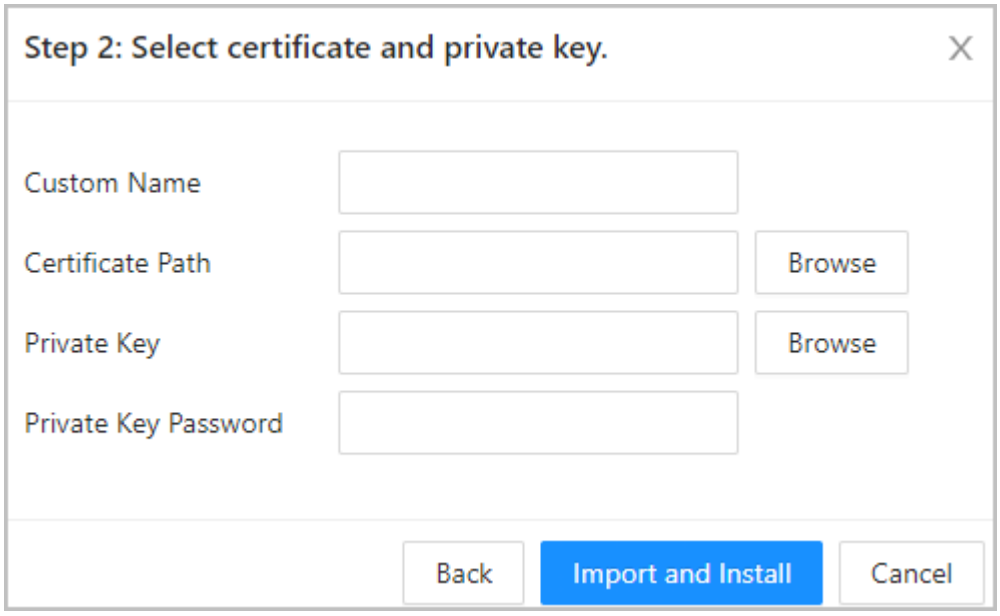
Step 1 Select **Security** > **CA Certificate** > **Device Certificate**.

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 2-48 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.

2.10.5 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.

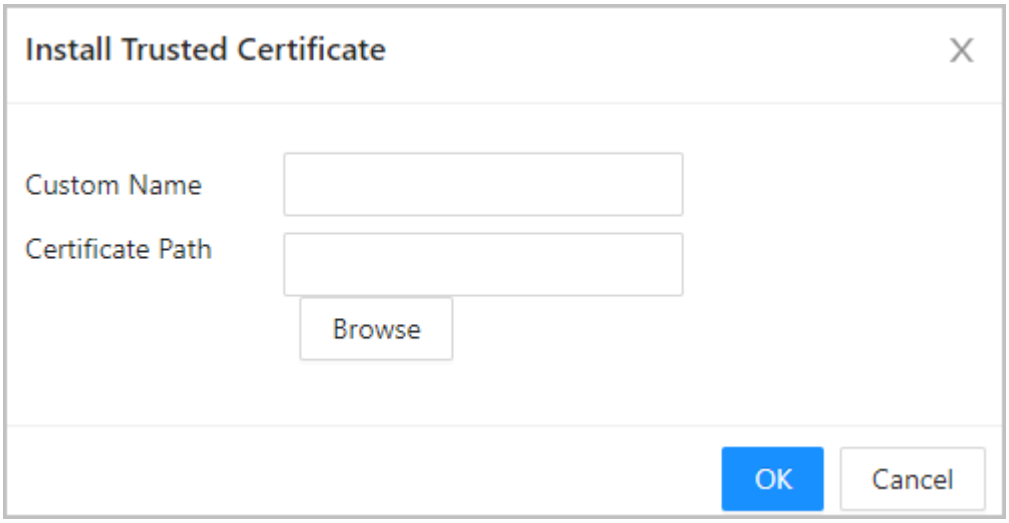
Procedure

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

Step 2 Select **Install Trusted Certificate**.

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

Figure 2-49 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.

2.10.6 Security Warning

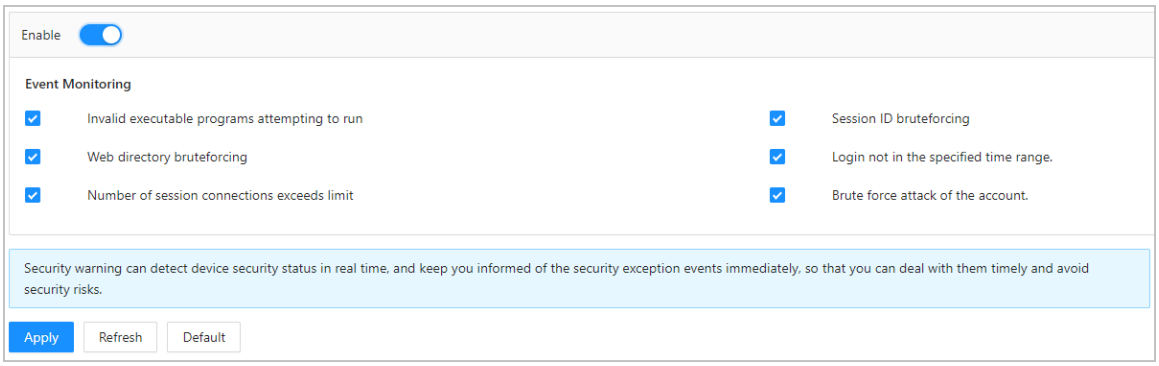
Procedure

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

Step 2 Enable the security warning function.

Step 3 Select the monitoring items.

Figure 2-50 Security warning



Step 4 Click **Apply**.

2.10.7 Security Authentication

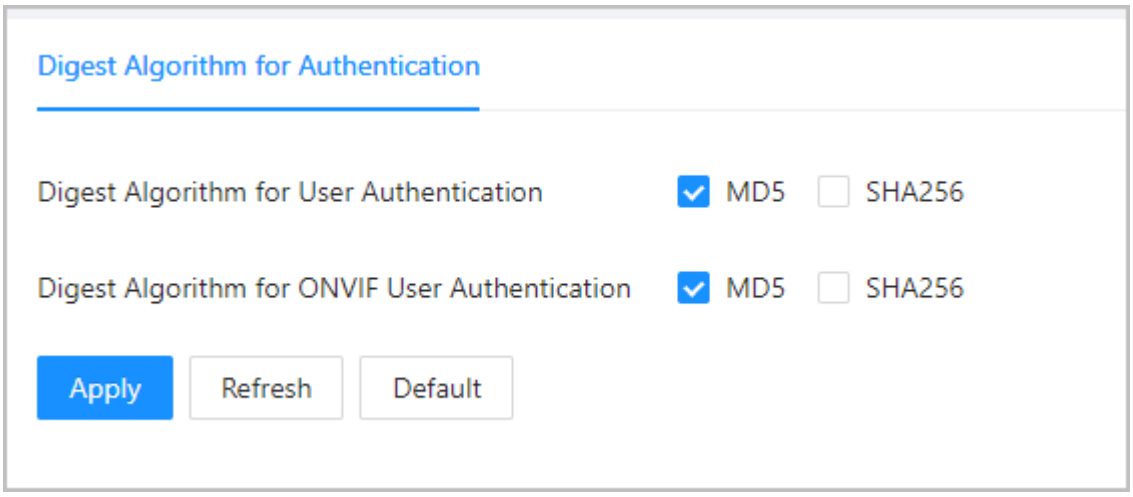
Procedure

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

Step 2 Select a message digest algorithm.

Step 3 Click **Apply**.

Figure 2-51 Security Authentication



2.11 Maintenance Center

2.11.1 One-click Diagnosis

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

Procedure

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

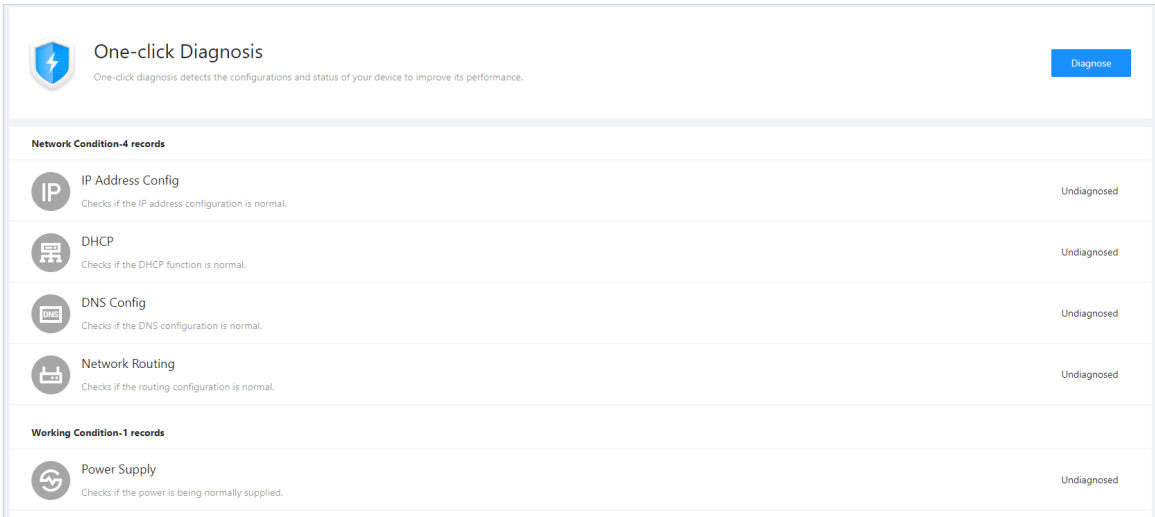
Step 2 Click **Diagnose**.

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

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

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

Figure 2-52 One-click diagnosis



2.11.2 System Information

2.11.2.1 Viewing Version Information

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

2.11.2.2 Viewing Legal Information

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

2.11.3 Data Capacity

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

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

2.11.4 Viewing Logs

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

2.11.4.1 System Logs

View and search for system logs.

Procedure

Step 1 Log in to the webpage.

Step 2 Select **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.

2.11.4.2 Unlock Records

Search for unlock records and export them.

Procedure

Step 1 Log in to the webpage.

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

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

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

2.11.4.3 Alarm Logs

View alarm logs.

Procedure

Step 1 Log in to the webpage.

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

Step 3 Select the type and the time range.

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

2.11.5 Maintenance Management

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

2.11.5.1 Exporting and Importing Configuration Files

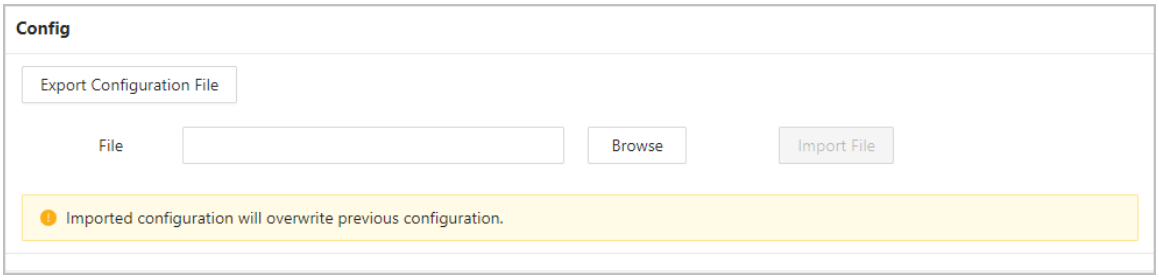
You can import and export the configuration file for the Device. When you want to apply the same configurations to multiple devices, you can import the configuration file to them.

Procedure

Step 1 Log in to the webpage.

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

Figure 2-53 Configuration management



Step 3 Export or import configuration files.

- Export the configuration file.

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

The IP will not be exported.

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

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

2.11.5.2 Configuring the Card Reader

Procedure

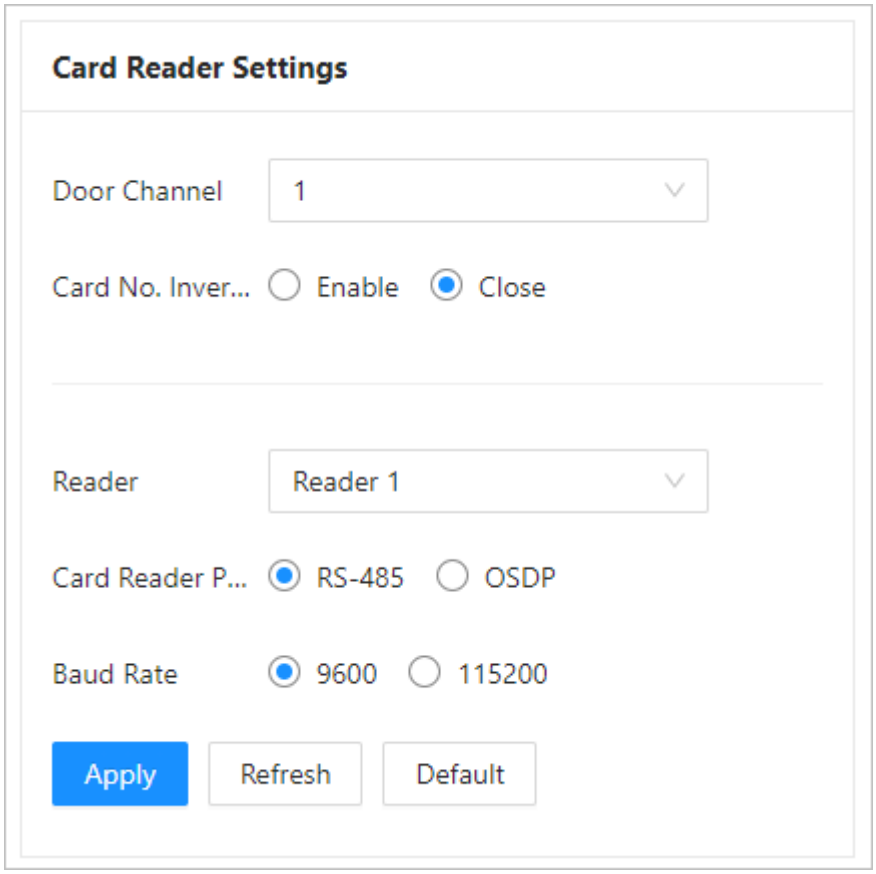
Step 1 Log in to the webpage.

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

Step 3 In the **Card Reader Settings** area, configure the card reader parameters, and then click **Apply**.

1. Select the door channel, and then enable or close **Card No. Inversion**.
2. Select the reader device, and then select the protocol and the baud rate.

Figure 2-54 Card reader settings



2.11.5.3 Configuring RS-485 Expansion

Procedure

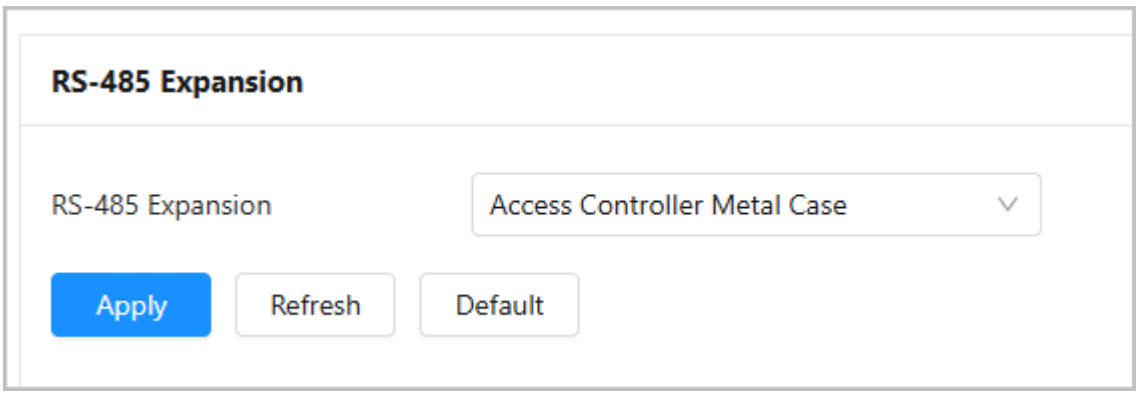
Step 1 Log in to the webpage.

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

Step 3 In the **RS-485 Expansion** area, select the RS-485 that connects to the access controller.

You can select from **Access Controller Metal Case** and **Alarm Expansion Module**

Figure 2-55 RS-485 settings



2.11.5.4 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

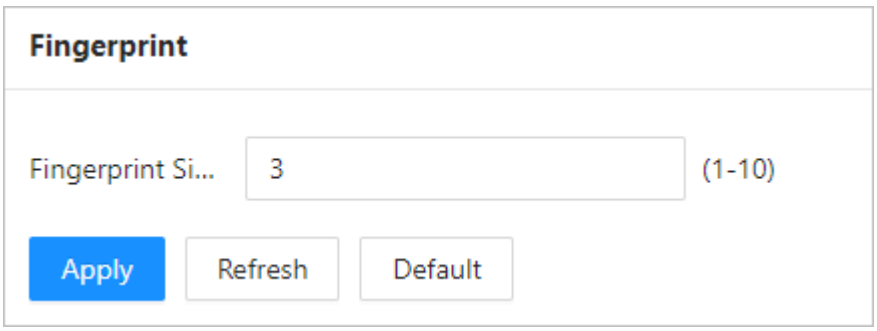
Step 1 Log in to the webpage.

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

Step 3 In the **Fingerprint** area, 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 2-56 Fingerprint similarity threshold



2.11.5.5 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.

2.11.5.6 Maintenance

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

Procedure

Step 1 Log in to the webpage.

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

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

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

2.11.6 Updating the System



- Use the correct update file. Make sure that you get the correct update file from technical support.
- Do not disconnect the power supply or network, and do not restart or shutdown the Device during the update.

2.11.6.1 File Update

Procedure

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

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



The update file should be a .bin file.

Step 3 Click **Update**.

The Device will restart after the update finishes.

2.11.6.2 Online Update

Procedure

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

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

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

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

2.11.7 Advanced Maintenance

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

2.11.7.1 Exporting

Procedure

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

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

2.11.7.2 Packet Capture

Packet Capture

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

Figure 2-57 Packet Capture



2. Enter the IP address, click .

   changes to .

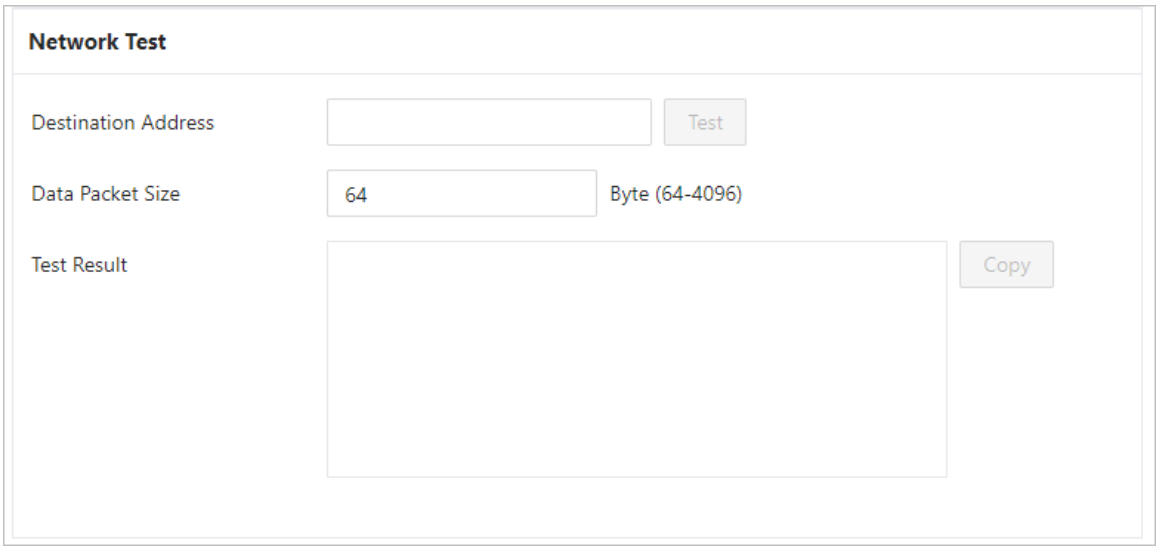
3. After you acquired enough data, click .

   Captured packets are automatically downloaded to your local computer.

Network Test

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

Figure 2-58 Network test



3. Click **Test**.

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

Appendix 1 Important Points of Fingerprint Registration Instructions

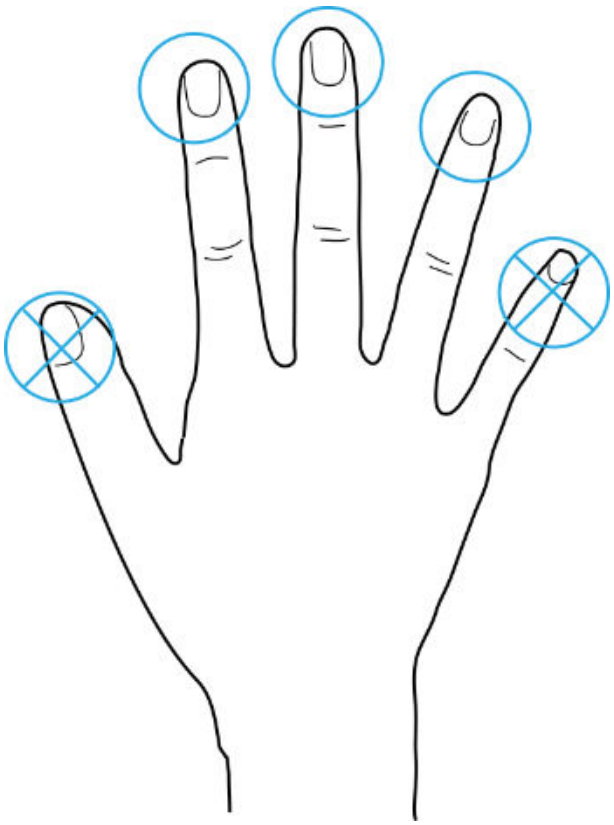
When you register the fingerprint, pay attention to the following points:

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

Fingers Recommended

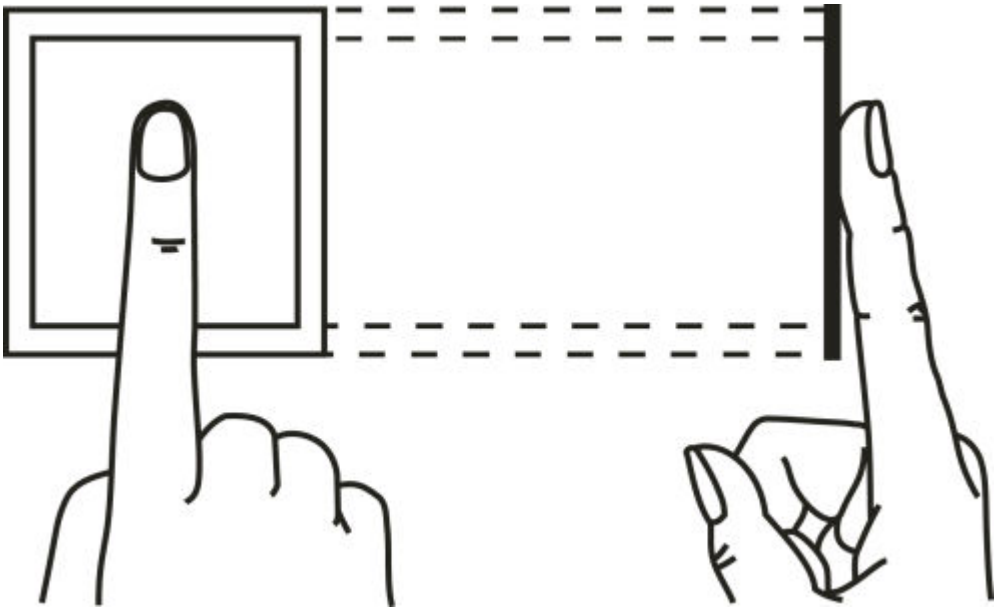
Forefingers, middle fingers, and ring fingers are recommended. Thumbs and little fingers cannot be put at the recording center easily.

Appendix Figure 1-1 Recommended fingers

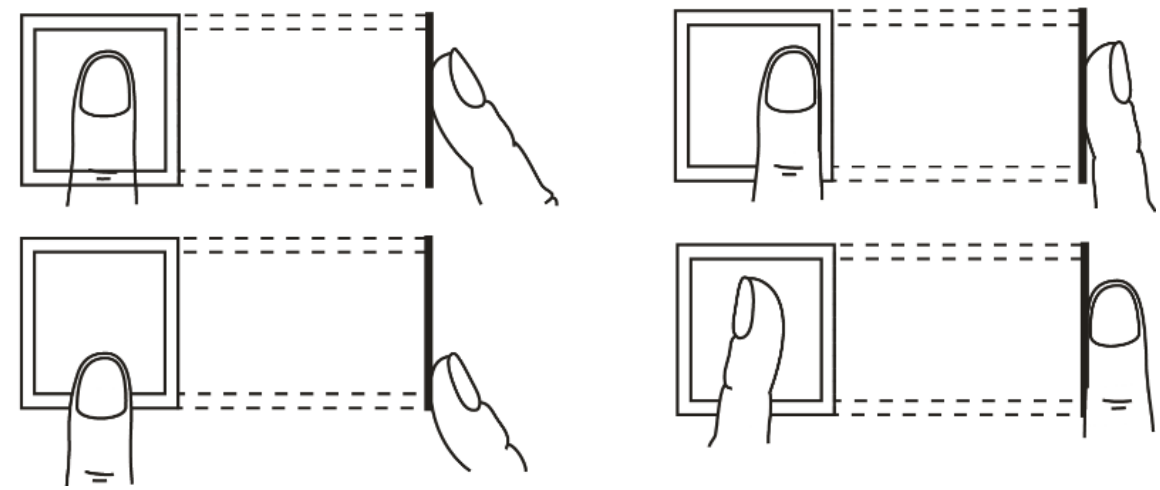


How to Press Your Fingerprint on the Scanner

Appendix Figure 1-2 Correct placement



Appendix Figure 1-3 Wrong placement



Appendix 2 Security Recommendation

Account Management

1. **Use complex passwords**

   Please refer to the following suggestions to set passwords:

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

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

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

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

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

Service Configuration

1. **Enable HTTPS**

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

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

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

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

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

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

Network Configuration

1. **Enable Allowlist**

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

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

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

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

Security Auditing

1. **Check online users**

   It is recommended to check online users regularly to identify illegal users.
2. **Check device log**

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

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

Software Security

1. **Update firmware in time**

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

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

Physical Protection

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

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