Face Recognition Access Controller

User Manual

V1.0.0

Foreword

General

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

Safety Instructions

The following signal words might appear in the manual.

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

Revision History

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

Privacy Protection Notice

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

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user manual, use our CD-ROM, scan the QR code or visit

our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.

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

Important Safeguards and Warnings

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

Transportation Requirement

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

Storage Requirement

Store the Device under allowed humidity and temperature conditions.

Installation Requirements

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

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

- Use an adapter or cabinet power supply provided by the manufacturer.
- Use the power cords that are recommended for the region and conform to the rated power specifications.
- The Device is a class I electrical appliance. Make sure that the power supply of the Device is connected to a power socket with protective earthing.
- The device must be installed at a height of 2 meters or below.
- If the product has a metal case, we recommend you install it in an environment with a temperature lower than 40℃ (104°F) to avoid overheating and affecting your experience.

Operation Requirements

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

Table of Contents

1 Overview

The device is an access controller that supports unlocking through faces, cards, Bluetooth and their combinations. Also it can connect external password or fingerprint reader to support more authentication methods.

Based on the deep-learning algorithm, it features faster recognition and higher accuracy. It can work with management platform which meets various needs of customers.

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

2 Local Operations

2.1 Powering On

After the device is powered on, the blue light flashes slowly. Once the device being powered on successfully, the green light stays on for 3 seconds, followed by a blue breathing light. When the device is uninitialized, the red light flashes slowly.

2.2 Unlock Methods

2.2.1 Unlocking by Cards

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

2.2.2 Unlocking by Face

Verify the identity of an individual by detecting their faces to unlock the door.

2.2.3 Unlocking by Fingerprint

Connect an external fingerprint scanner to the access controller, and then place your finger on the fingerprint scanner.

2.2.4 Unlocking by User Password

Connect an external device to the access controller, and then enter the user ID and password on the external device to unlock the door.

2.2.5 Unlocking by Bluetooth

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

The function is supported on select models.

Prepare the following things.

- The Bluetooth function has been enabled on webpage. For details, see"3.10.2 Bluetooth Settings".
- The device has been added to the DMSS app. For details, see the corresponding user manual.

Unlock the door through the DMSS app.

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

2.2.6 Unlocking by QR Code

Use the QR code to unlock the door.

The QR code method is available when the Device is used with the visitor module of DSS.

2.3 Restoring to Factory Defaults

Within 5 minutes of the device starting up, press the tamper switch five times consecutively within 8 seconds. The indicator lights up green, and then press and hold the tamper switch for more than 3 seconds to restore the device to factory defaults.

3 Web Operations

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

Web configurations differ depending on models of the Device.

3.1 Initialization

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

Prerequisites

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

Procedure

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

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

Step 2 Select a language on Device.

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

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

3.2 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**.

3.3 Resetting the Password

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

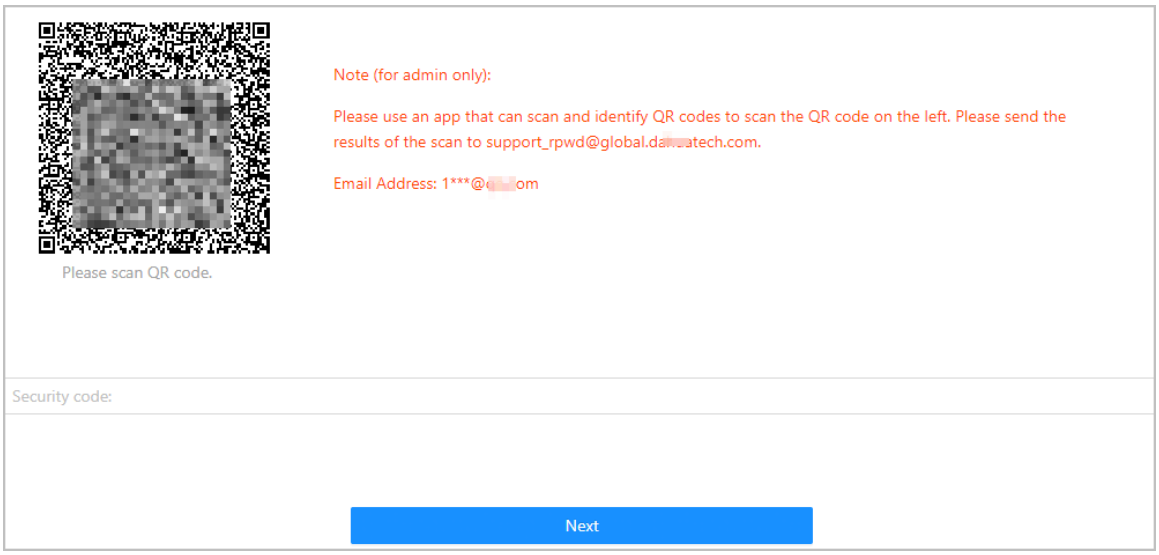
Procedure

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

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

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

Figure 3-1 Reset password



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

Step 4 Enter the security code.

Step 5 Click **Next**.

Step 6 Reset and confirm the password.

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

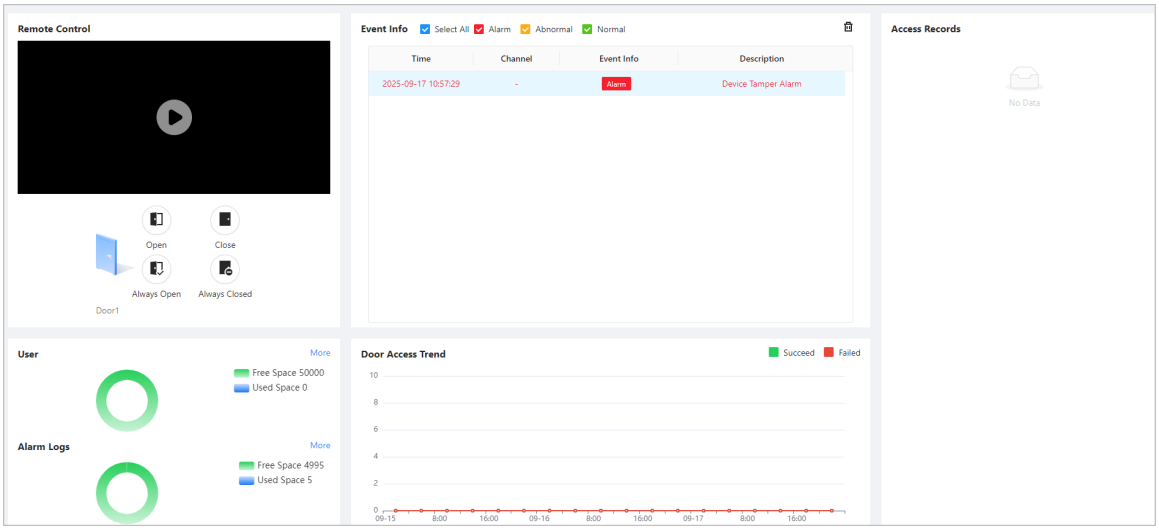
Step 7 Click **OK**.

3.4 Access Monitoring

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

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

Figure 3-2 Access monitoring



Remote Control

- Click **Open** or **Close** next to the door to remotely control the door.
- Click **Always Open** or **Always Closed** to remotely control the door. Click **Restore** to restore the door to normal status.
- Click  to preview the screen image and perform related operations.

Table 3-1 Description of remote control screen icons

Icons	Description
	Take the snapshot.
	Start to record the video.
	Turn on the sound of the video.
	Turn on the intercom function.
	Zoom in the image.

Door Access Trend

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

Access Records

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

Event Information

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

User and Alarm Logs

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

3.5 Home Page

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

Figure 3-3 Home page

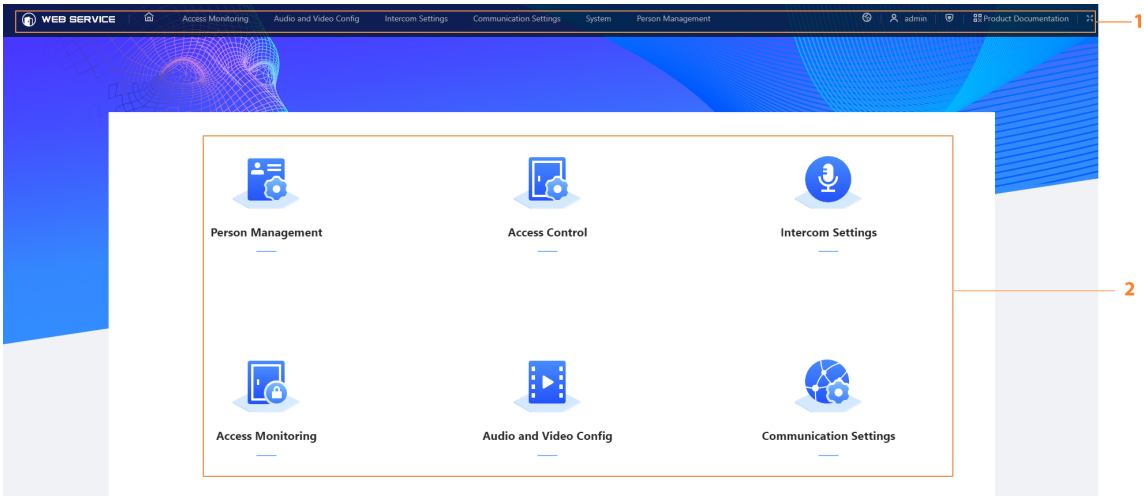


Table 3-2 Home page description

No.	Description
1	Main menu.

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

3.6 Person Management

Procedure

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

Step 2 Configure user information.

Figure 3-4 Basic information

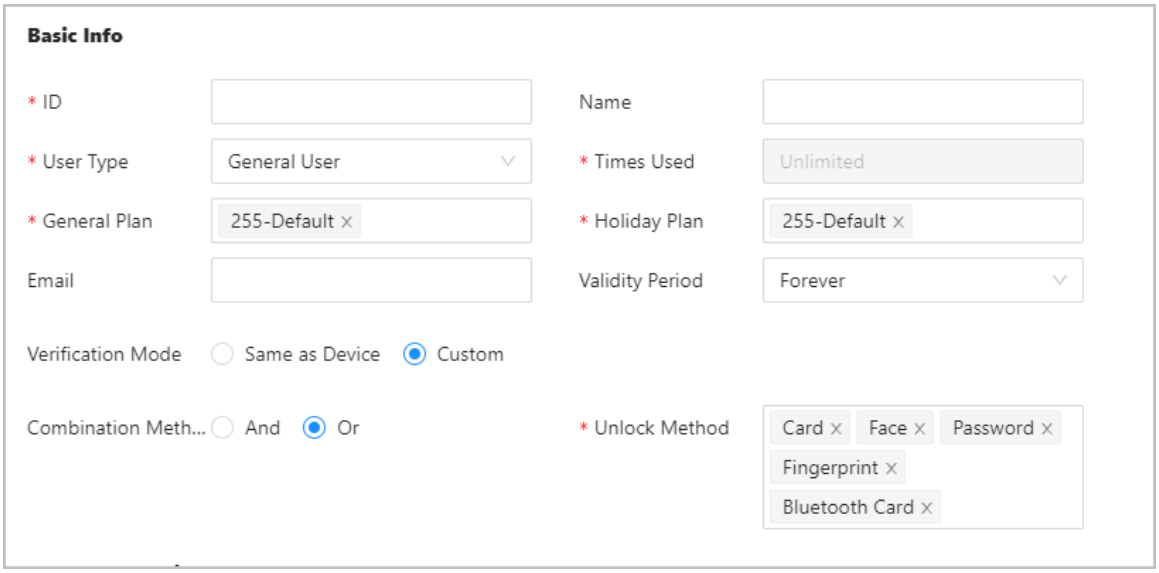


Table 3-3 Description of basic information

Parameter	Description
ID	The user ID is like employee ID, which can be numbers, letters, and their combinations, and the maximum length of the number is 30 characters.
Name	The name can contain up to 32 characters (including numbers, symbols, and letters).
Validity Period	Select from **Forever** and **Custom**. If you select **Custom**, you need to set a date on which the door access permissions of the person will be expired.

Parameter	Description
User Type	• **General User** : General users can unlock the door. • **Blocklist User** : When users in the blocklist unlock the door, service personnel will receive a notification. • **Guest User** : Guests can unlock the door within a defined period or for certain amount of times. After the defined period expires or the unlocking times runs out, they cannot unlock the door. • **Patrol User** : Patrol users do not have door permissions. • **VIP User** : When VIP unlock the door, service personnel will receive a notice. • **Other User** : When they unlock the door, the door will stay unlocked for 5 more seconds. • **Custom User 1** /**Custom User 2**: Same as general users.
Times Used	Set an unlock limit for guest users. After the unlock times run out, they cannot unlock the door.
General Plan	People can unlock the door during the defined period.  You can select more than one plan.
Holiday Plan	People can unlock the door during the defined holiday.  You can select more than one holiday.
Verification Mode	Configure the verification mode for the person. You can use the mode that is the same as the device or customize the mode. • **Same as Device** : The mode is the same as the device. • **Custom** : After you select **Custom**, **Combination Method** and **Unlock Method** are displayed. Select the combination method and unlock methods as needed. ◇ Or: Use one of the selected unlock methods to open the door. ◇ And: Use all the selected unlock methods to open the door.  ◇ The customized verification mode is only valid for the local device. It cannot be used in external card readers. ◇ When the customized verification mode is different from the mode of the device, the customized mode takes the priority.
Unlock Method	Select the method(s) according to your needs.

Figure 3-5 Access credentials

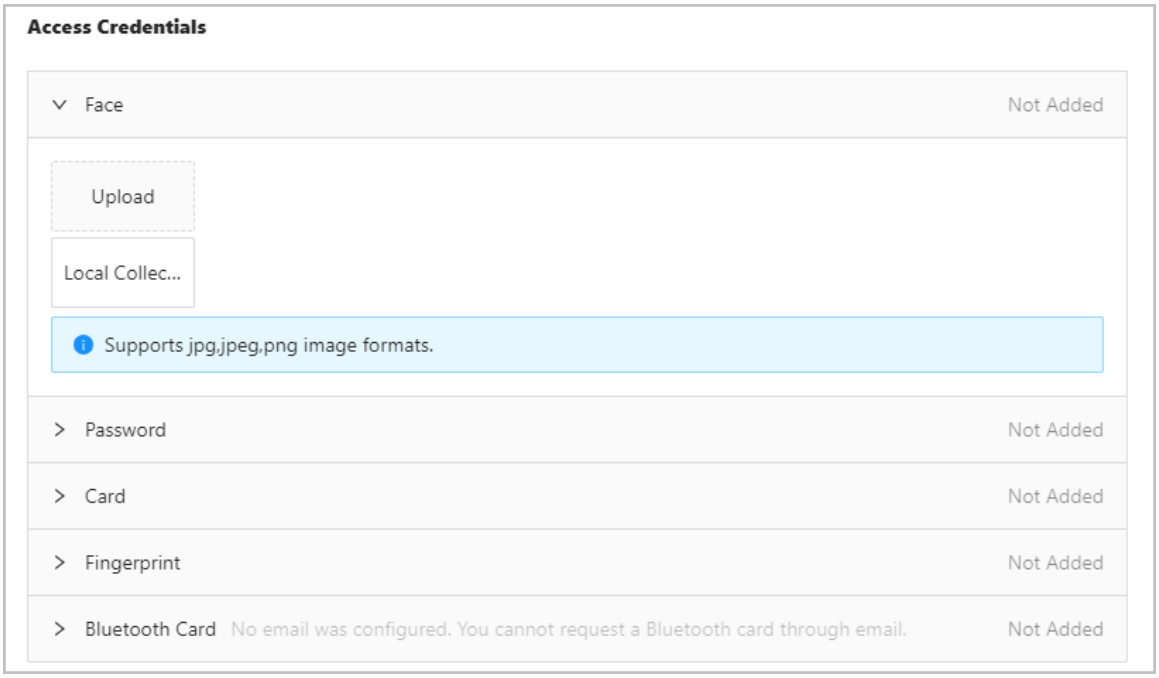


Table 3-4 Description of access credentials

Parameter	Description
Face	• Upload: Click **Upload** to upload a face image. Each person can only add up to 2 face images. You can view or delete the face image after you upload it. • Local collection: Use the camera of the device or the USB camera to collect the face images. You can view or delete the face image after you take the snapshot. 1. Click **Local Collection**. 2. Click **Modify** to select the acquisition device. 3. Click **Start Snapshot** to collect the face image. 4. Click **Add**.
Password	You need to connect an externally device that can enter password. Enter the user password. The maximum length of the password is 8 digits. The duress password is the unlock password + 1. For example, if the user password is 12345, the duress password will be 12346. A duress alarm will be triggered when a duress password is used to unlock the door.

Parameter	Description
Card	• Enter the card number manually. 1. Click **Add**. 2. Enter the card number, and then click **Add**. • Read the number automatically through the enrollment reader or the Device. 1. Click **Add** , and then click **Modify** to select an enrollment reader or the Device. 2. Read the card. ◇ For the enrollment reader of IC and ID card, Click **Read Card**, and then swipe cards on the card reader. A 60-second countdown is displayed to remind you to swipe cards, and the system will read the card number automatically. If the 60-second countdown expires, click **Read Card** again to start a new countdown. ◇ For the enrollment reader of the Desfire card, place the card on the enrollment reader, and then click **Read Card**. If the Desfire card has been written with the card number, it will be read and displayed here. If the card is empty, then the card number needs to be written first. The card number will be automatically generated on the computer, and be written to the card. 3. Click **Add**. A user can register up to 5 cards at most. Enter your card number or swipe your card, and then the card information will be read by the Device. You can enable the **Duress Card** function. An alarm will be triggered if a duress card is used to unlock the door. • : Set duress card. • : Change card number. One user can only set one duress card.
Fingerprint	Register fingerprints. A user can register up to 3 fingerprints, and you can set a fingerprint to the duress fingerprint. An alarm will be triggered when the duress fingerprint is used to unlock the door. Enroll fingerprints through an enrollment reader. 1. Click **Add** , and then click **Modify** to select an enrollment reader or the Device. 2. Press finger on the scanner according to the on-screen instructions. 3. Click **Add**. • We do not recommend you set the first fingerprint as the duress fingerprint. • One user can only sets one duress fingerprint. • Fingerprint function is available if the Device supports connecting a fingerprint module.

Parameter	Description
Bluetooth Card	You can select **Request through Email** or **Request through Registration Code**. • **Request through Email** : Suitable for the first time a Bluetooth card is requested. You can request up to 5 Bluetooth cards, and have to use the email that is registered to DMSS. You must have entered your reserved Email before you use the function. 1. Configure the Email that is registered to DMSS. 2. Click **Request through Email**, and then the Bluetooth cards can be requested. • **Request through Registration Code** : Suitable when you already have a Bluetooth card and want to reuse it on another access controller supporting Bluetooth function. 1. Copy the Bluetooth registration code from the DMSS. 2. Click **Request through Registration Code**, and then enter the code. 3. Click **OK**.

Step 3 Click **Add**.

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

Related Operations

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

  Select users and then click **Issue Cards to Selected Users** or click **Issue Cards to All Users**.

  - ◇ On **Requestable** tab, you can view all users who can be issued Bluetooth cards, and then click **Request through Email** to issue Bluetooth card in batches.

    ○ Bluetooth cards can only be generated in batches through emails.
    ○ Cloud service should be online.
  - ◇ On **Non-Requestable** tab, you can view users without Email who cannot be issued cards.
    - ○ Click **Export Users that Lack Emails** to download the user list on the local compute, and then enter the Email.
    - ○ Click **Import** to import the user list so that you can issue card to them.
- Click **Bluetooth Cards Records**, and then you can view the Bluetooth card records. For users who issued cards unsuccessfully, you can reissue cards here.

3.7 Configuring Intercom

The Device can function as a door station to realize video intercom.

The intercom function is only available on select models.

3.7.1 Using the Device as the SIP Server

3.7.1.1 Configuring SIP Server

When the Device functions as the SIP server, it can connect up to 500 VTHs.

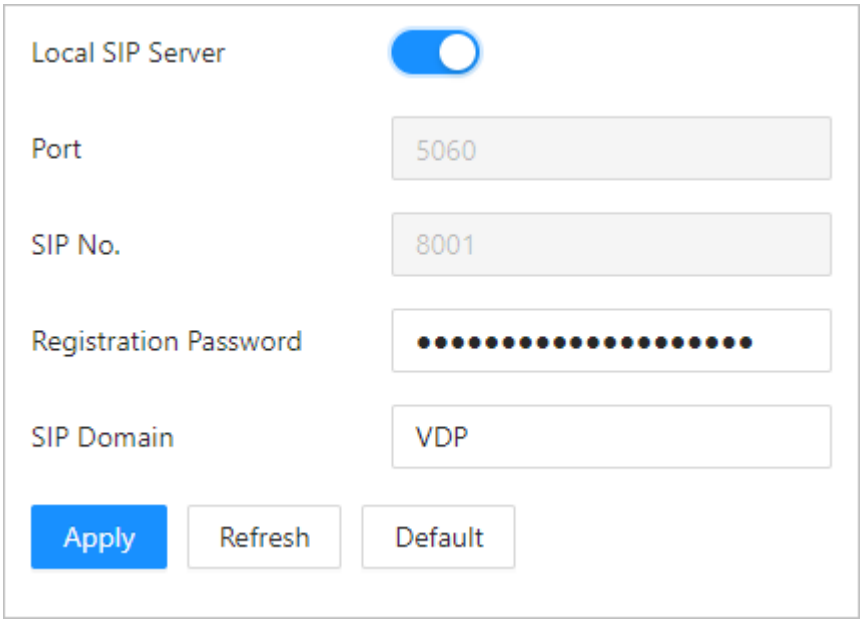
Procedure

Step 1 Select **Intercom Settings** > **SIP Server**.

Step 2 Turn on **SIP Server**.

The device settings will be automatically restored to factory defaults if the SIP server status changes.

Figure 3-6 SIP server



Step 3 Click **Apply**.

3.7.1.2 Configuring Local Parameters

When the Device functions as the SIP server, configure the parameters of the Device.

Procedure

Step 1 Select **Intercom Settings** > **Local Device Config**.

Step 2 Configure the parameters.

Figure 3-7 Basic parameters

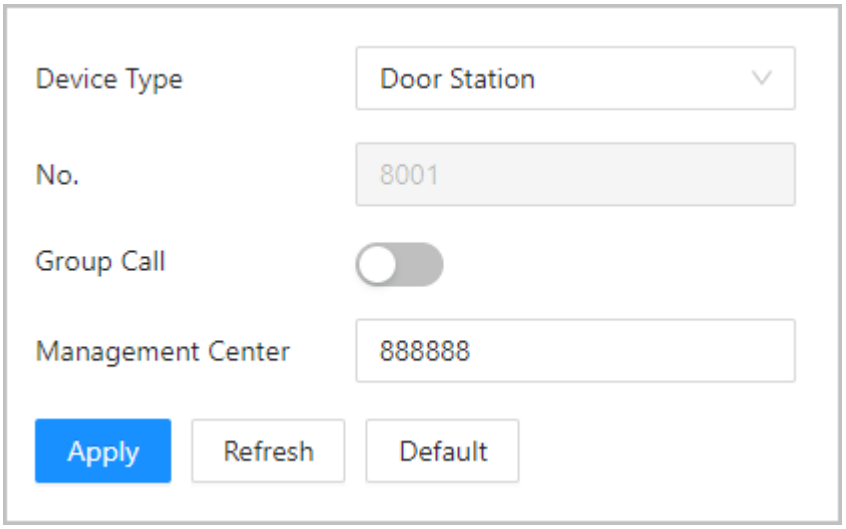


Table 3-5 Basic parameters description

Parameter	Description
Device Type	Select **Door Station**.
No.	Cannot be set.
Group Call	When you turn on the group call function, the door station calls the main VTH and the extensions at the same time. The setup is effective after the door station restarts.
Management Center	The default call number of the management center is 888888+VTS No. For the VTS No, go to the **Project Setting** > **General** of the management center.

Step 3 Click **Apply**.

3.7.1.3 Adding the VTO

When the Device functions as the SIP Server, you need to add door station to the SIP server to make sure they can call each other.

Procedure

Step 1 On the webpage of the Device, select **Intercom Settings** > **Device Setting**.

Step 2 Click **Add**, and then configure the door station.

Figure 3-8 Add VTO

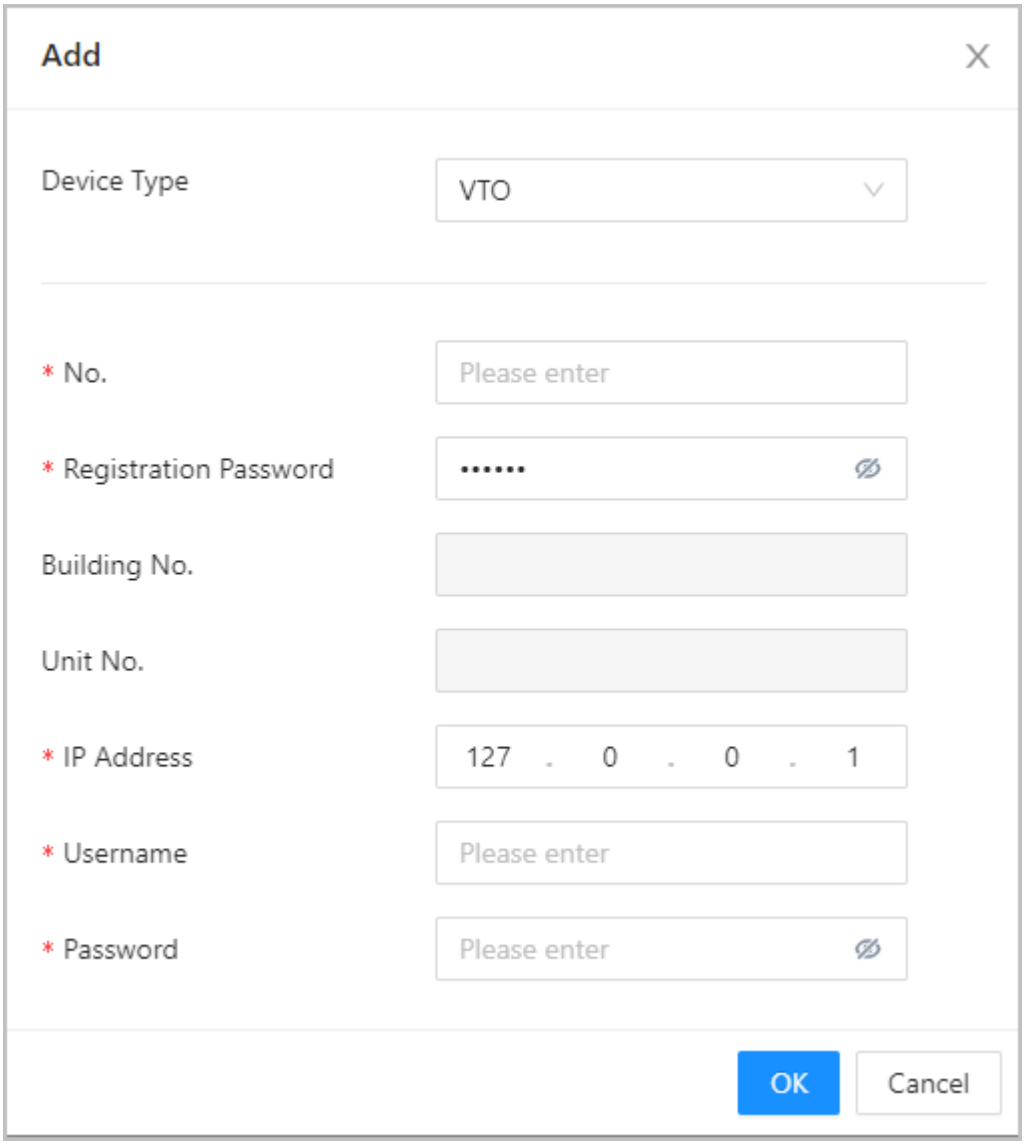


Table 3-6 Add VTO configuration

Parameter	Description
Device Type	Select **VTO**.
No.	To view the number of the door station, go to the **Device** screen of the door station, and then enter the number of door station on this page.
Registration Password	Keep it default.
Building No.	Cannot be configured.
Unit No.	
IP Address	The IP address of the added door station.
Username	The user name and password that are used to log in to the webpage of the added door station.
Password	

Step 3 Click **OK**.

3.7.1.4 Adding the VTH

When the Device functions as the SIP Server, you can add all VTHs in the same unit to the SIP server to make sure that they can call each other.

Background Information

- When there are main VTH and extension, you need to turn on the group call function first, and then add main VTH and extension on the **VTH Management** page.
- Extension cannot be added when the main VTHs are not added.

Procedure

Step 1 On the home page, select **Intercom Settings** > **Device Setting**.

Step 2 Add the VTH.

- Add one by one.
  1. Click **Add**.
  2. Configure parameters, and then click **OK**.

Figure 3-9 Add one by one

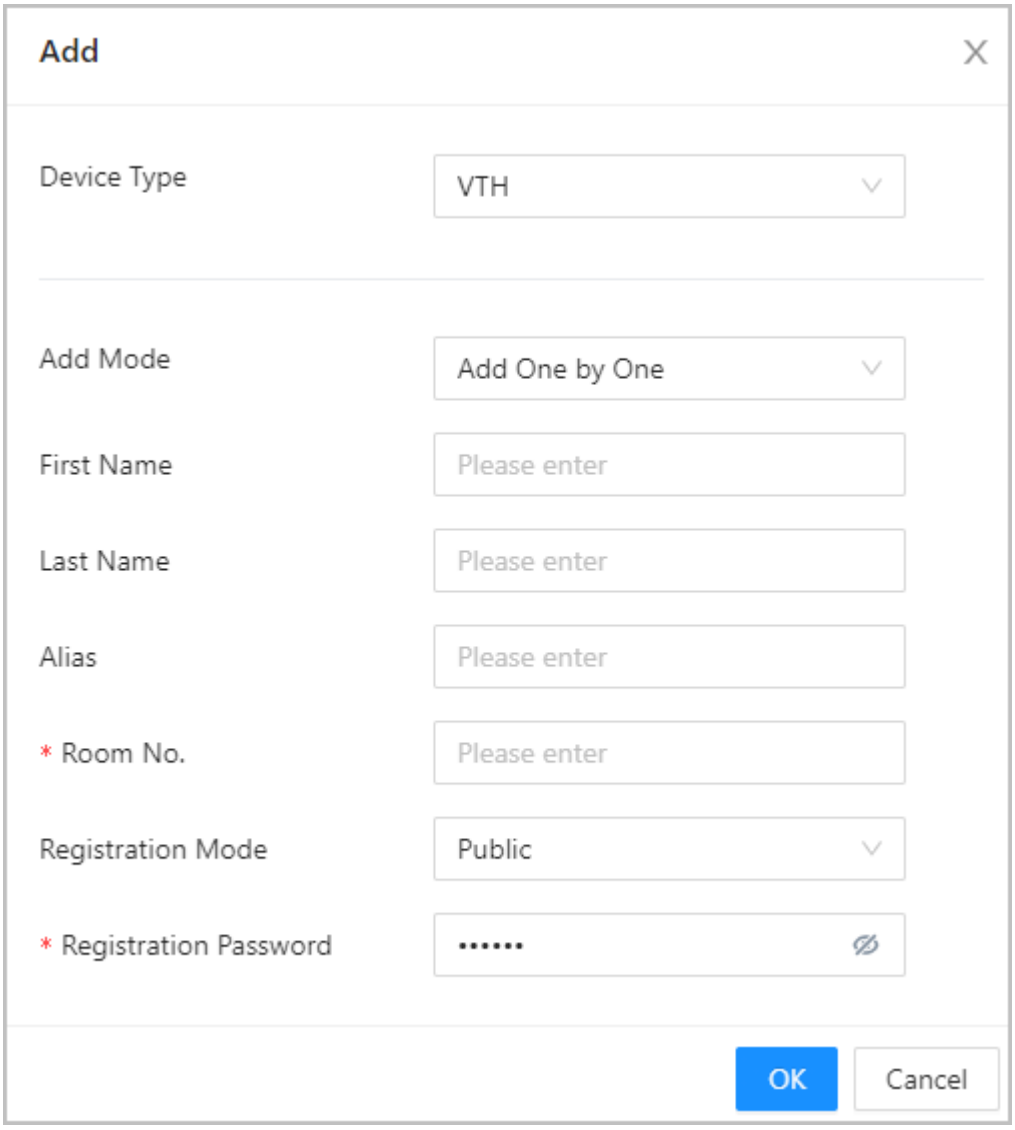


Table 3-7 Room information

Parameter	Description
First Name	Enter the name of the VTH to help you differentiate VTHs.
Last Name	
Alias	
Room No.	Enter the room number of the VTH. ◇ The room number consists of 1-5 digits, and must conform to the configured room number on the VTH. ◇ When there are main VTH and extensions, the room number of main VTH ends with -0 and the room number of extension ends with -1, -2 or -3. For example, the main VTH is 101-0, and the room number of the extension is 101-1, 101-2... ◇ If the group call function is not turned on, room number in the format of 9901-xx cannot be set.
Registration Mode	Keep them as defaults.
Registration Password	

- Add in batches.
  1. Click **Add in Batches**.
  2. Configure the parameters.
  3. Click **Add**.

Figure 3-10 Batch add

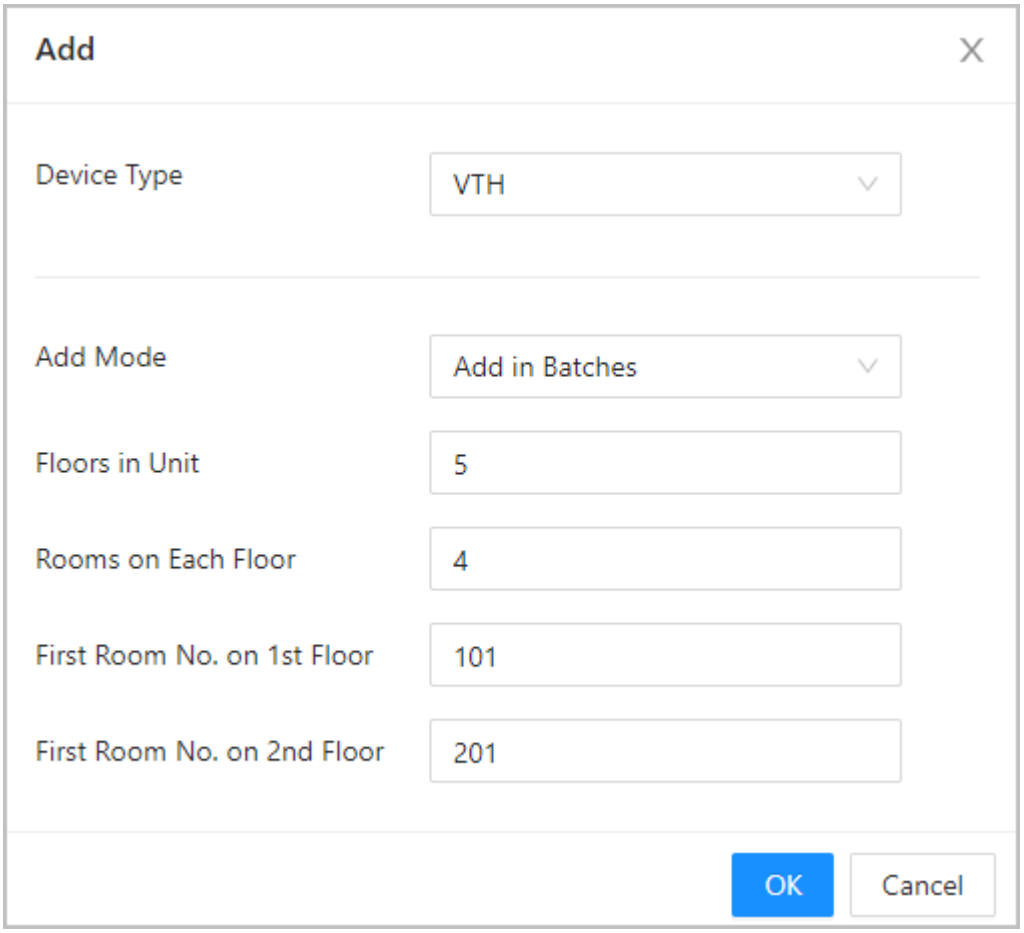


Table 3-8 Add in batches

Parameter	Description
Floors in Unit	The number of floors of the building, which ranges from 1 to 99.
Rooms on Each Floor	The number of rooms on each floor, which ranges from 1 to 99.
First Room No. on 1st Floor	The first room on the first floor.
First Room No. on 2nd Floor	The first room number on the 2nd floor = The first digit of the first room number on the 1st floor plus 1. For example, if the first room number on the first floor is 101, the first room number on the 2nd floor must be 201.

3.7.1.5 Adding the VTS

When the Device functions as the SIP Server, you can add VTSs to the SIP server to make sure that they can call each other.

Procedure

Step 1 On the Homepage, select **Intercom Settings** > **Device Setting**.

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

Figure 3-11 VTS management

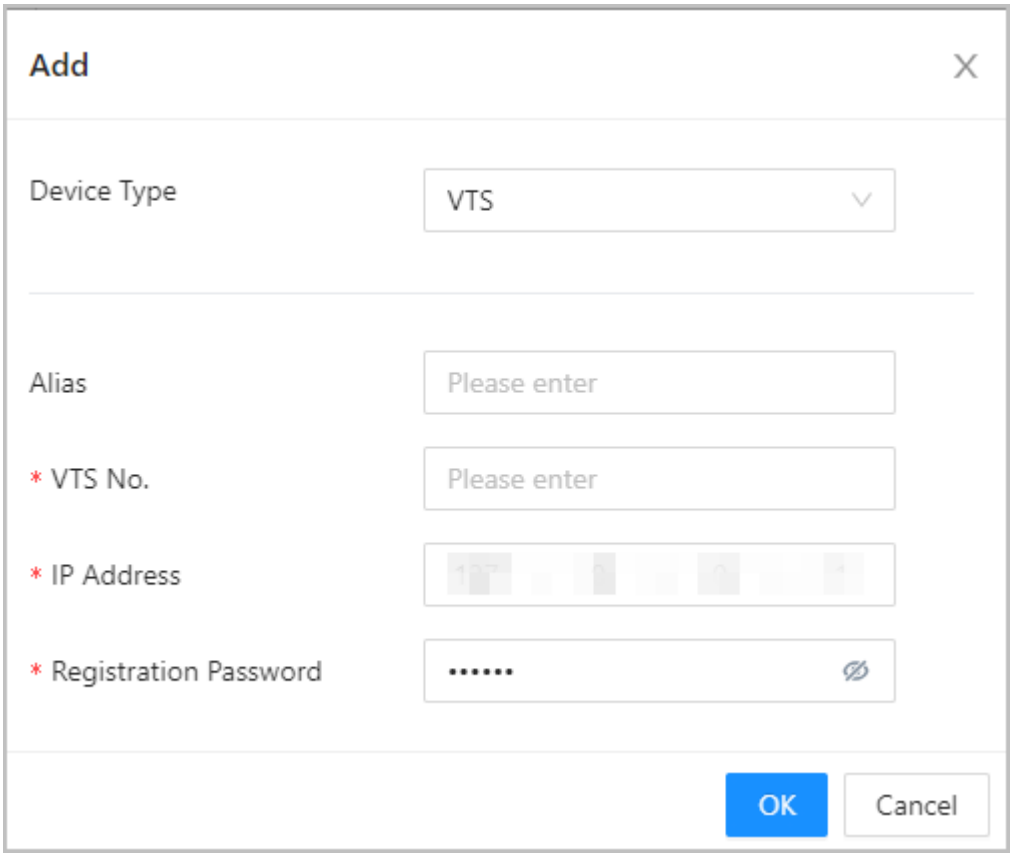


Table 3-9 VTS parameters

Parameter	Description
Alias	Enter the name of the VTS.
VTS No.	Enter 888888+ VTS No, which can include up to 9 digits. For the VTS No, go to **Device** screen on the VTS.
IP Address	The IP address of the VTS.
Registration Password	Keep it as default.

Step 3 Click **OK**.

3.7.2 Using VTO as the SIP server

3.7.2.1 Configuring SIP Server

Use another VTO as the SIP server.

Procedure

Step 1 Select **Intercom Settings** > **SIP Server**.

Step 2 Select **Device** from the **Server Type**.

Do not enable **Local SIP server**.

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

Figure 3-12 Use VTO as the SIP server

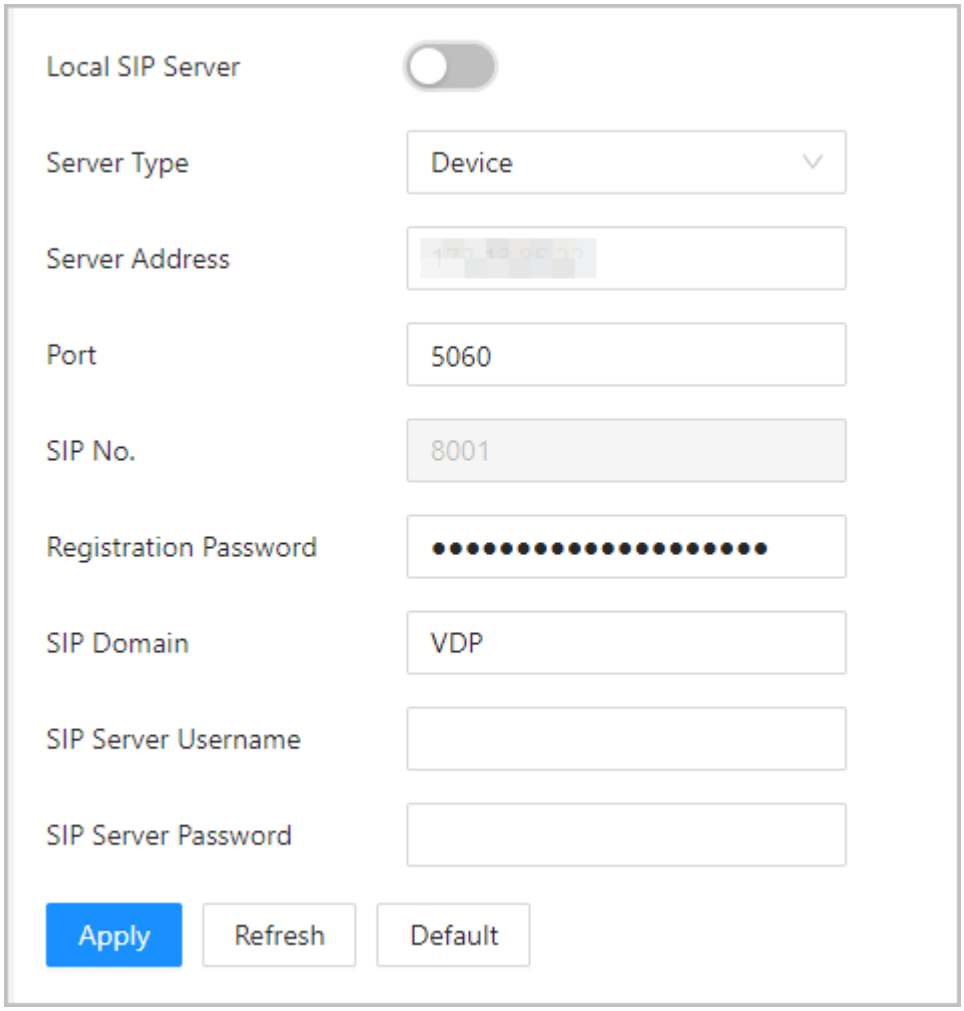


Table 3-10 SIP server configuration

Parameter	Description
Server Address	IP address or domain name of the VTO.
Port	5060 by default when VTO works as SIP server.
SIP No.	Leave them as default.
Registration Password	
SIP Domain	VDP.
SIP Server Username	The login username and password of the SIP server.
SIP Server Password	

Step 4 Click **Apply**.

3.7.2.2 Configuring Local Parameters

Configure the parameters of the Device when you use another VTO as the SIP server.

Procedure

Step 1 Select **Intercom Settings** > **Local Device Config**.

Step 2 Configure the parameters.

Figure 3-13 Configure the parameters

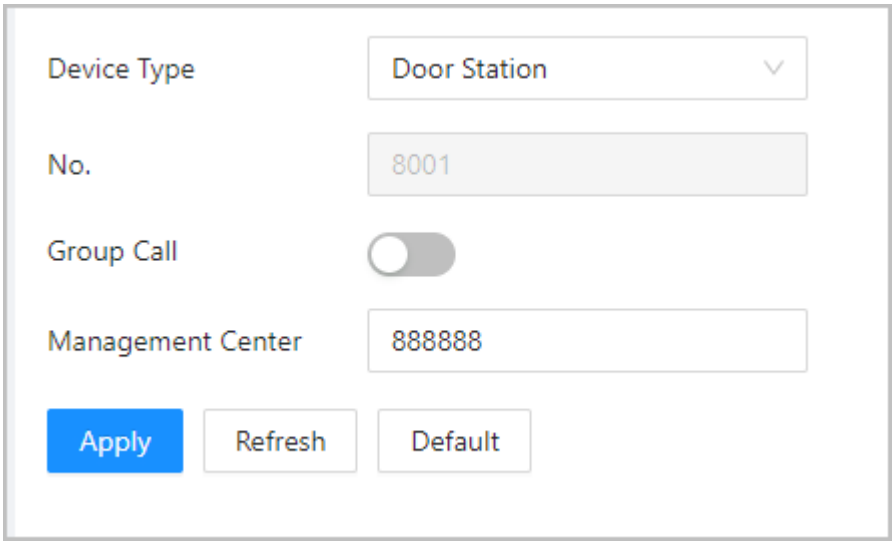


Table 3-11 Parameters description

Parameter	Description
Device Type	Select **Door Station**.
No.	The number of the VTO. ● The number must have 4 digits. The first 2 digits must be 80, and the last 2 digits start from 01. For example, 8001. ● If multiple VTOs exist in one unit, the VTO No. cannot be repeated.
Group Call	The call between door stations can be achieved.
Management Center	The call number for the management center is 888888. Keep it as default.

Step 3 Click **Apply**.

3.7.3 Using the Platform as the SIP server

3.7.3.1 Configuring SIP Server

The management platform is used as the SIP server.

Procedure

Step 1 Select **Intercom Settings** > **SIP Server**.

Step 2 Select **Private SIP Server** from the **Server Type**.

Do not enable **SIP Server**.

Figure 3-14 Alternate server

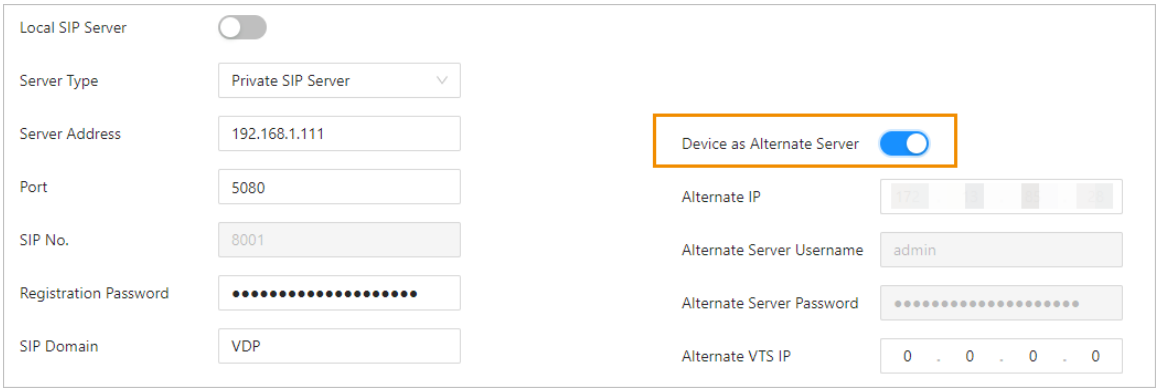


Table 3-12 SIP server configuration

Parameter	Description
Server Address	IP address of the platform.
Port	5080 by default when the platform works as SIP server.
Registration Password	Leave them as default.
SIP Domain	Leave it as default.
Alternate IP	The alternate server will be used as the SIP server when the platform does not respond. ● If you turn on the **Alternate Server** function, you will set the Device as the alternate server. ● If you want another VTO to function as the alternate server, you need to enter the IP address, username, password of the VTO. Do not enable **Alternate Server** in this case. ● We recommend you set the main VTO as the alternate server.
Alternate Server Username	After you set the alternate server, when the management platform does not respond, the alternate server will be activated to make sure VTO and VTH can each other. ● If **Alternate Server** is enabled, the Device is set as the alternate server. ● If **Alternate Server** is not enabled, enter the IP of the alternate server, its username and password to set VTO as the alternate server. We recommend you set the main VTO as the alternate server.
Alternate Server Password	
Alternate Server	
Alternate VTS IP	Enter the IP address of the alternate VTS. When the management platform does not respond, the alternate VTS will be activated to make sure VTO, VTH and VTS can each other.

Step 3 Click **Apply**.

3.7.3.2 Configuring Local Parameters

Configure the parameters of the Device when the platform is used as the SIP server.

Procedure

Step 1 Select **Intercom Settings** > **Local Device Config**.

Step 2 Configure the parameters.

Figure 3-15 Basic parameter

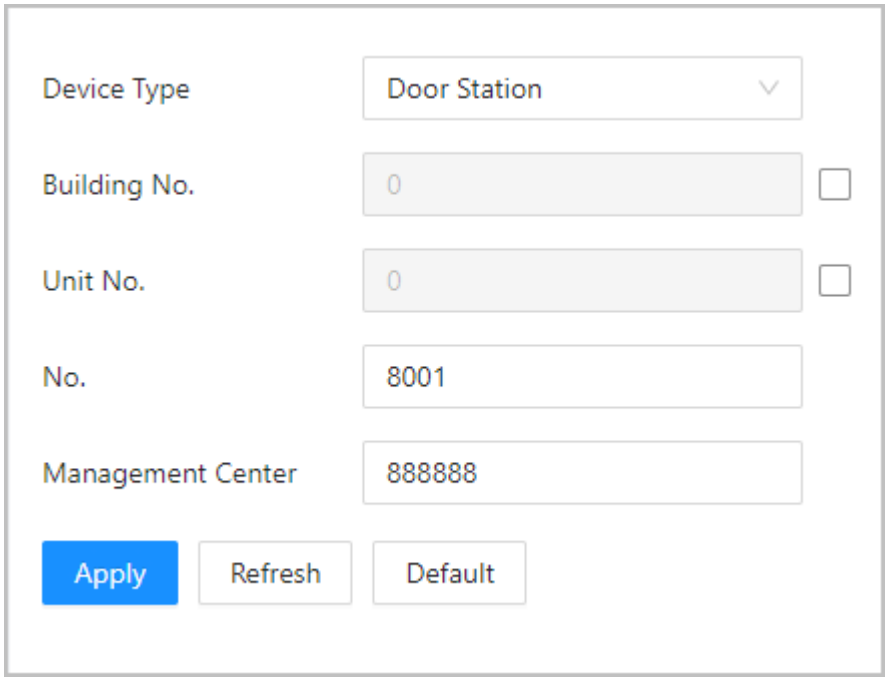


Table 3-13 Parameters description

Parameter	Description
Device Type	Select fence station or door station based on its installation site.
Building No.	Select the checkbox and then enter the number of the building where the unit door station is installed.
Unit No.	Select the checkbox, and then enter the number of the unit where the unit door station is installed.
No.	• The number must have 4 digits. The first 2 digits must be 80, and the last 2 digits start from 01. For example, 8001. • If multiple VTOs exist in one unit, the VTO No. cannot be repeated.
Management Center	The default phone number is 888888 when the VTO calls the VTS. Keep it as default.

Step 3 Click **Apply**.

After settings, the user name in **Intercom** > **SIP Server** page is automatically refreshed. Make sure the user name is same to the call number when you add the device to the management platform.

3.7.4 Configuring Call parameters

You can configure call and doorbell functions.

Procedure

Step 1 Select **Intercom Settings** > **Call Config**.

Step 2 Enable **Function Config**.

Step 3 Select **Call** or **Doorbell**, and then configure parameters.

Figure 3-16 Configure Doorbell

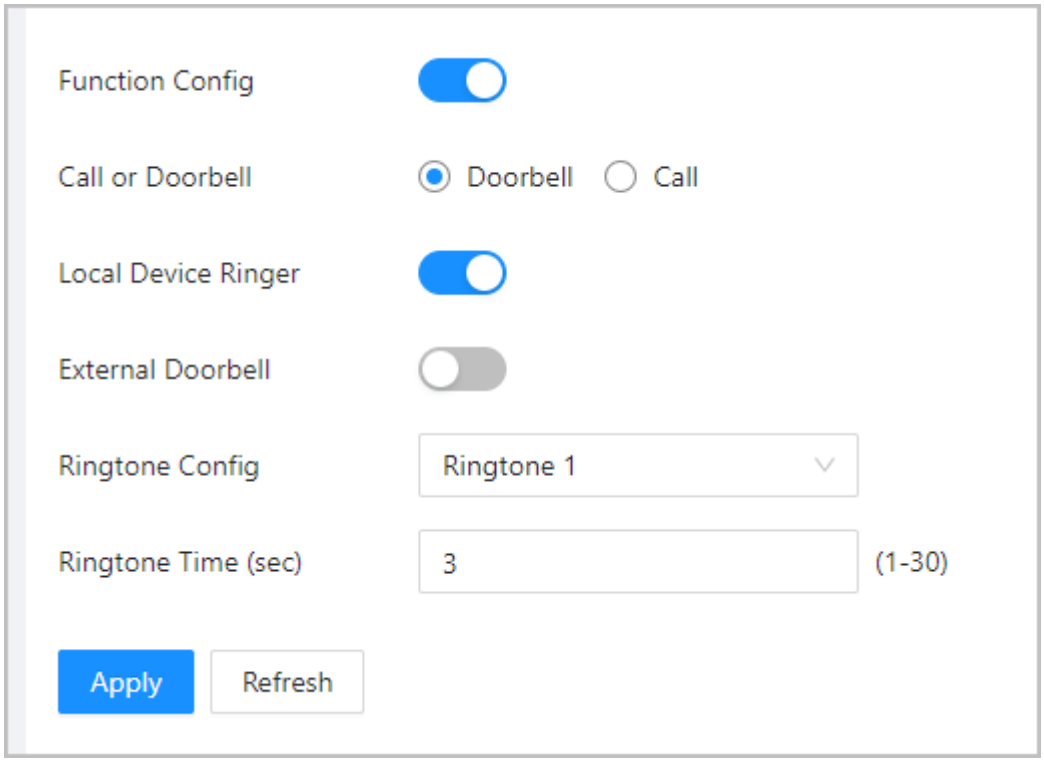


Figure 3-17 Configuring call

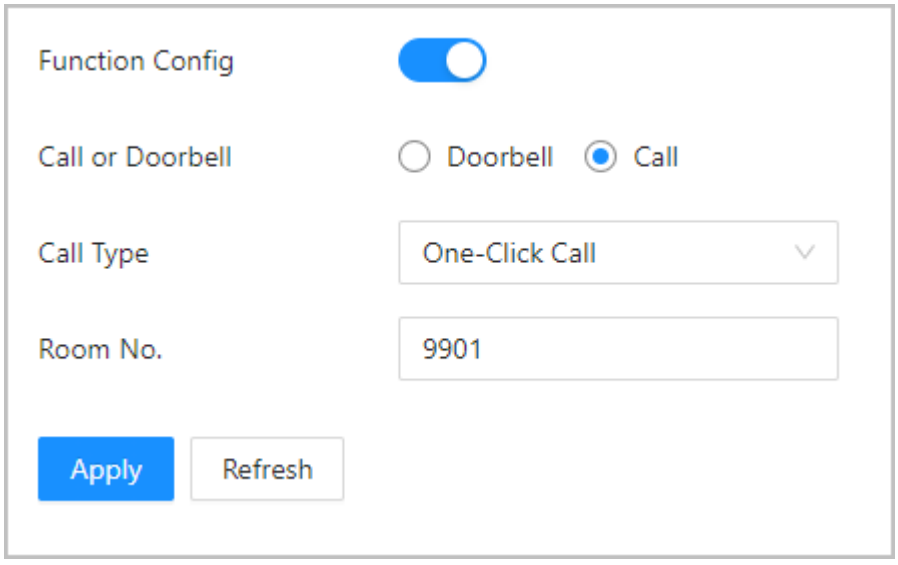


Table 3-14 Description of call and doorbell parameters

Parameter	Description
Call	• **Call type** : You can select **One-click Call** or **Call Management Center**. • **Room No.** : If you select **One-click Call**, you need to configure the room number.
Doorbell	• **Local Device Ringer** : Controls whether the device's built-in speaker plays a ringtone. • **External Doorbell** : Controls whether the ring signal is sent to an external doorbell device. You need to switch the alarm output port to the doorbell port. • **Ringtone Config** : Selects the ringtone played when the device is triggered. • **Ringtone Time (sec)** : Configure the duration for which the ringtone plays.

Step 4 Click **Apply**.

3.8 Configuring Access Control

3.8.1 Access Control Parameters

3.8.1.1 Configuring Basic Parameters

Procedure

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

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

Figure 3-18 Basic parameters

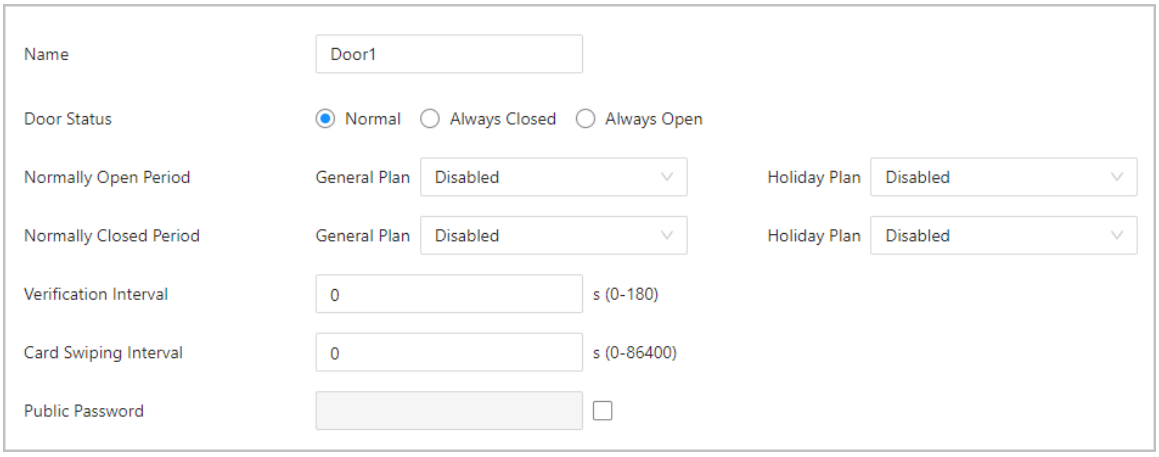


Table 3-15 Basic parameters description

Parameter	Description
Name	The name of the door.

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

Step 3 Click **Apply**.

3.8.1.2 Configuring Unlock Methods

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

Procedure

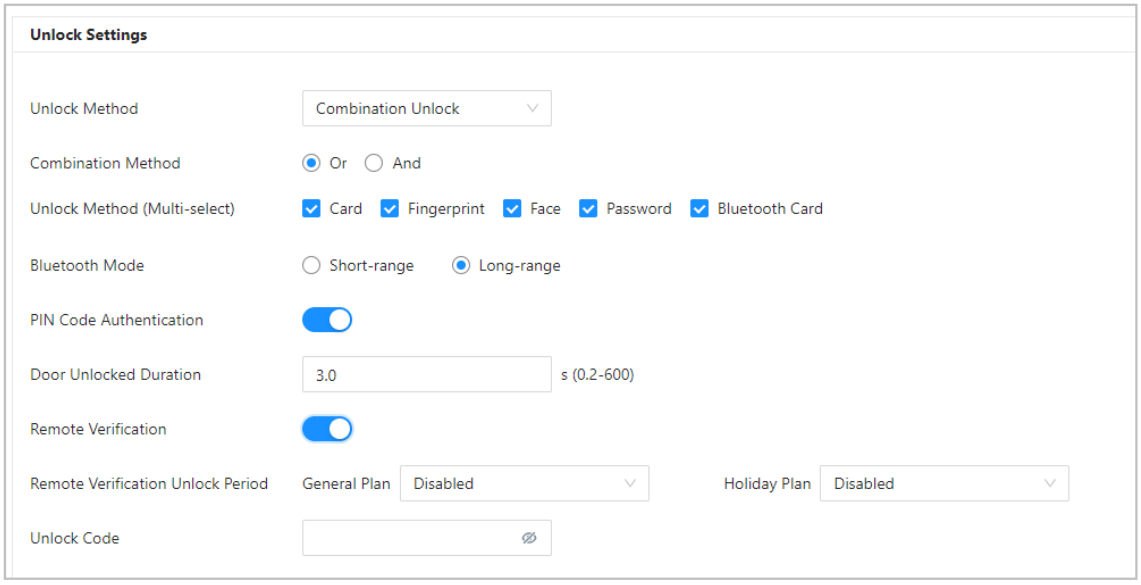
Step 1 Select **Access Control** > **Access Control Parameters**.

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

- Combination unlock
  1. Select **Combination Unlock** from the **Unlock Method** list.
  2. Select **Or** or **And**.
     - Or: Use one of the selected unlock methods to open the door.
     - And: Use all the selected unlock methods to open the door.

3. Select unlock methods, and then configure other parameters.

Figure 3-19 Combination unlock



- Unlock by multiple users.
  - ◇ If only one group is added, the door unlocks only after the number of people in the group who grant access equals the defined valid number.
  - ◇ If more than one groups are added, the door unlocks only after the number of people in each group who grant access equals the defined valid number.

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

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

Figure 3-20 Add group

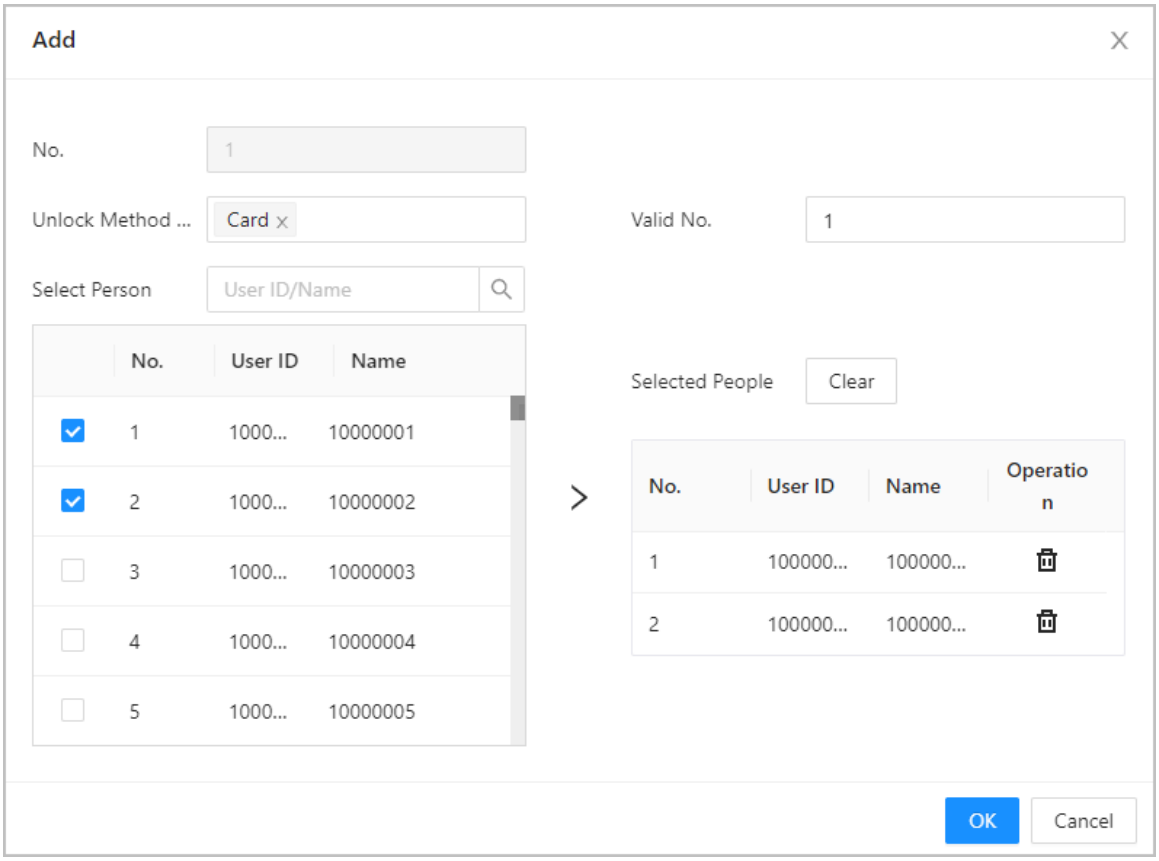


Figure 3-21 Unlock by multiple users

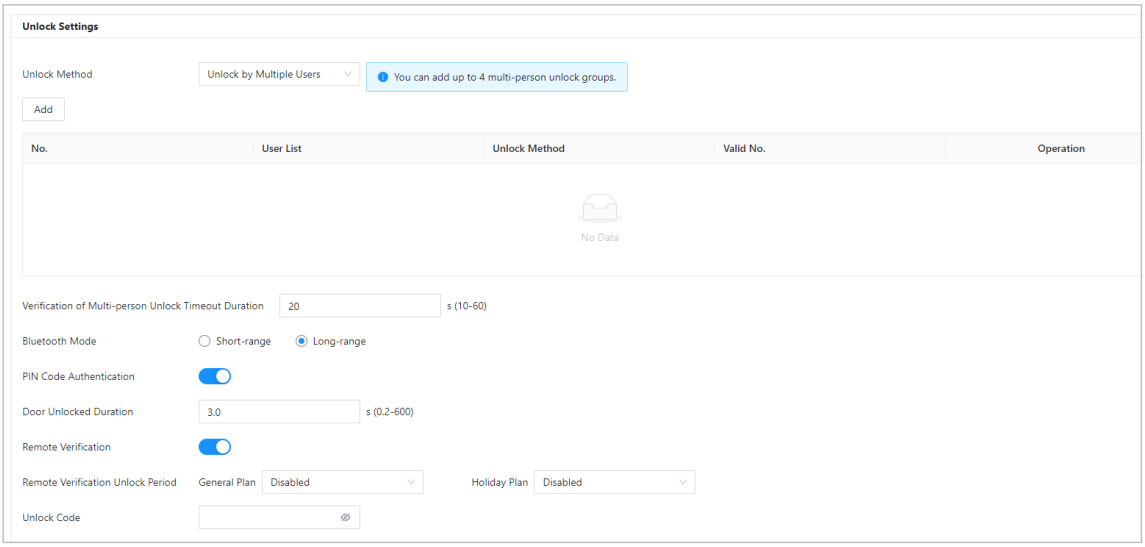


Table 3-16 Unlock settings description

Parameter	Description
Verification of Multi-person Unlock Timeout Duration	During verification, the interval between every two verifiers must be within this time period.

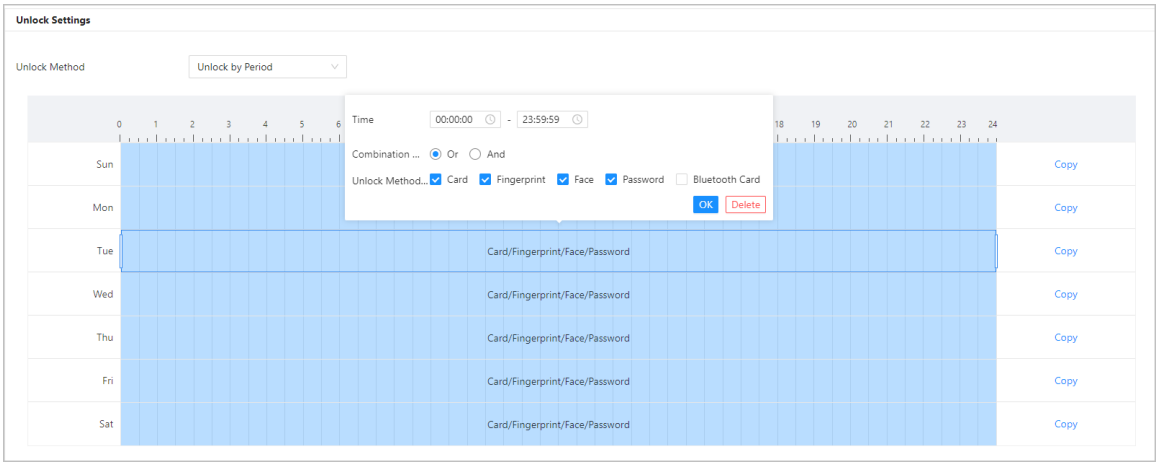
Parameter	Description
PIN Code Authentication	When PIN code authentication is enabled and you select user password to unlock, you only need to enter the user password without the user ID. When PIN code authentication is enabled, the remote verification is not supported when using user password to unlock.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

- Unlock by period

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

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

Figure 3-22 Unlock by period



Step 3 Click **Apply**.

3.8.2 Alarm

3.8.2.1 Configuring Alarm

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

Procedure

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

Step 2 (Optional) Select the door channel.

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

Figure 3-23 Select the channel

Step 3 Configure alarm parameters.

Figure 3-24 Alarm

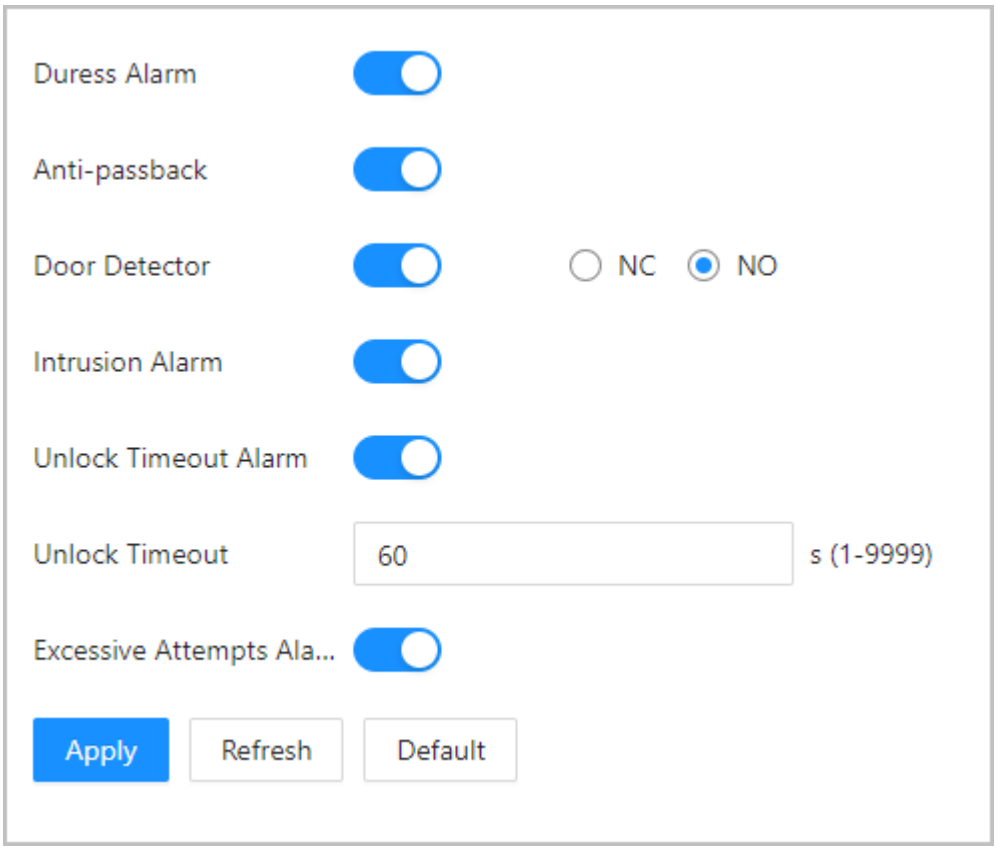


Table 3-17 Description of alarm parameters

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

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

Step 4 Click **Apply**.

3.8.2.2 Configuring Alarm Linkages (Optional)

You can configure alarm linkages.

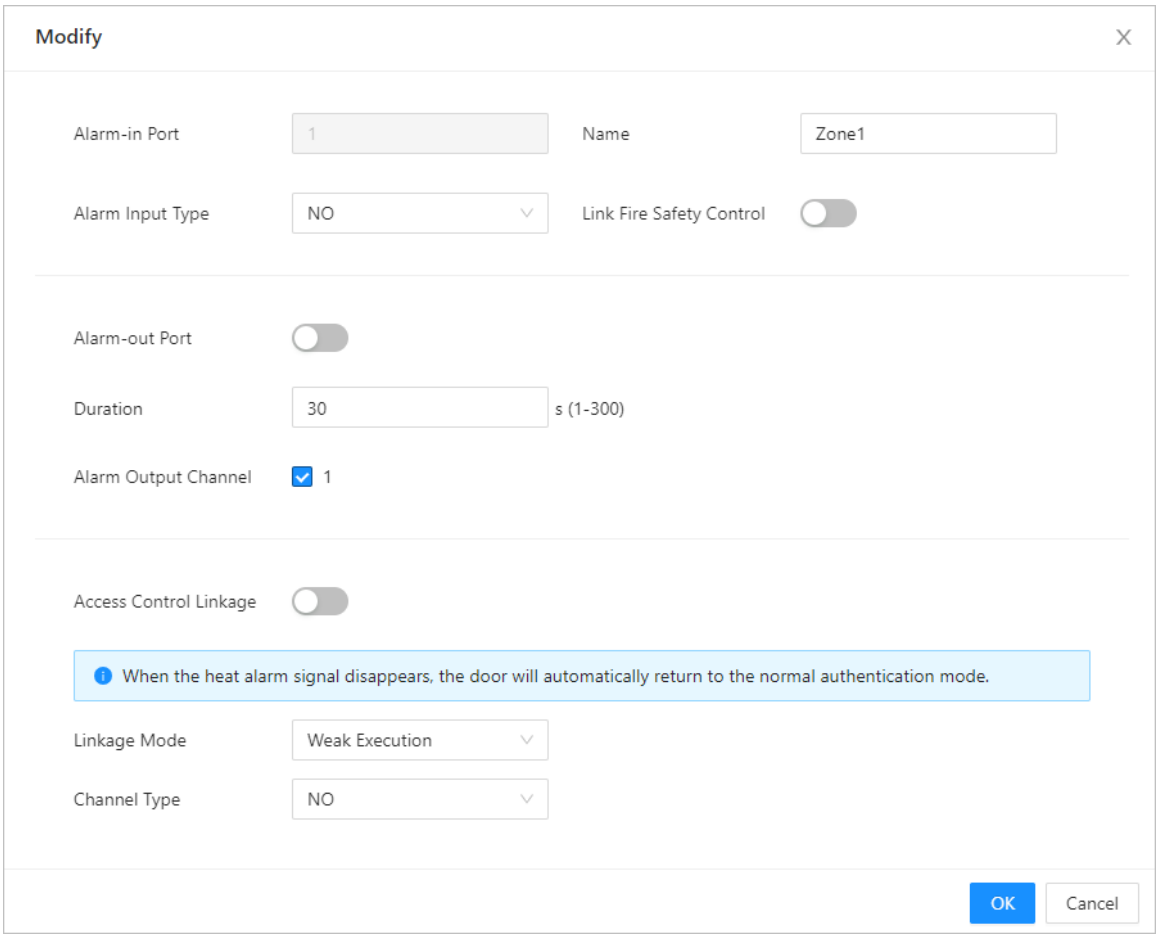
Procedure

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

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

Step 2 Click to configure alarm.

Figure 3-25 Alarm linkage



Step 3 Create a name for the alarm zone.

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

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

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

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

Step 6 Select a linkage mode.

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

Step 7 Select a channel type.

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

Step 8 Click **OK**.

3.8.2.3 Configuring Alarm Event Linkage

Procedure

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

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

Figure 3-26 Alarm event linkage

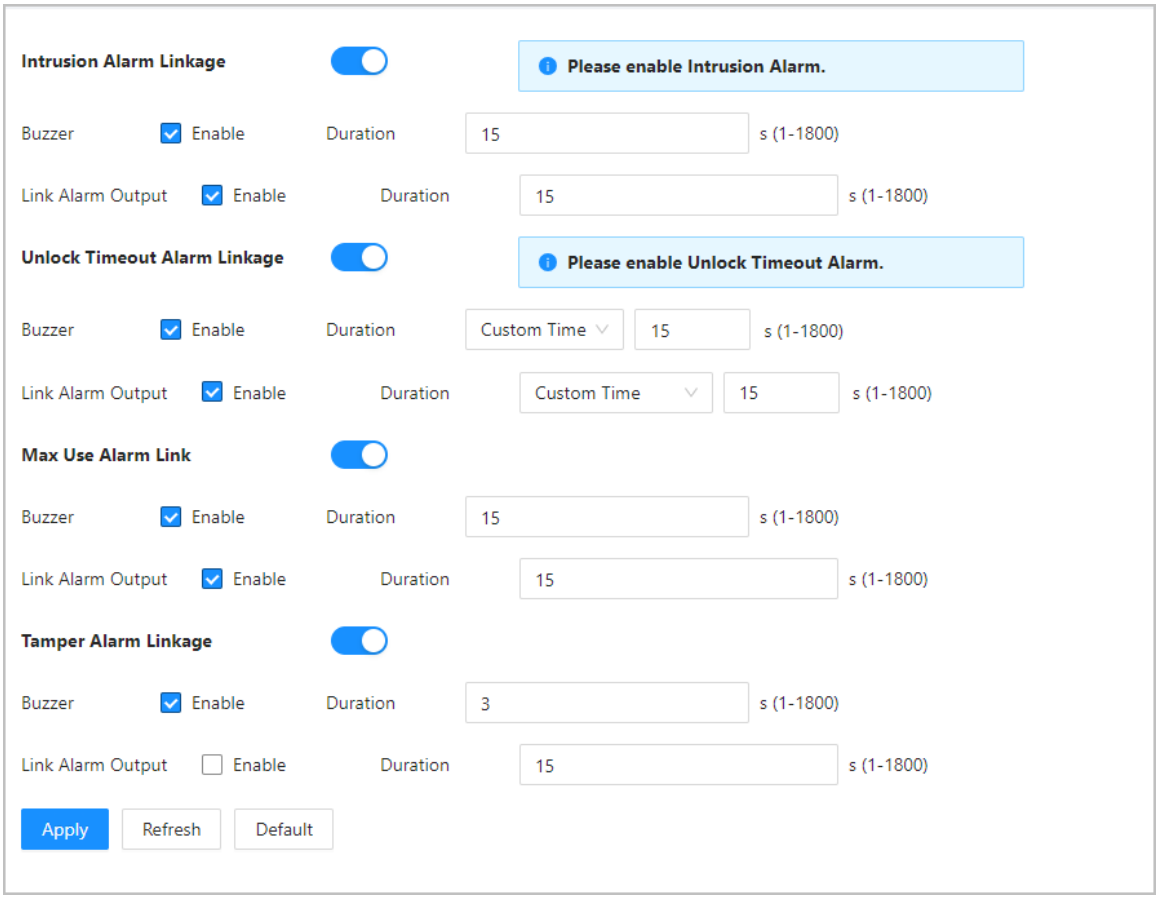


Table 3-18 Alarm event linkage

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

3.8.3 Configuring Face Parameters

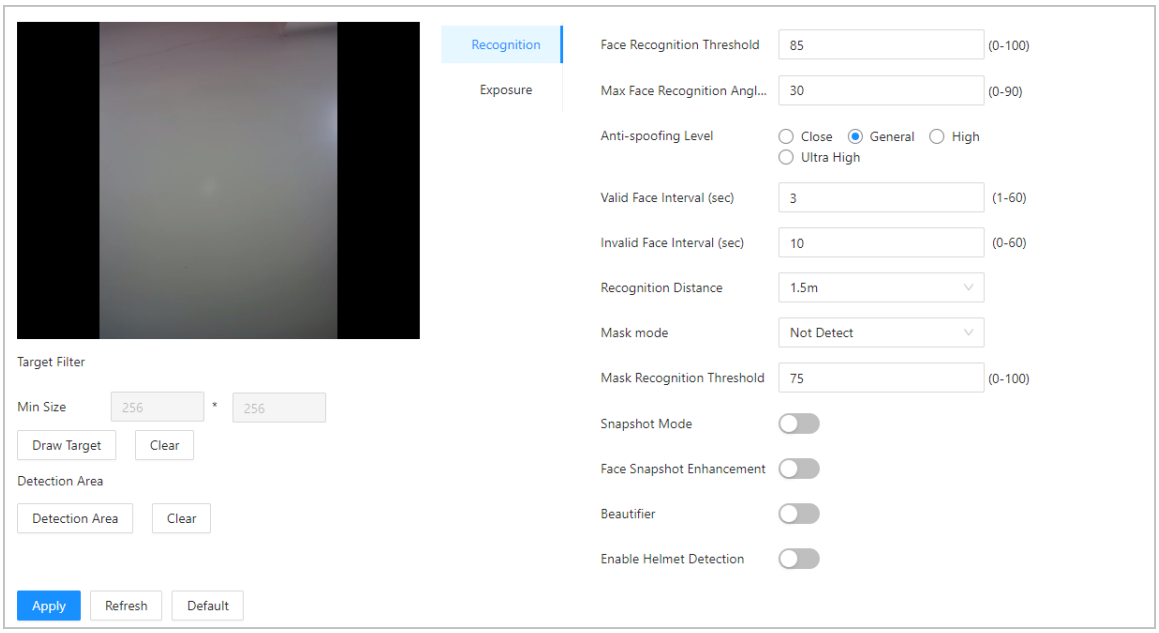
Configure face detection parameters. Face parameters might differ depending on models of the product.

Procedure

Step 1 Log in to the webpage.

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

Figure 3-27 Face detection parameters



Step 3 Configure the parameters.

Table 3-19 Description of face parameters

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

Name	Description
Valid Face Interval (sec)	When the same face remains in front of the lens after the first successful recognition, the Device will perform recognition again for the face after a defined interval.
Invalid Face Interval (sec)	When the same face remains in front of the lens after the first failed recognition, the Device will perform recognition again for the face after a defined interval. If you configure **0**, the face will not be captured and there is no unlock records.
Recognition Distance	The distance between the face and the lens.
Mask Mode	• **Not Detect** : Mask is not detected during face recognition. • **Mask Alert** : Mask is detected during face recognition. If the person is not wearing a mask, the system will remind them to wear a mask, but they will still be allowed access. • **Mask Required** : Mask is detected during face recognition. If a person is not wearing a mask, the system will remind them to wear masks, and access will be denied.
Mask Recognition Threshold	The higher the threshold, the more accurate face recognition will be when a person is wearing a mask, and there will be a lower false recognition rate.
Snapshot Mode	After the function is enabled, low-quality snapshots in the unlock records can be filtered out.
Face Snapshot Enhancement	After the function is enabled, the snapshots in the unlock records are beautified.
Beautifier	Beautify captured face images.
Enable Helmet Detection	Detects safety hats. The door will not unlock if a person does not wear a helmet.

Step 4 Configure the exposure parameters.

Figure 3-28 Exposure parameters

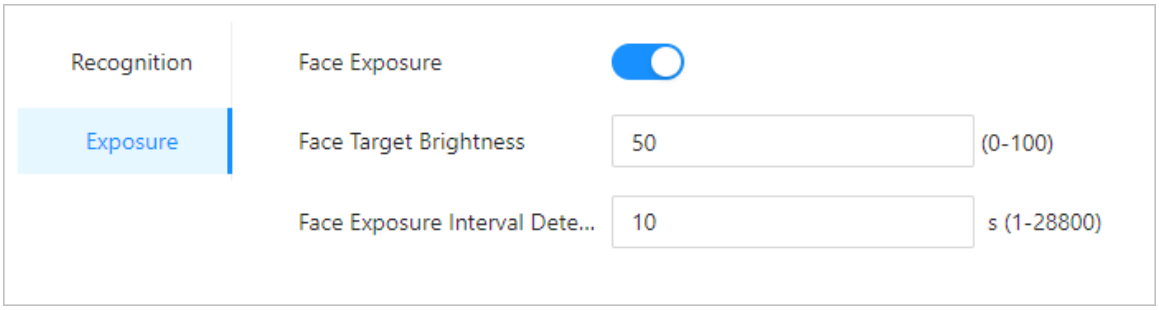


Table 3-20 Exposure parameters description

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

Step 5 Draw the face detection area.

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

The face in the defined area will be detected.

Step 6 Draw the target size.

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

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

Step 7 Draw the detection area.

Step 8 Click **OK**.

3.8.4 Card Settings

3.8.4.1 Configuring Card Settings

This function is only available on select models.

Procedure

Step 1 Log in to the webpage.

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

Step 3 Configure the card parameters.

Figure 3-29 Card parameters

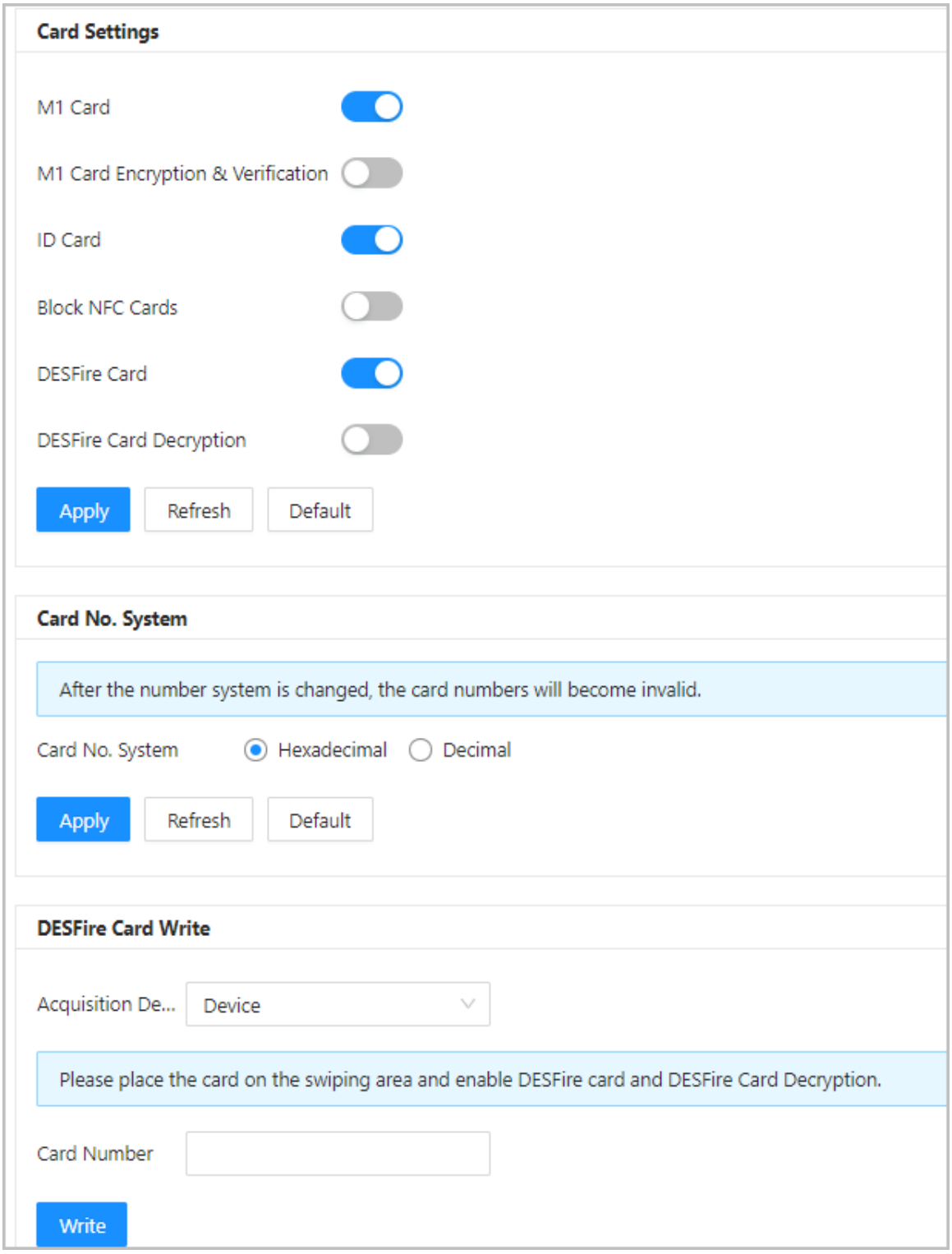


Table 3-21 Card parameters description

Item	Parameter	Description
Card Settings	M1 Card	The M1 card can be read when this function is enabled.

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

Step 4 Click **Apply**.

3.8.4.2 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 3-30 Add new Wiegand formats

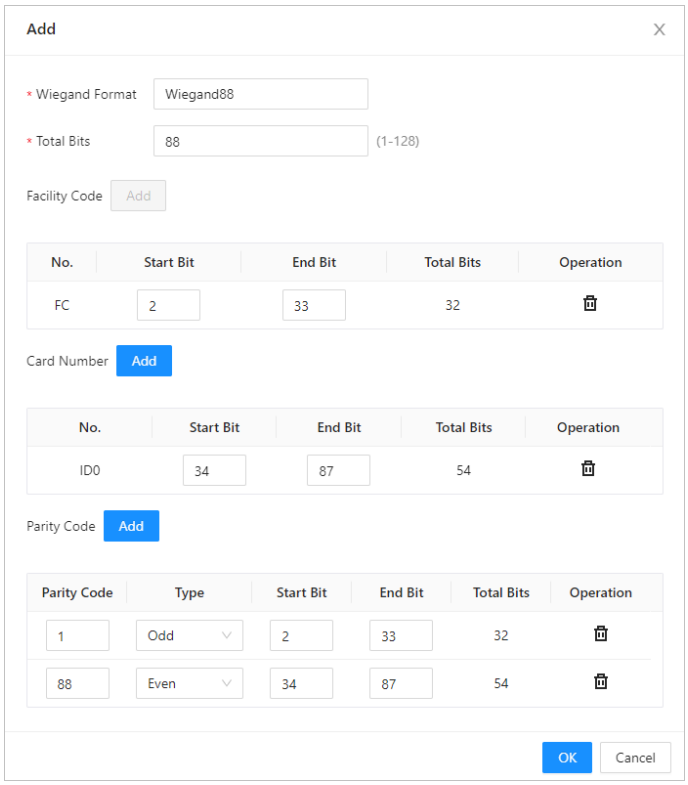


Table 3-22 Wiegand format description

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.

3.8.4.3 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

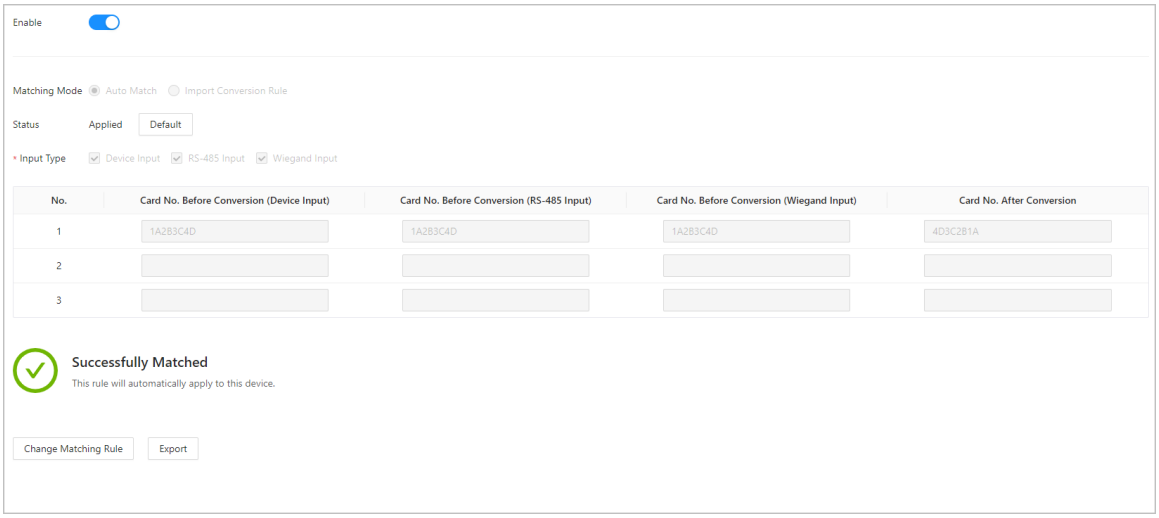
Step 1 Log in to the webpage.

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.
     - Device input: Swipe the card on the Device to read the card.
     - 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 customized 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**.

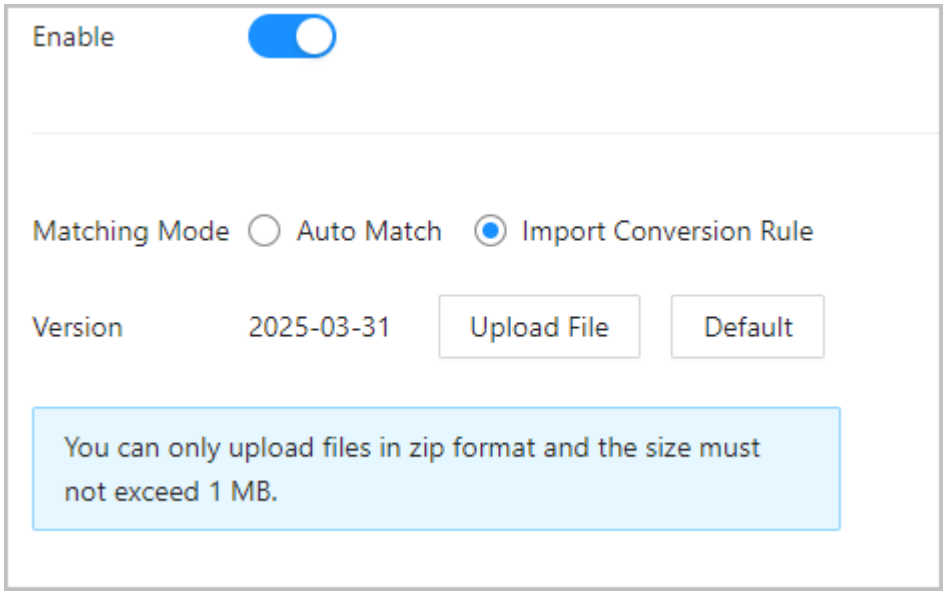
Figure 3-31 Auto match (successfully matched)



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

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

Figure 3-32 Import conversion rule



3.8.5 Configuring QR Code

Procedure

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

Figure 3-33 QR code

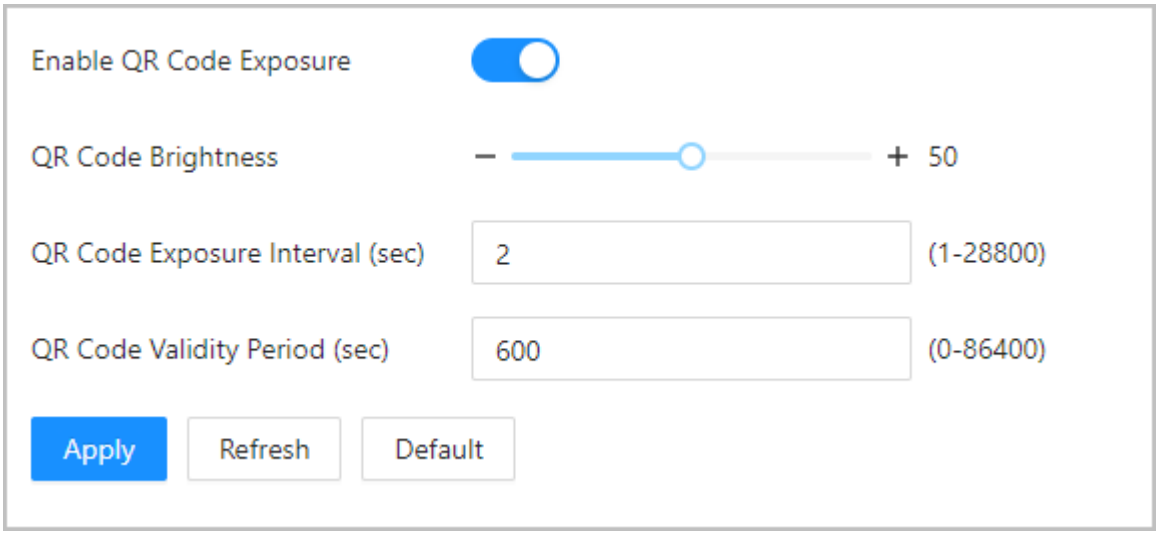


Table 3-23 QRR code parameters

Parameters	Description
Enable QR Code Exposure	The QR code will be exposed at the defined brightness, and the QR code can be detected and read clearly.
QR Code Brightness	
QR Code Exposure Interval (sec)	The QR code will be exposed only once during the defined interval.
QR Code Validity Period (min)	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.

3.8.6 Configuring Periods

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

3.8.6.1 Configuring General Plan

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

Procedure

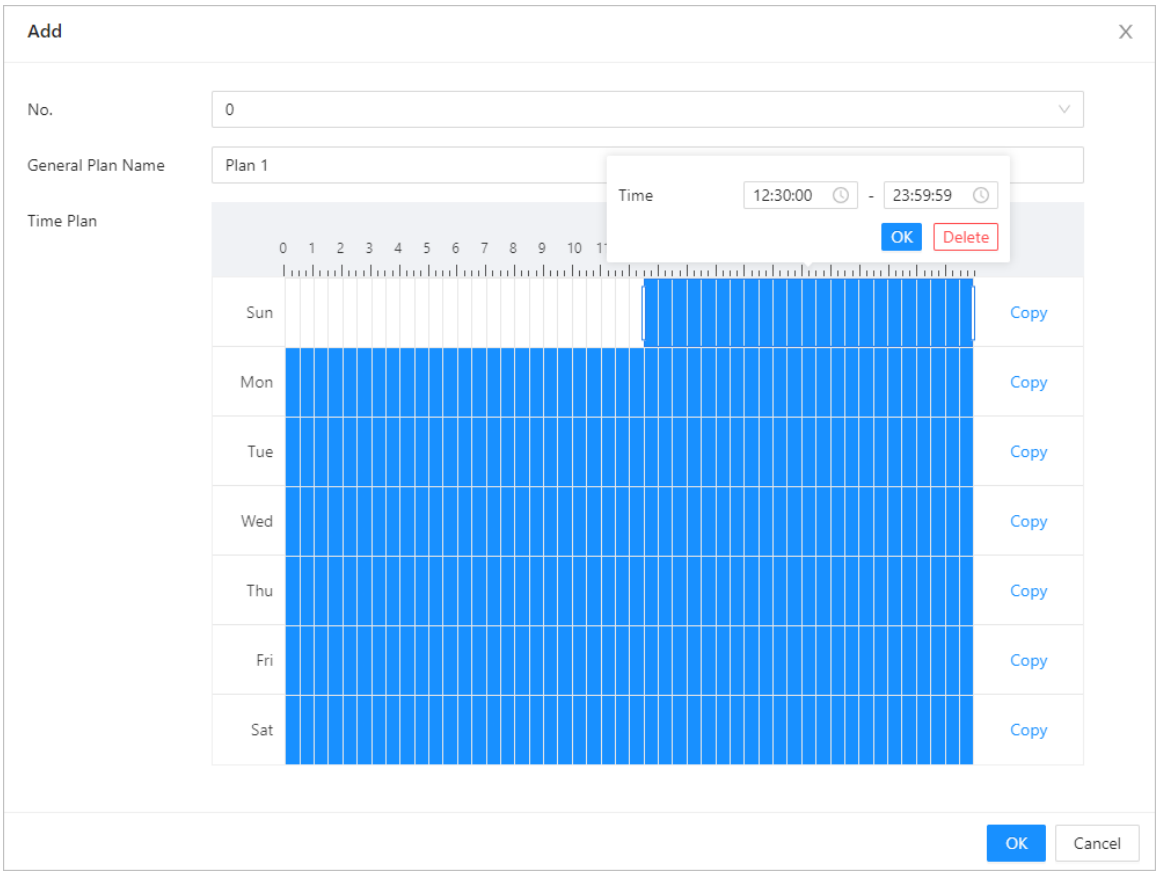
Step 1 Log in to the webpage.

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

Step 3 Click **Add**.

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

Figure 3-34 Configure general plan



Step 4 Click **OK**.

3.8.6.2 Configuring Holiday Plan

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

Procedure

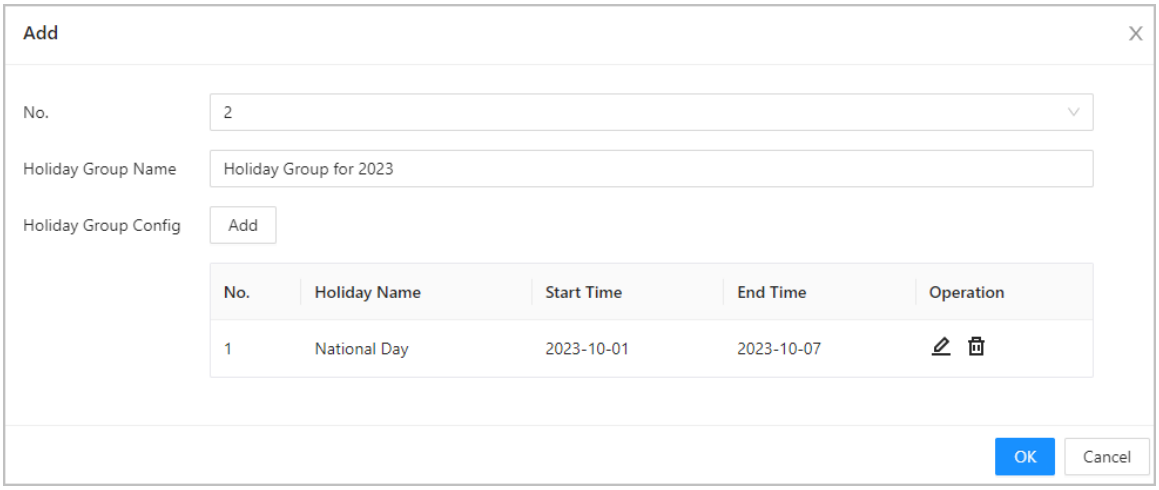
Step 1 Log in to the webpage.

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

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

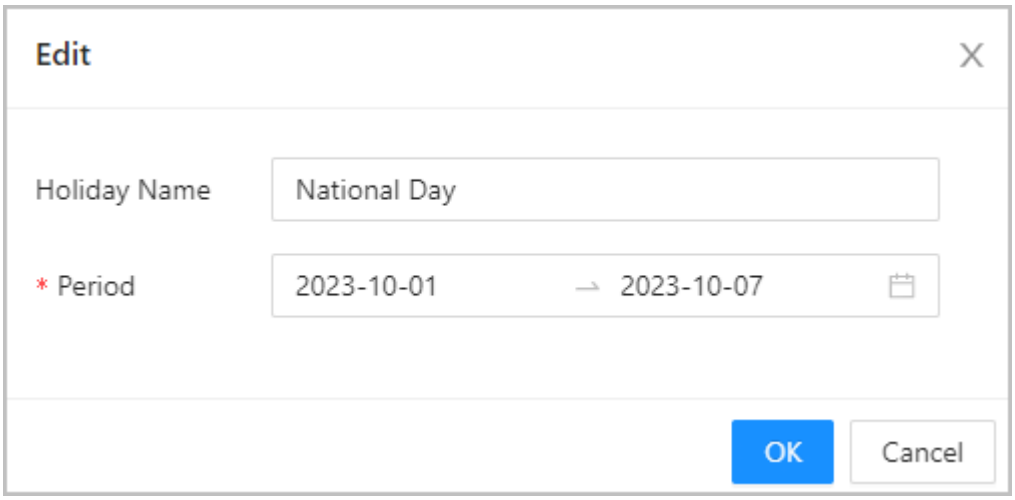
1. Select a number for the holiday group, and then enter a name for the group.

Figure 3-35 Add a holiday group



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

Figure 3-36 Add a holiday to a holiday group



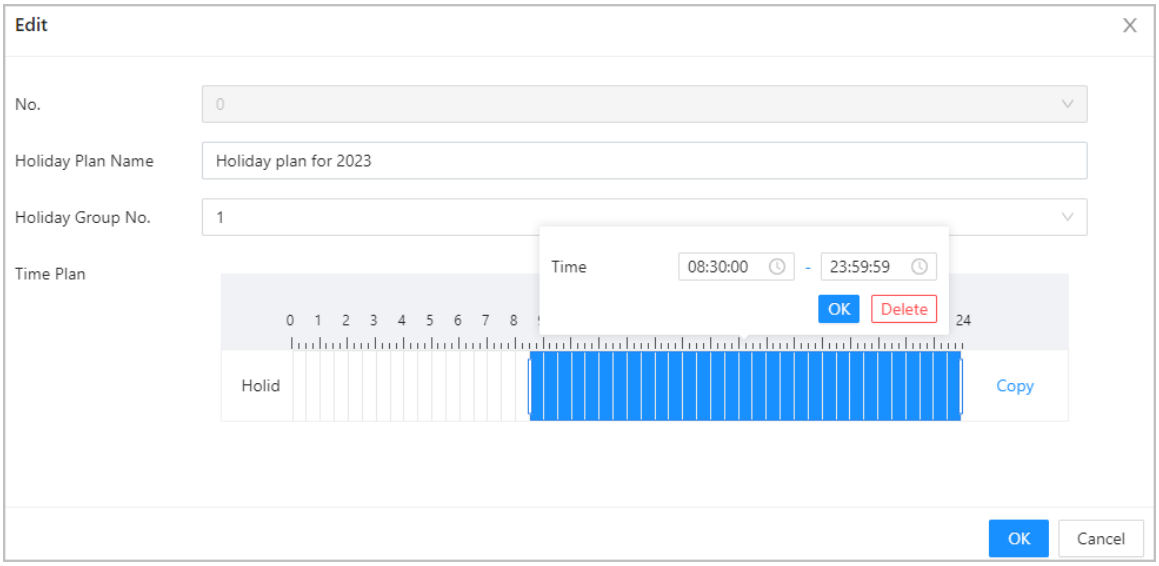
Step 4 Click **OK**.

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

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

   Supports adding up to 4 time sections on a day.

Figure 3-37 Add holiday plan



Step 6 Click **OK**.

3.8.7 Privacy Settings

Procedure

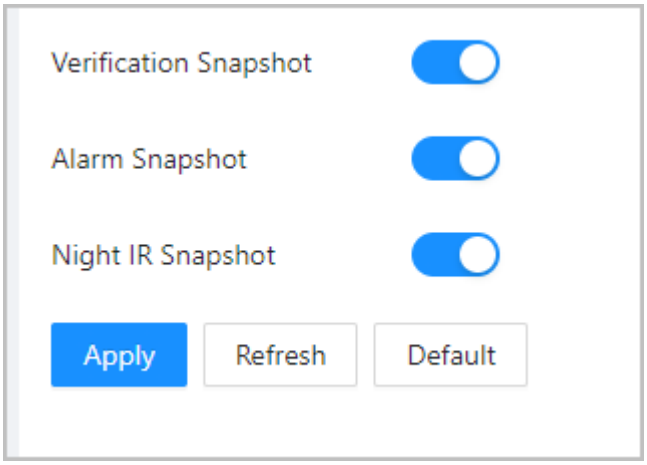
Step 1 On the webpage, select **Access Control** > **Privacy Settings**.

Step 2 Enable the function as needed.

- Verification snapshot: Face images will be captured automatically when people unlock the door.
- Alarm snapshot: When enabled, snapshots will be captured upon triggering anti-passback, duress, blocklist and unauthorized excessive attempts. It is turned off by default.
- Night IR snapshot: Clear images can be captured in low-light or complete darkness.

- When **Verification Snapshot** is enabled, **Night IR Snapshot** will be automatically enabled. During daytime, **Verification Snapshot** uses white light capture, while at night, it uses IR capture. If only **Night IR Snapshot** is disabled, **Verification Snapshot** will use white light capture in both daytime and nighttime scenarios.
- When **Alarm Snapshot** is enabled, **Night IR Snapshot** will be automatically enabled. During daytime, **Alarm Snapshot** uses white light capture, while at night, it uses IR capture. If only **Night IR Snapshot** is disabled, **Alarm Snapshot** will use white light capture in both daytime and nighttime scenarios.
- When **Verification Snapshot** , **Alarm Snapshot**, and **Night IR Snapshot** are all enabled, and both **Verification Snapshot** and **Alarm Snapshot** are disabled, the **Night IR Snapshot** will be automatically hidden.

Figure 3-38 Privacy settings



Step 3 Click **Apply**.

3.8.8 Configuring Output Port Functions

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

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

Procedure

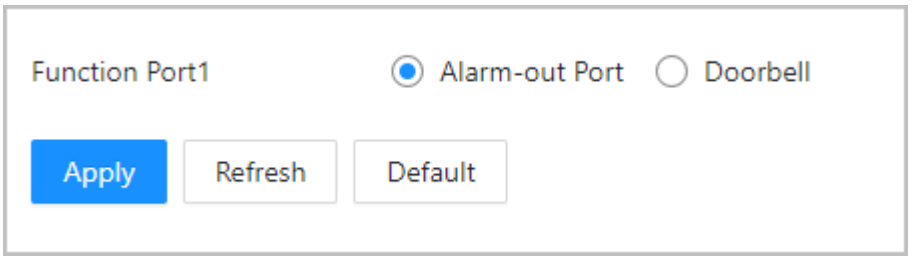
Step 1 On the webpage, select **Access Control** > **Output Port Config**.

Step 2 Select the type of the port.

When the alarm cable and the doorbell cable are shared, configure the interface to **Doorbell** to make sure the doorbell will ring.

Step 3 Click **Apply**.

Figure 3-39 Configure ports



3.8.9 Configuring Back-end Comparison

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

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

Figure 3-40 Back-end comparison

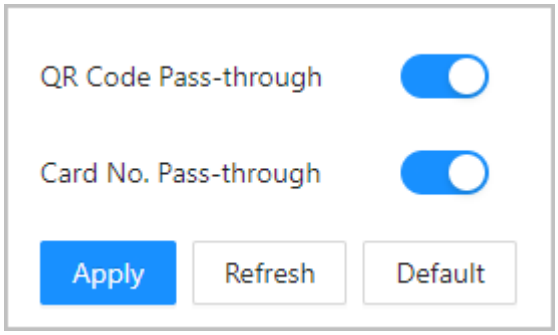


Table 3-24 Back-end comparison

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

3.8.10 Configuring First-Person Unlock

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

Prerequisites

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

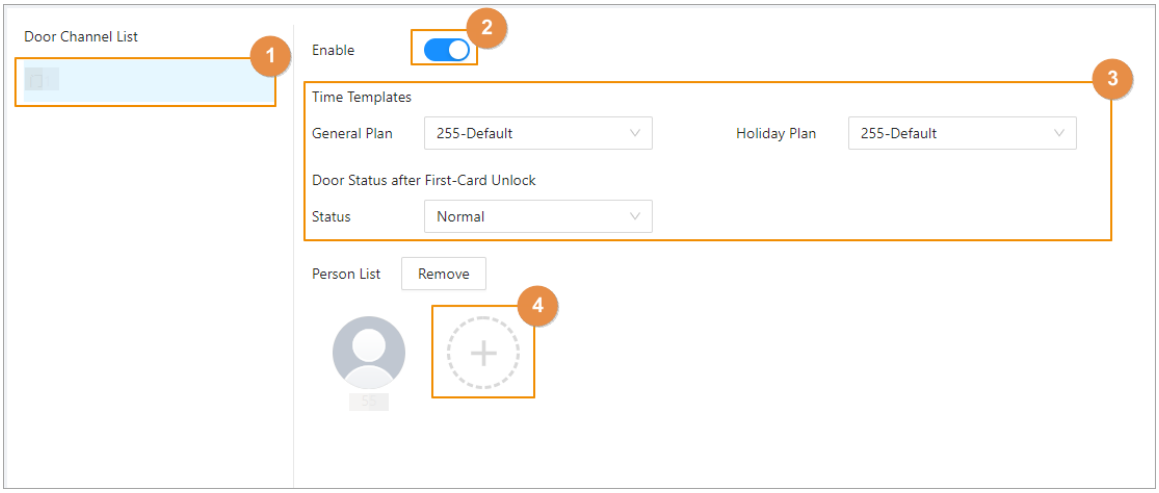
- Only the general users can be configured as the first person.
- After the first person verifies the identity, if the Device restarts, the first person needs to verify the identity again.
- After the function is enabled, patrol users can normally clock in and out.

Procedure

Step 1 Select **Access Control** > **First-Person Unlock**.

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

Figure 3-41 First-person unlock



Step 3 Configure the parameters.

Table 3-25 Parameter description

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

Step 4 Click **Apply**.

3.9 Configuring Audio and Video

3.9.1 Configuring Video

Procedure

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

Step 2 Configure the bit rate.

Figure 3-42 Bit rate

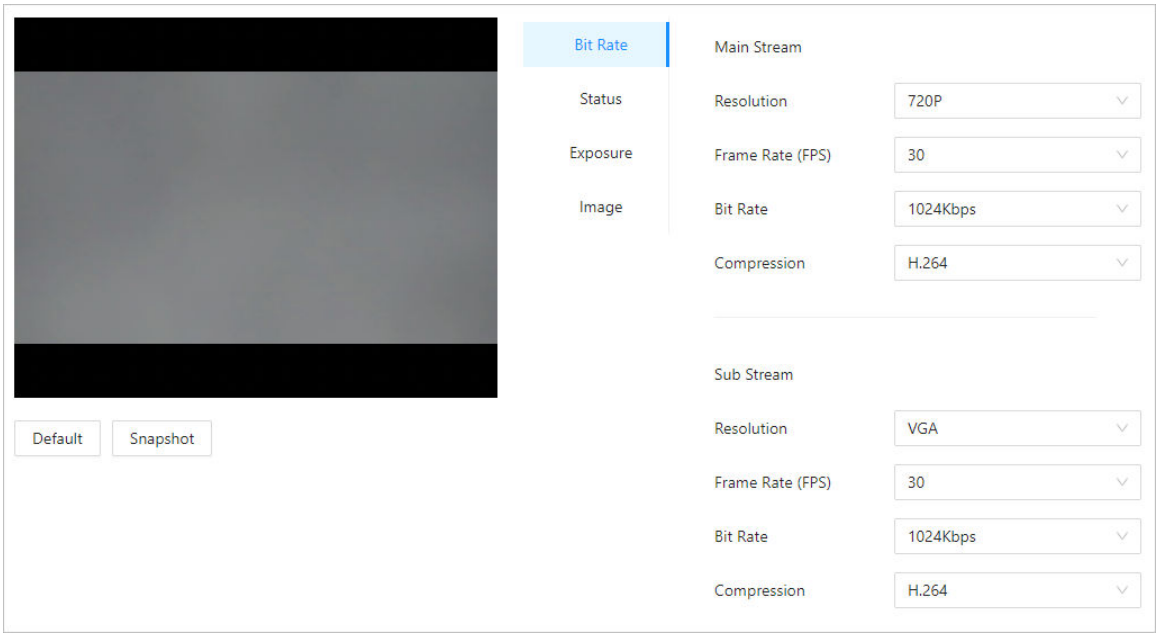


Table 3-26 Bit rate description

Parameter		Description
Main Format	Resolution	When the Device functions as the VTO and connects the VTH, the acquired stream limit of VTH is 720p.When resolution is changed to 1080p, the call and monitor function might be affected.
	Frame Rate (FPS)	The number of frames (or images) per second.
	Bit Rate	The amount of data transmitted over an internet connection in a given amount of time. Select a proper value based on your network speed.
	Compression	Video compression standard to deliver good video quality at lower bit rates.
Sub Stream	Resolution	The sub-stream supports D1, VGA and QVGA.
	Frame Rate (FPS)	The number of frames (or images) per second.
	Bit Rate	It indicates the amount of data transmitted over an internet connection in a given amount of time.
	Compression	Video compression standard to deliver good video quality at lower bit rates.

Step 3 Configure the status.

Figure 3-43 Status

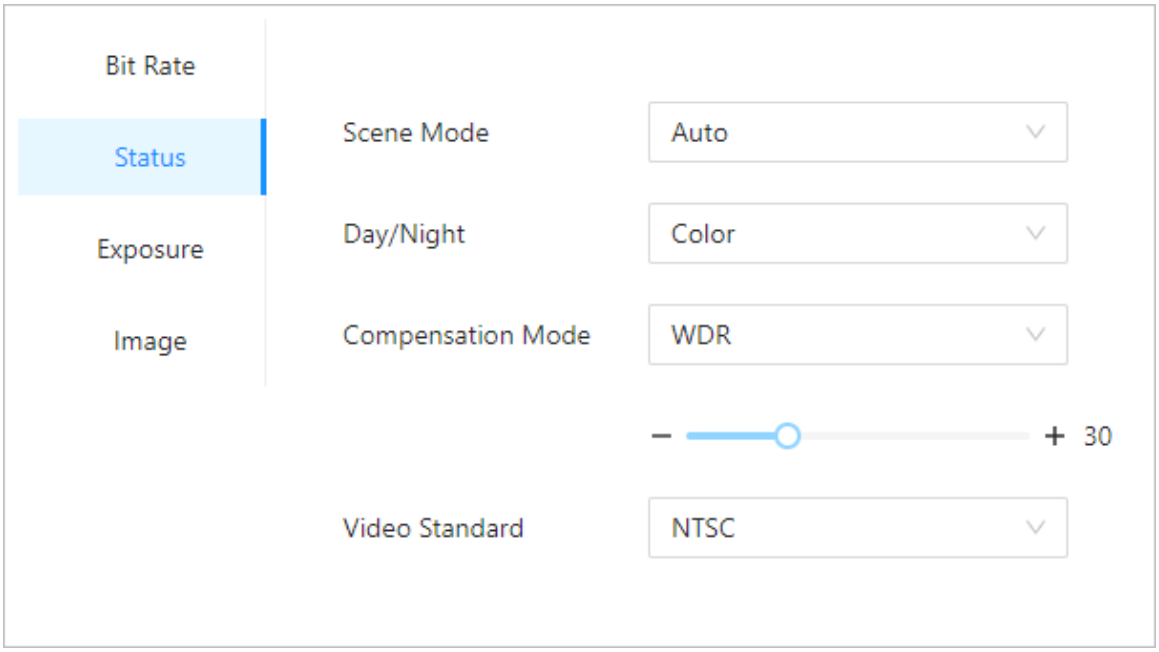


Table 3-27 Parameters description of status

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

Step 4 Configure the exposure parameters.

Figure 3-44 Exposure

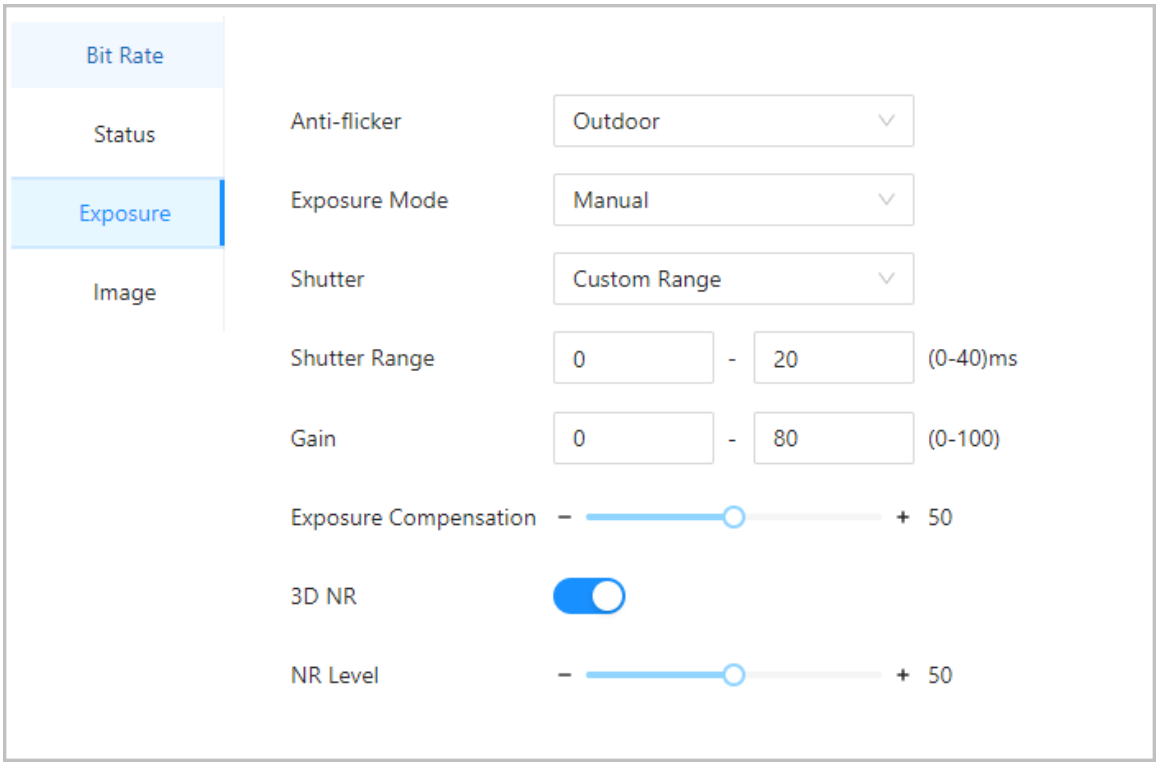


Table 3-28 Exposure parameter description

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

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

Step 5 Configure the image.

Figure 3-45 Image

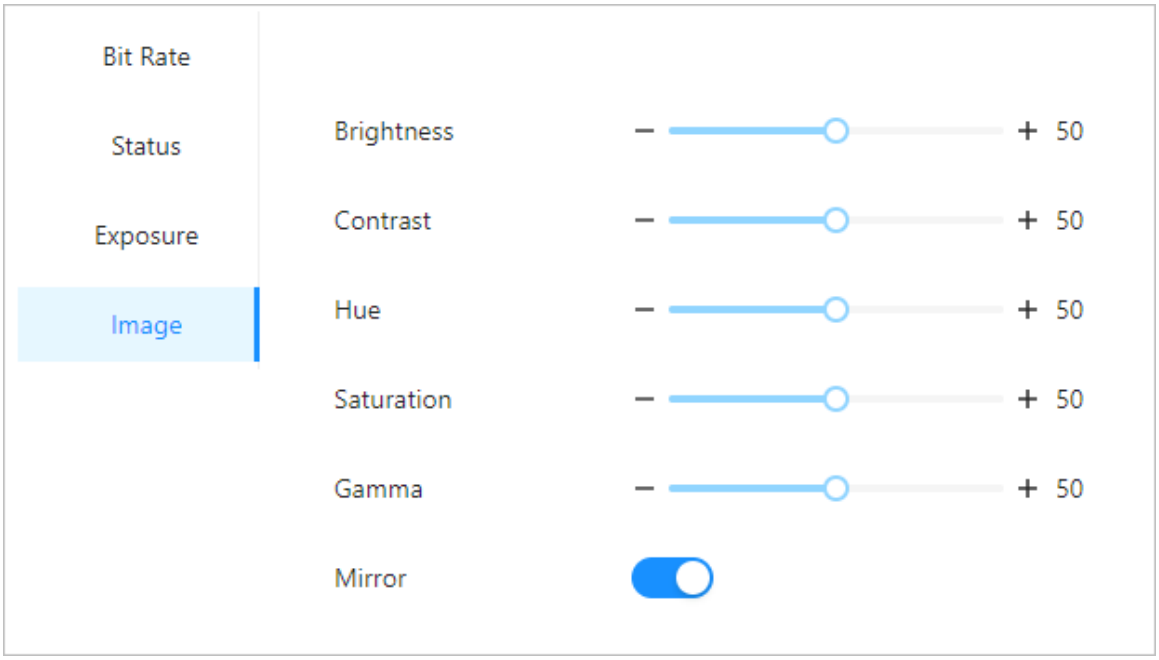


Table 3-29 Image description

Parameter	Description
Brightness	The brightness of the image. Higher value means brighter images.
Contrast	Contrast is the difference in the luminance or color that makes an object distinguishable. The larger the contrast value is, the greater the color contrast will be.
Hue	Refers to the strength or saturation of a color. It describes the color intensity, or how pure it is.
Saturation	Color saturation indicates the intensity of color in an image. As the saturation increases, the appear stronger, for example being more red or more blue. The saturation value does not change image brightness.
Gamma	Change the image brightness and contrast in a non-linear way. The higher the value, the brighter the image.
Mirror	When the function is turned on, images will be displayed with the left and right side reversed. The device screen does not support configuration, and it always displays the mirror image.

Related Operations

- Default: Click **Default**, and the parameters on this page restore to default settings.
- Snapshot: Click **Snapshot** to take the snapshot of the current device screen.

3.9.2 Configuring Audio Prompts

Set audio prompts during identity verification.

Procedure

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

Step 2 Configure the audio parameters.

Figure 3-46 Configure audio parameters

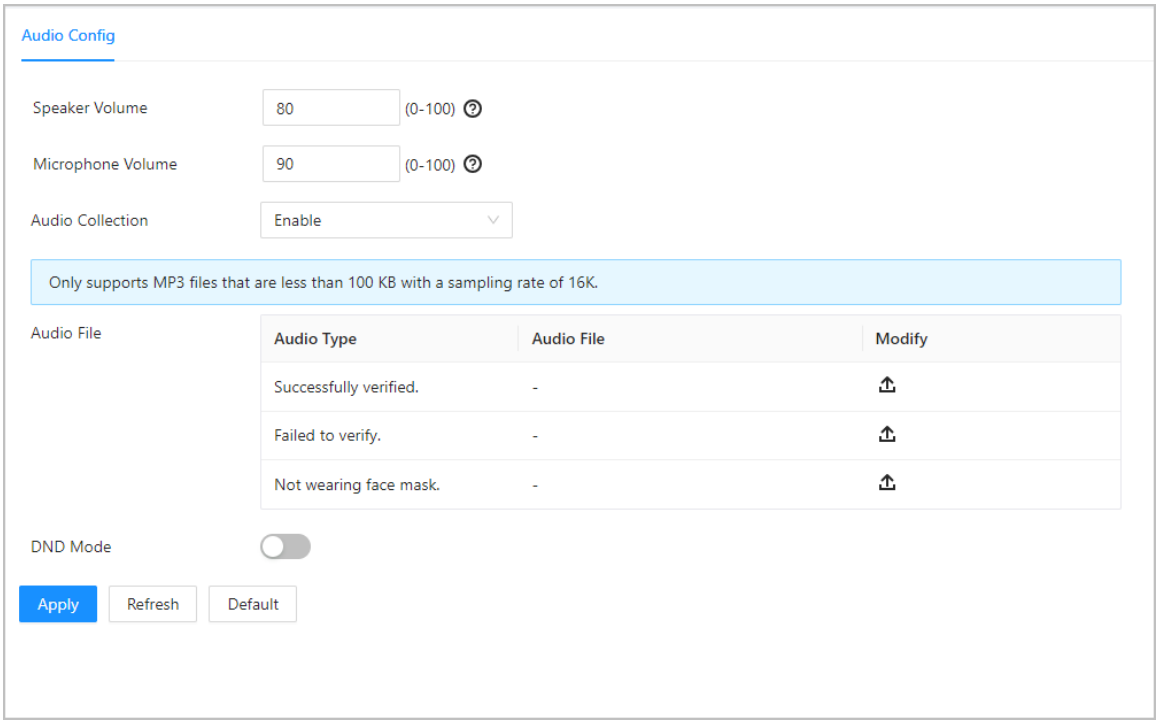


Table 3-30 Parameters description

Parameters	Description
Speaker Volume	Set the volume of the speaker.
Microphone Volume	Set the volume of the microphone.
Audio Collection	If this function is enabled, the sound from the device mic will be captured during live view and recording.
Audio File	You can upload audio files to the device.
DND Mode	No voice prompts during the set time when you verify your identity on the Device. You can set up to 4 periods.

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

Only supports MP3 files that are less than 100 KB with a sampling rate of 16K.

Step 4 Click **Apply**.

3.9.3 Configuring Local Code

Set the view area in the video talk and preview.

Background Information

This function is enabled by default when it works with a VTH. The preview might be not accessible when this function is turned off.

Procedure

Step 1 Log in to the webpage.

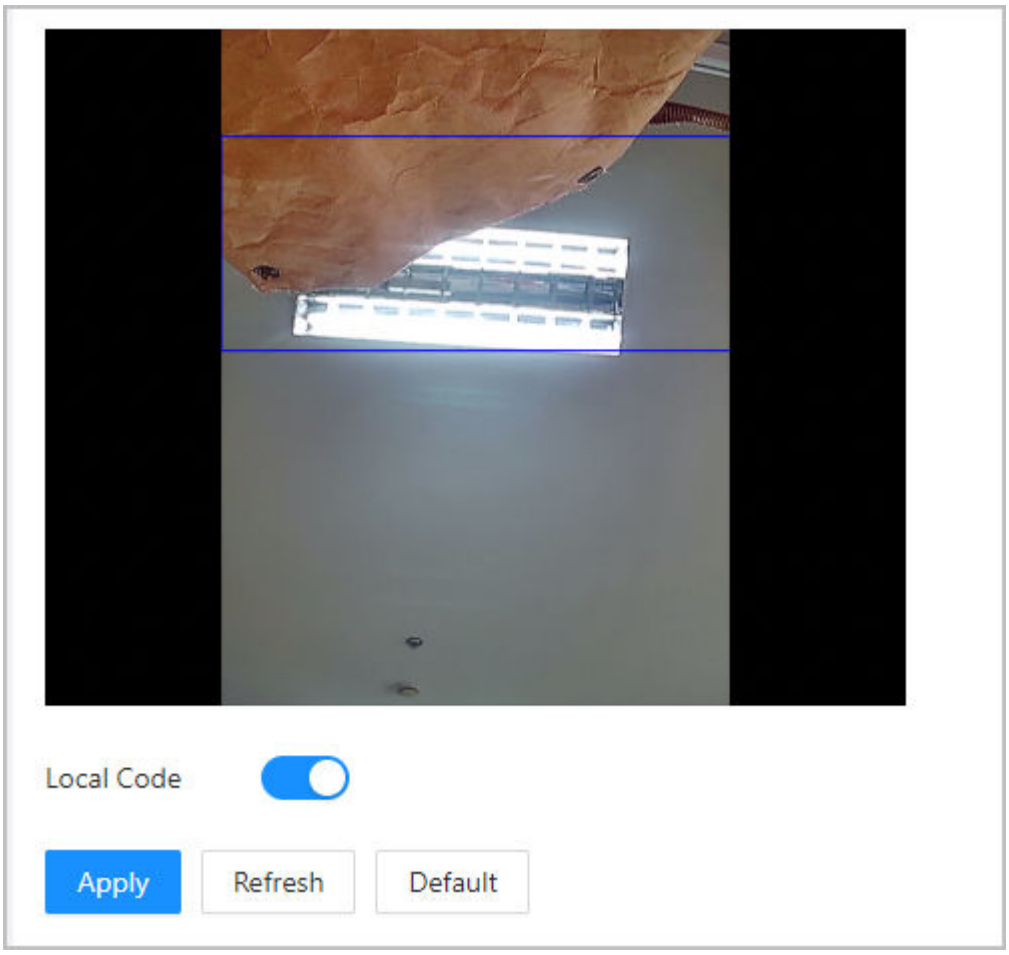
Step 2 Select **Audio and Video Config** > **Local Code**.

Step 3 Select **Enable** to turn on the function.

Step 4 Drag the box to a designated position.

The box indicates the preview area during the video talk.

Figure 3-47 Local coding



Step 5 Click **Apply**.

3.10 Communication Settings

3.10.1 Network Settings

3.10.1.1 Configuring TCP/IP

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

Procedure

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

Step 2 Configure the parameters.

Figure 3-48 TCP/IP

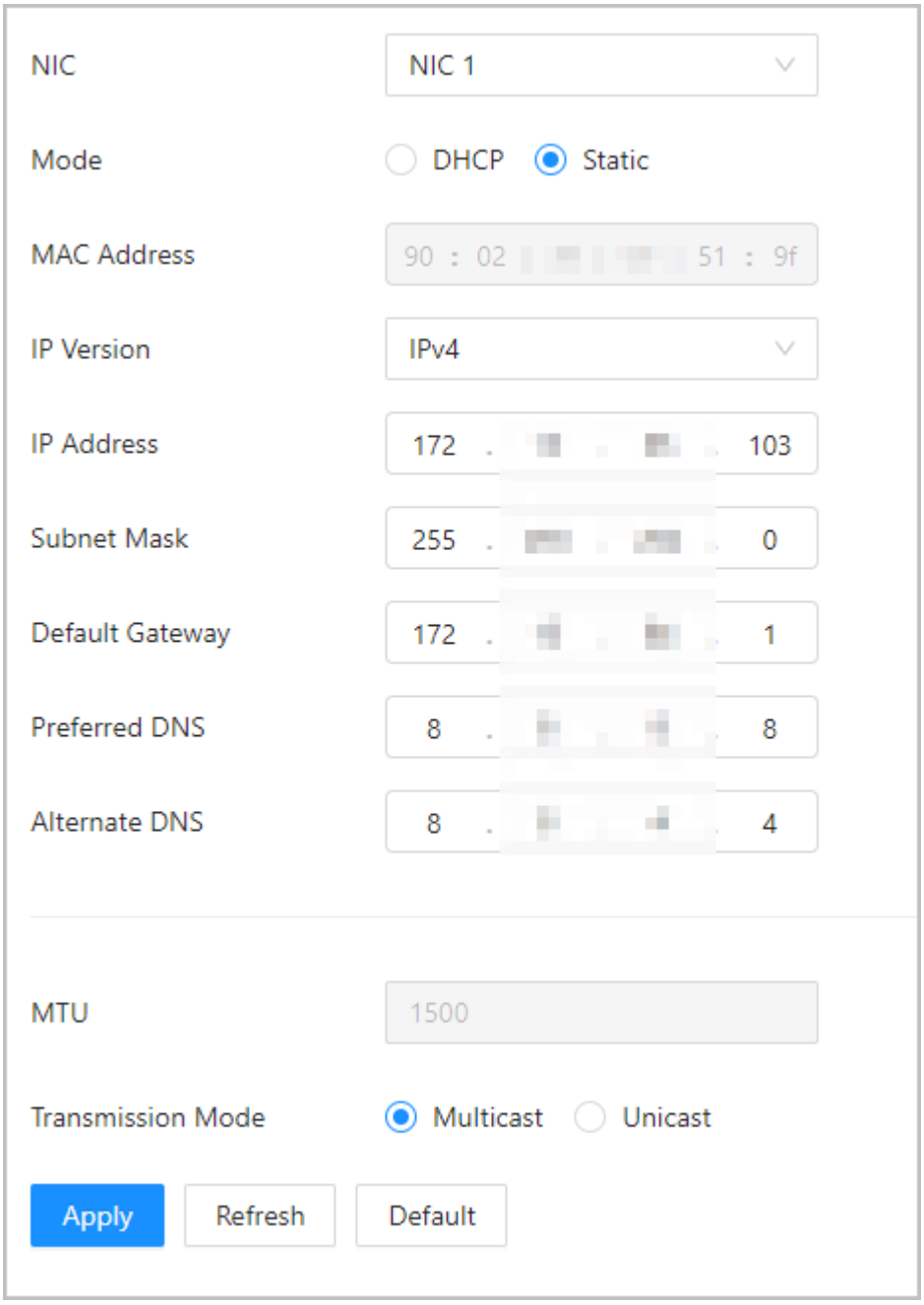


Table 3-31 Description of TCP/IP

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

Parameter	Description
IP Address	If you set the mode to **Static**, configure the IP address, subnet mask and gateway. ● IPv6 address is represented in hexadecimal. ● IPv6 version do not require setting subnet masks. ● The IP address and default gateway must be in the same network segment.
Subnet Mask	
Default Gateway	
Preferred DNS	Set IP address of the preferred DNS server.
Alternate DNS	Set IP address of the alternate DNS server.
MTU	MTU (Maximum Transmission Unit) refers to the maximum size of data that can be transmitted in a single network packet in computer networks. It is 1500 by default.
Transmission Mode	● Multicast: Ideal for video talk. ● Unicast: Ideal for group call.

Step 3 Click **OK**.

3.10.1.2 Configuring Wi-Fi

- The Wi-Fi function is available only on select models.
- Wi-Fi and Wi-Fi AP can be enabled at the same time, and Wi-Fi function is enabled by default.

Procedure

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

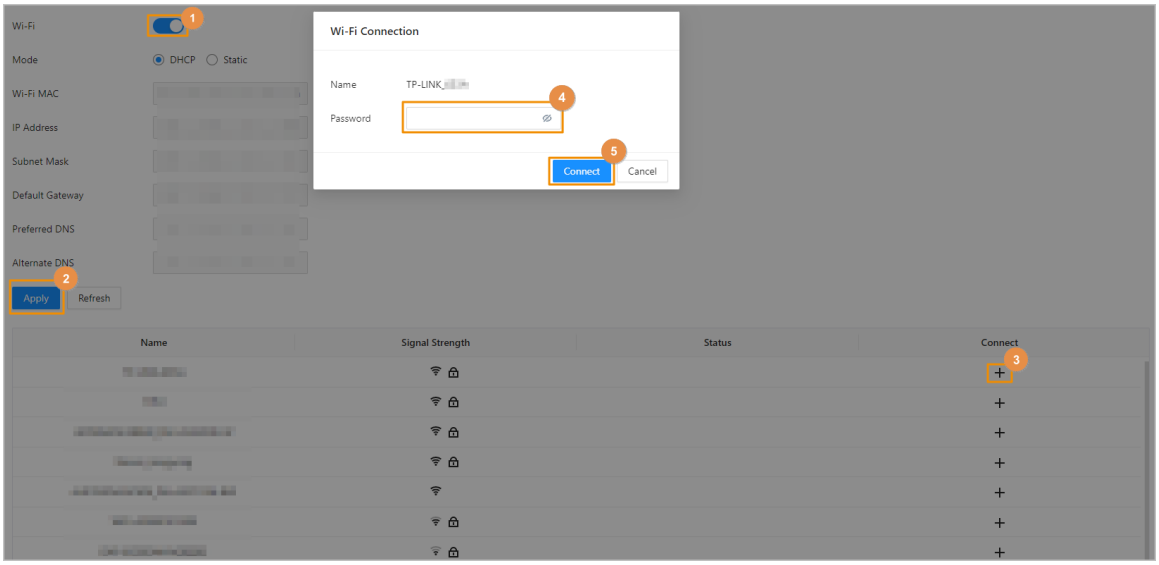
Step 2 Turn on Wi-Fi, and then click **Apply**.

All available Wi-Fi are displayed.

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

The Wi-Fi is connected.

Figure 3-49 Wi-Fi



Related Operations

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

3.10.1.3 Configuring Wi-Fi AP

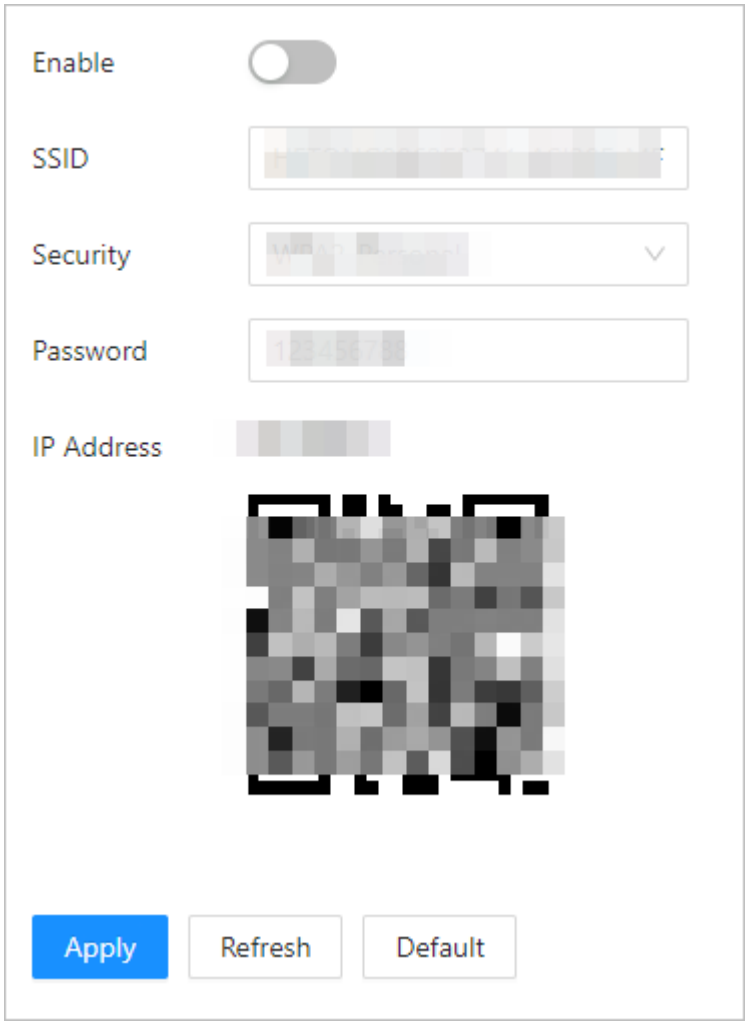
Wi-Fi and Wi-Fi AP can be enabled at the same time, and Wi-Fi function is enabled by default.

Procedure

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

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

Figure 3-50 Wi-Fi AP



Results

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

3.10.1.4 Configuring Port

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

Procedure

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

Step 2 Configure the ports.

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

Figure 3-51 Configure ports

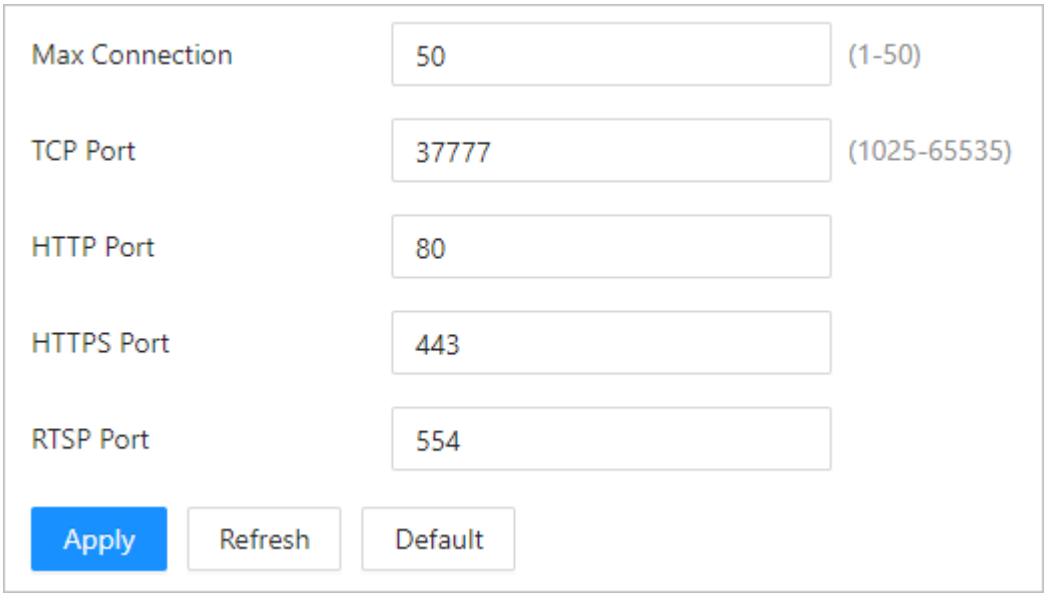


Table 3-32 Description of ports

Parameter	Description
Max Connection	You can set the maximum number of clients (such as webpage, desktop client and mobile client) that can access the Device at the same time.
TCP Port	Default value is 37777.
HTTP Port	Default value is 80. If you have changed the port number, add the port number after the IP address when access the webpage.
HTTPS Port	Default value is 443.
RTSP Port	Default value is 554.

Step 3 Click **Apply**.

3.10.1.5 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** > **Network Settings** > **Basic Services**.

Step 2 Configure the basic services.

Figure 3-52 Basic service

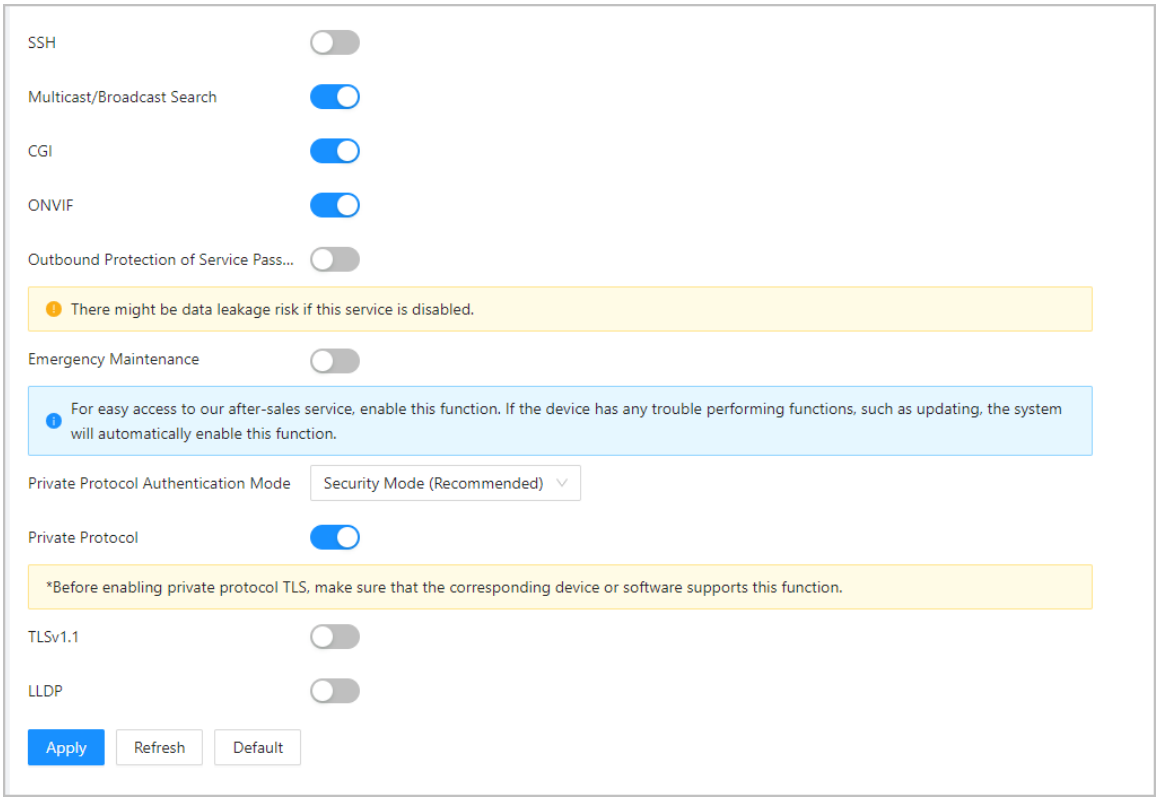


Table 3-33 Basic service parameter description

Parameter	Description
SSH	SSH, or Secure Shell Protocol, is a remote administration protocol that allows users to access, control, and modify their remote servers over the internet.
Mutlicast/Broadcast Search	Search for devices through multicast or broadcast protocol.
CGI	The Common Gateway Interface (CGI) is an intersection between web servers through which the standardized data exchange between external applications and servers is possible.
ONVIF	ONVIF stands for Open Network Video Interface Forum. Its aim is to provide a standard for the interface between different IP-based security devices. These standardized ONVIF specifications are like a common language that all devices can use to communicate.
Outbound Protection of Service Password	Make sure that devices and software which are compatible with the VTO can perform their services while **Outbound Protection of Service Password** is enabled. There might be data leakage risk if this service is disabled.
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. Security risks might present when TLSv1.1 is enabled. Please be advised.
LLDP	LLDP is the abbreviation for Link Layer Discovery Protocol, which is a data link layer protocol. It allows network devices, such as switches, routers, or servers, to exchange information about their identities and capabilities with each other. The LLDP protocol helps network administrators gain a better understanding of network topology and provides a standardized way to automate the discovery and mapping of connections between network devices. This makes it easier to perform network configuration, troubleshoot issues, and optimize performance.

Step 3 Click **Apply**.

3.10.1.6 Configuring Cloud Service

The cloud service provides a NAT penetration service. Users can manage multiple devices through DMSS. You do not have to apply for dynamic domain name, configure port mapping or deploy server.

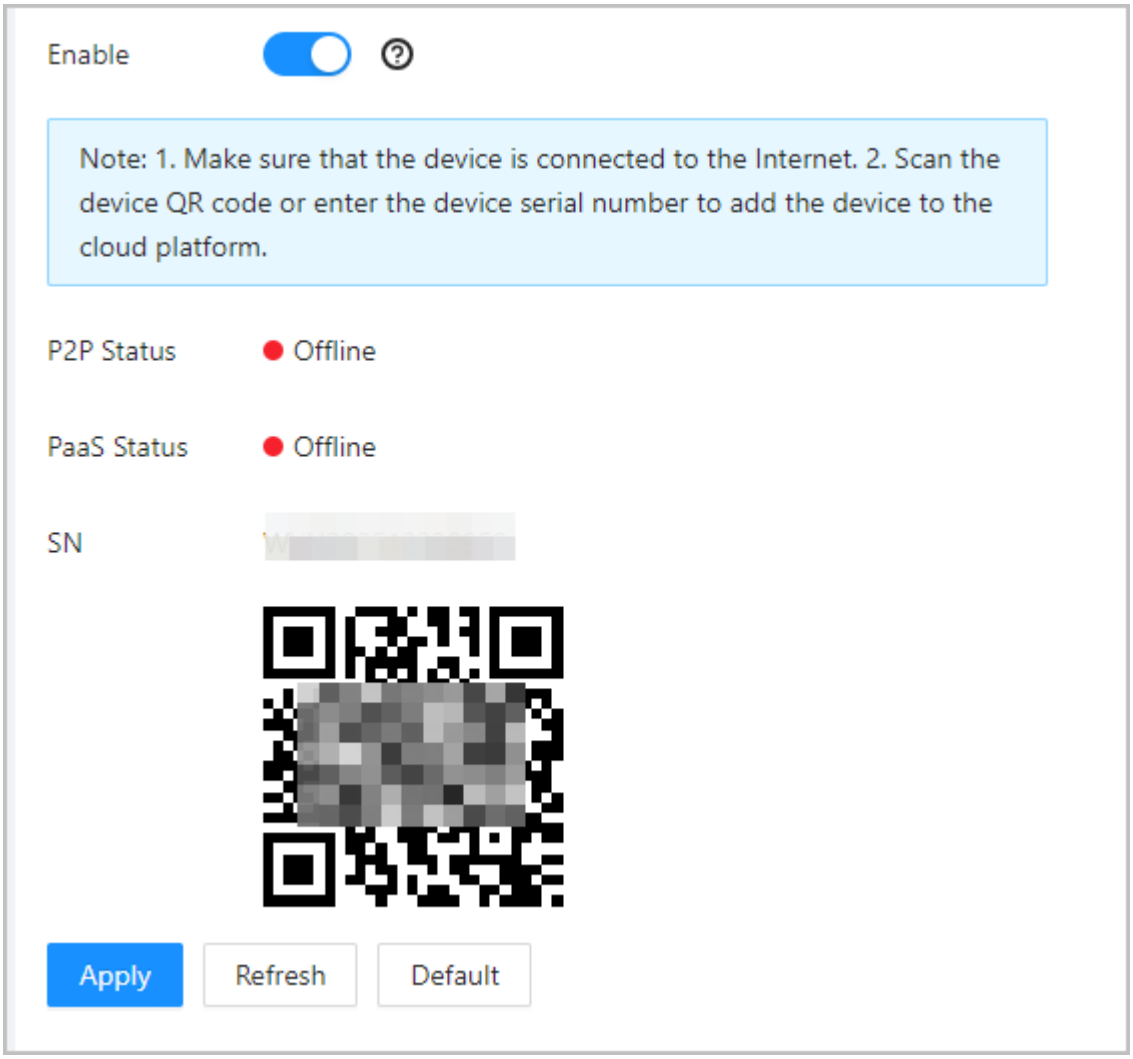
Procedure

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

Step 2 Turn on the cloud service function.

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

Figure 3-53 Cloud service



Step 3 Click **Apply**.

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

3.10.1.7 Configuring SDK Auto Registration

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

Background Information

The auto registration only supports SDK.

Procedure

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

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

Figure 3-54 Auto Registration

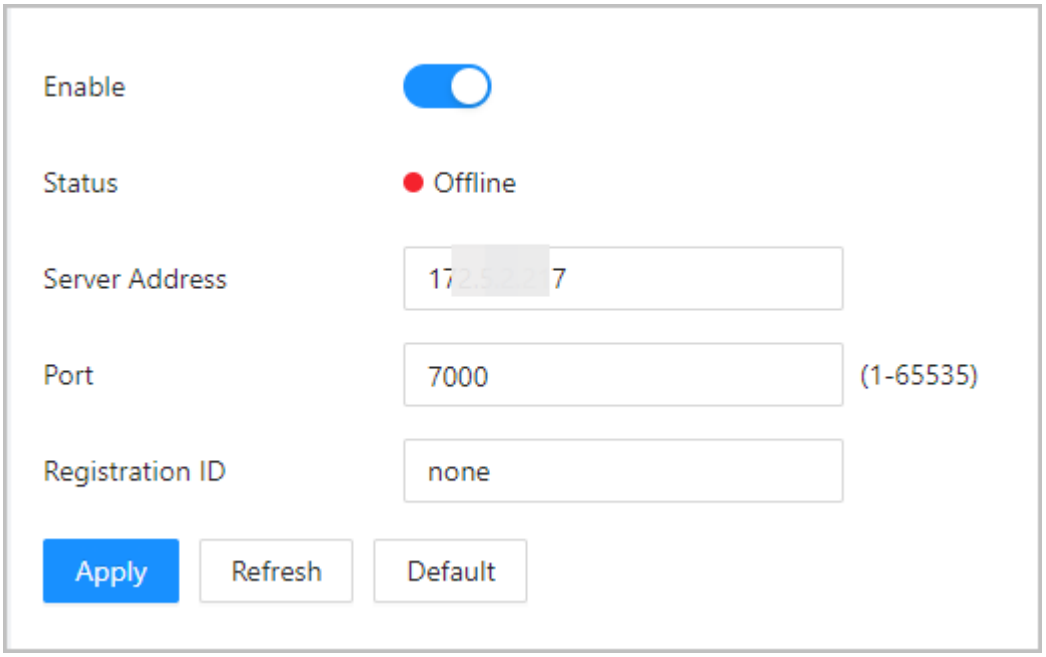


Table 3-34 Automatic registration description

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

Step 3 Click **Apply**.

3.10.1.8 Configuring CGI Auto Registers

Connect to a third-party platform through CGI protocol.

Background Information

Only supports IPv4.

Procedure

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

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

Step 3 Click , and then configure parameters.

Figure 3-55 CGI auto registration

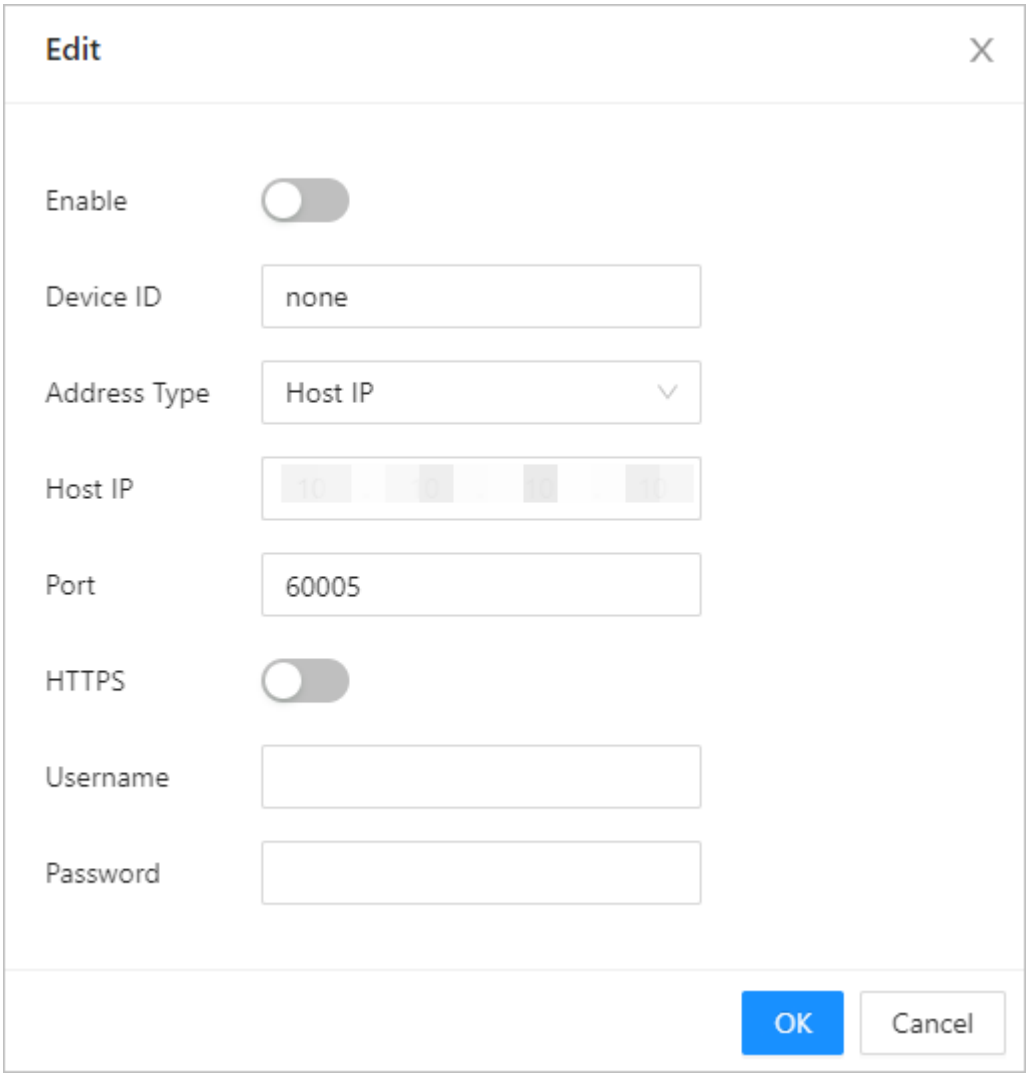


Table 3-35 Automatic registration description

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/Password	Enter the username and password of the device.

Step 4 Click **OK**.

3.10.1.9 Configuring Auto Upload

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

Procedure

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

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

When the user information is updated or new users are added, the Device will automatically push user information to the management platform.

Step 3 Enable HTTP upload mode.

Step 4 Click **Add**, and then configure parameters.

Figure 3-56 Automatic upload

Table 3-36 Parameters description

Parameter	Description
IP/Domain Name	The IP or domain name of the management platform.
Port	The port of the management platform.
HTTPS	Access the management platform through HTTPS. HTTPS secures communication over a computer network.
Authentication	Enable account authentication when you access the management platform. Login username and password are required.
Event Type	Select the type of event that will be pushed to the management platform. ● Before you use this function, enable **Push Person Info**. ● Person information can only be pushed to one management platform and unlock records can be pushed to multiple management platforms.

Step 5 Click **Apply**.

3.10.2 Bluetooth Settings

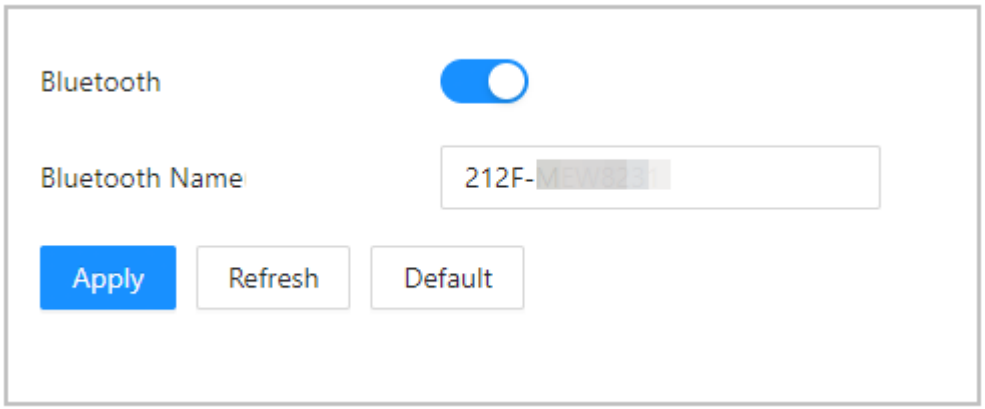
Configure the Bluetooth function of the Device. This function is only available on select models.

Procedure

Step 1 Select **Communication Settings** > **Bluetooth Setting**.

Step 2 Enable or turn off **Bluetooth**, and then configure Bluetooth name.

Figure 3-57 Bluetooth



Step 3 Click **Apply**.

Results

You can unlock the door through the Bluetooth through the DMSS app. For details, see"2.2.5 Unlocking by Bluetooth" .

3.10.3 Configuring RS-485

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

Procedure

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

Step 2 Configure the parameters.

Figure 3-58 Configure parameters

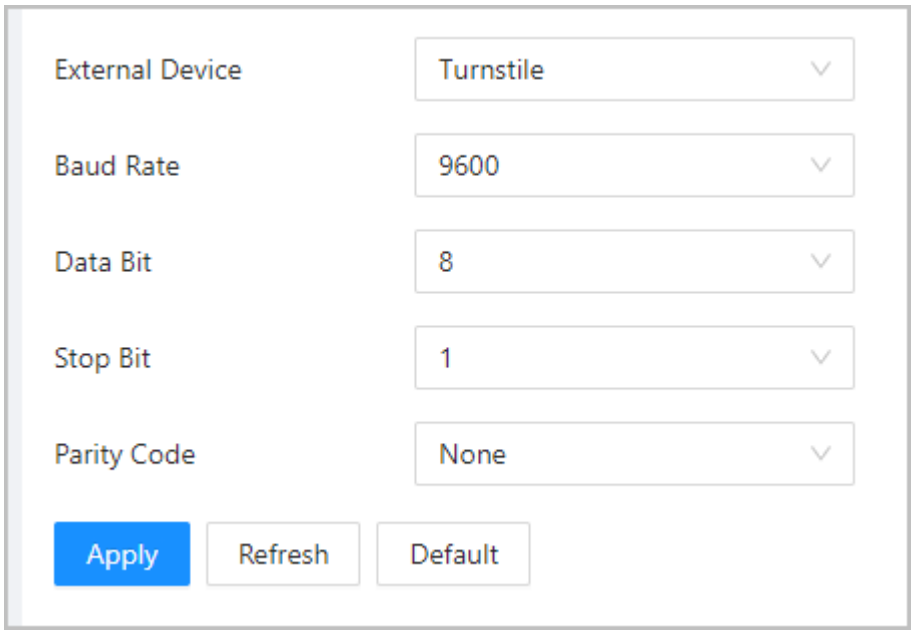


Table 3-37 Configure the RS-485 parameters

Parameter	Description
External Device	• Access Controller Select **Access Controller** when the Device functions as a card reader, and sends data to other external access controllers to control access. Output Data type: ◇ Card Number: Outputs data based on card number when users swipe card to unlock door; outputs data based on user's first card number when they use other unlock methods. ◇ No.: Outputs data based on the user ID. • Card Reader: The Device functions as an access controller, and connects to an external card reader. • Reader (OSDP): The Device is connected to a card reader based on OSDP protocol. • Door Control Security Module: The door exit button, lock and fire linkage is not effective after the security module is enabled. • Turnstile: When the Device connects to a turnstile, and the access controller board of the turnstile connects to an external QR code module or card swiping module, the board will transmit the verification data to the turnstile. • Lock extension mode: When the Access Controller is connected to external lock extension module, if you select **Lock Extension Module**, the local lock is unlocked after you verify the identification on the local device, and the extension lock is unlocked after you verify the identification on the external card reader. After you select **Lock Extension Module** , you can select channel 2 on the **Access Control Parameters** and **Alarm** page on the webpage of the Access Controller.
Data Bit	The number of bits used to transmit the actual data in a serial communication. It represents the binary digits that carry the information being transmitted.
Stop Bit	A bit sent after the data and optional parity bits to indicate the end of a data transmission. It allows the receiver to prepare for the next byte of data and provides synchronization in the communication protocol.
Parity Code	An additional bit sent after the data bits to detect transmission errors. It helps verify the integrity of the transmitted data by ensuring a specific number of logical high or low bits.

Step 3 Click **Apply**.

3.10.4 Configuring Wiegand

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

Procedure

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

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

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

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

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

Figure 3-59 Wiegand output

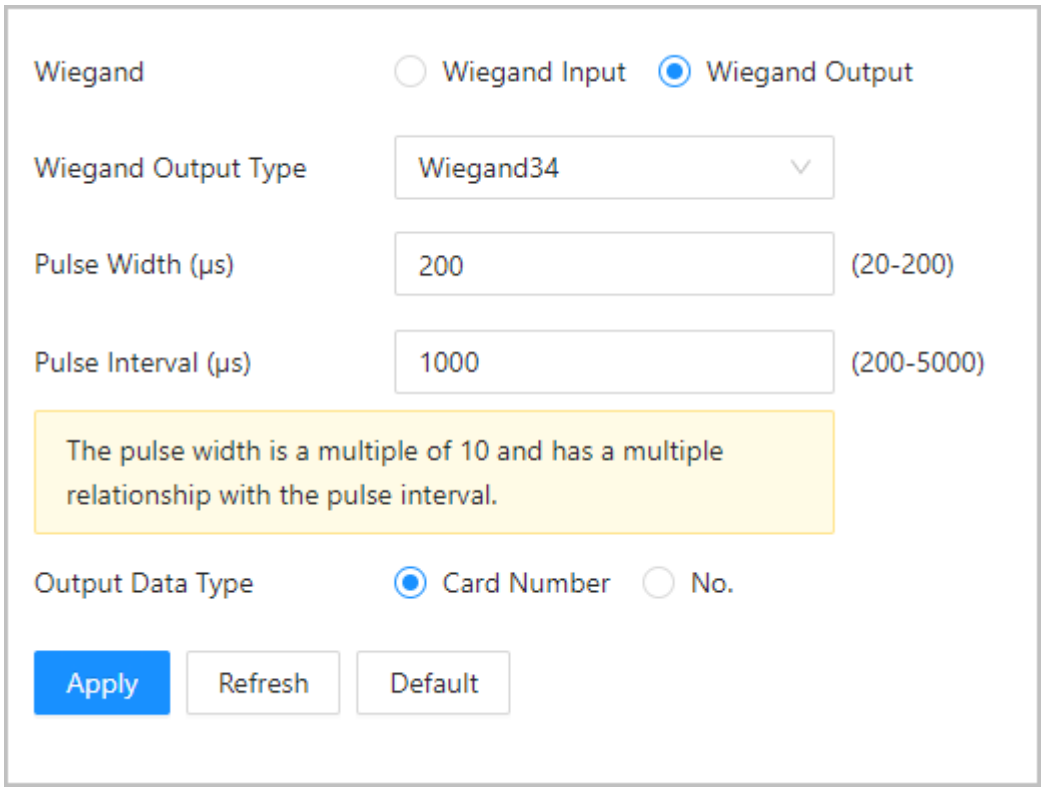


Table 3-38 Description of Wiegand output

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

Step 3 Click **Apply**.

3.11 Management Center

3.11.1 One-click Diagnosis

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

Procedure

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

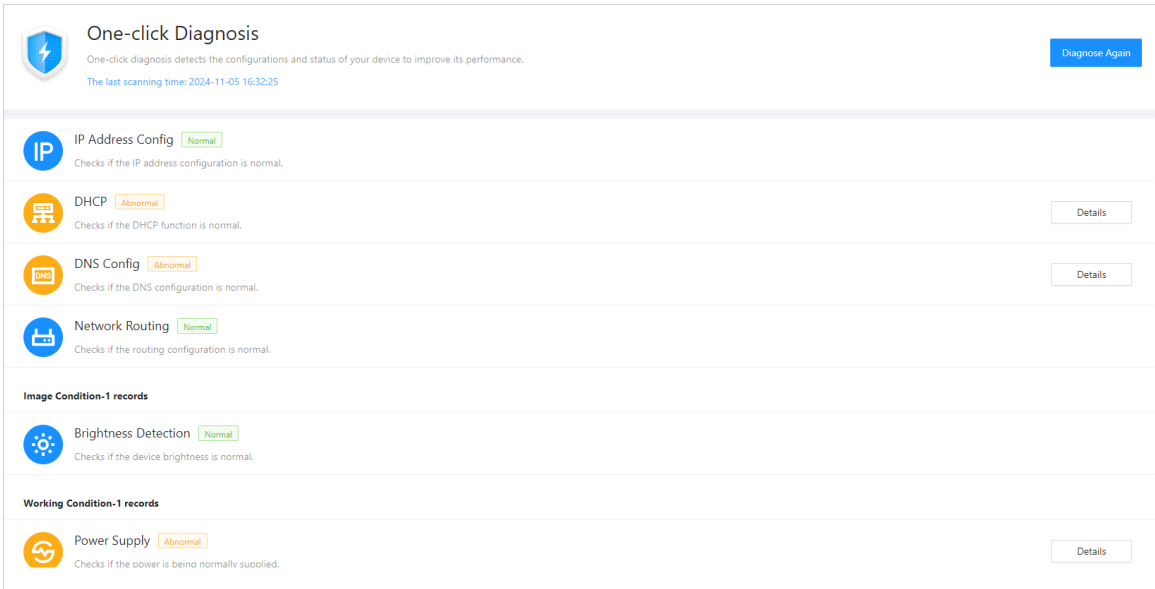
Step 2 Click **Diagnose**.

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

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

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

Figure 3-60 One-click diagnosis



3.11.2 System Information

3.11.2.1 Viewing Version Information

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

3.11.2.2 Viewing Legal Information

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

3.11.3 Data Capacity

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

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

3.11.4 Viewing Logs

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

3.11.4.1 System Logs

Search for and view system logs.

Procedure

Step 1 Log in to the webpage.

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

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

Related Operations

- click **Export** to export the searched logs to your local computer.
- Click **Encrypt Log Backup**, and then enter a password. The exported file can be opened only after entering the password.
- Click to view details of a log.

3.11.4.2 Unlock Records

Search for unlock records and export them.

Procedure

Step 1 Log in to the webpage.

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

Store Unlock Records is enabled by default. After it is turned off, unlock records cannot be stored in the Device.

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

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

Related Operations

- Click **Export** to export the unlock records to your computer.
- Click to view the collected face image.
- Click to view the face image that is collected during verification.

3.11.4.3 Call History

View call logs.

Procedure

Step 1 Log in to the webpage.

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

3.11.4.4 Alarm Logs

View alarm logs.

Procedure

Step 1 Log in to the webpage.

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

Step 3 Select the type and the time range.

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

3.11.4.5 USB Management

Export user information from/to USB.

Procedure

Step 1 Log in to the webpage.

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

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

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

3.11.5 Maintenance Center

3.11.5.1 Configuration Management

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

3.11.5.1.1 Exporting and Importing Configuration Files

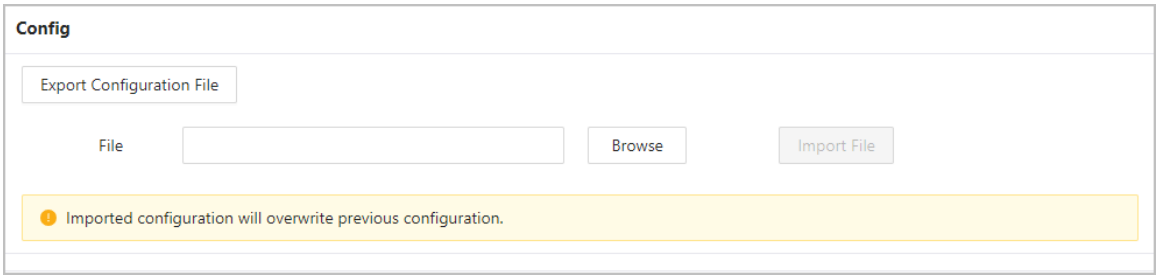
You can import and export the configuration file for the Device. When you want to apply the same configurations to multiple devices, you can import the configuration file to them.

Procedure

Step 1 Log in to the webpage.

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

Figure 3-61 Configuration management



Step 3 Export or import configuration files.

- Export the configuration file.

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

  The IP will not be exported.

- Import the configuration file.

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

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

3.11.5.1.2 Restoring the Factory Default Settings

Procedure

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

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

Step 2 Restore to the factory default settings if necessary.

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

3.11.5.2 Maintenance

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

Procedure

Step 1 Log in to the webpage.

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

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

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

3.11.6 Updating the System

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

3.11.6.1 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.

3.11.6.2 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.

3.11.7 Advanced Maintenance

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

3.11.7.1 Exporting

Procedure

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

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

3.11.7.2 Packet Capture

Packet Capture

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

Figure 3-62 Packet capture

2. Enter the IP address, click .

   changes to .

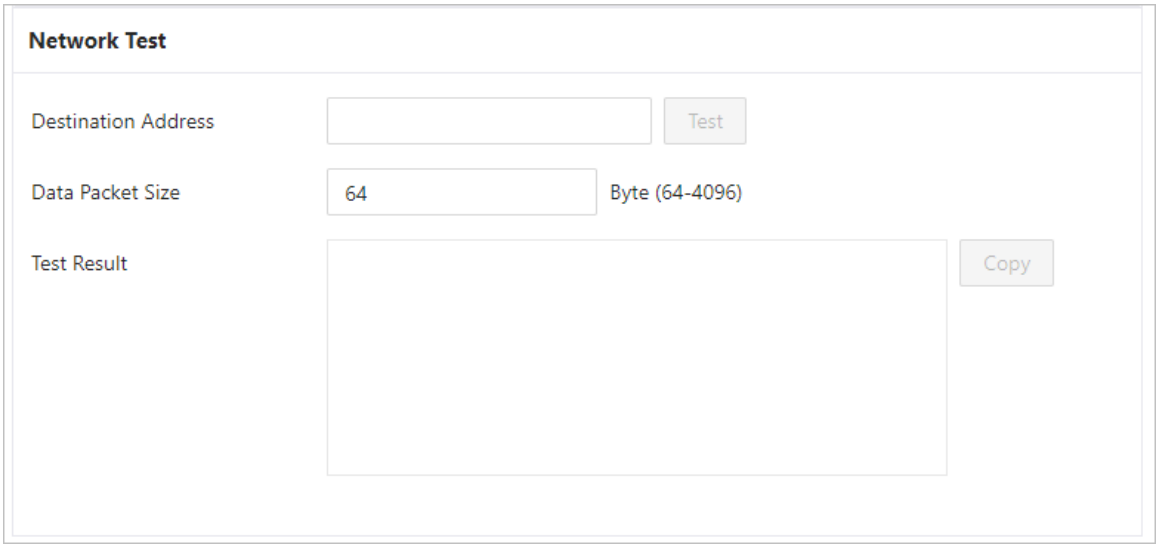
3. After you acquired enough data, click .

   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 3-63 Network test



3. Click **Test**.

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

3.12 (Optional) Security Settings

3.12.1 Security Status

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

Background Information

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

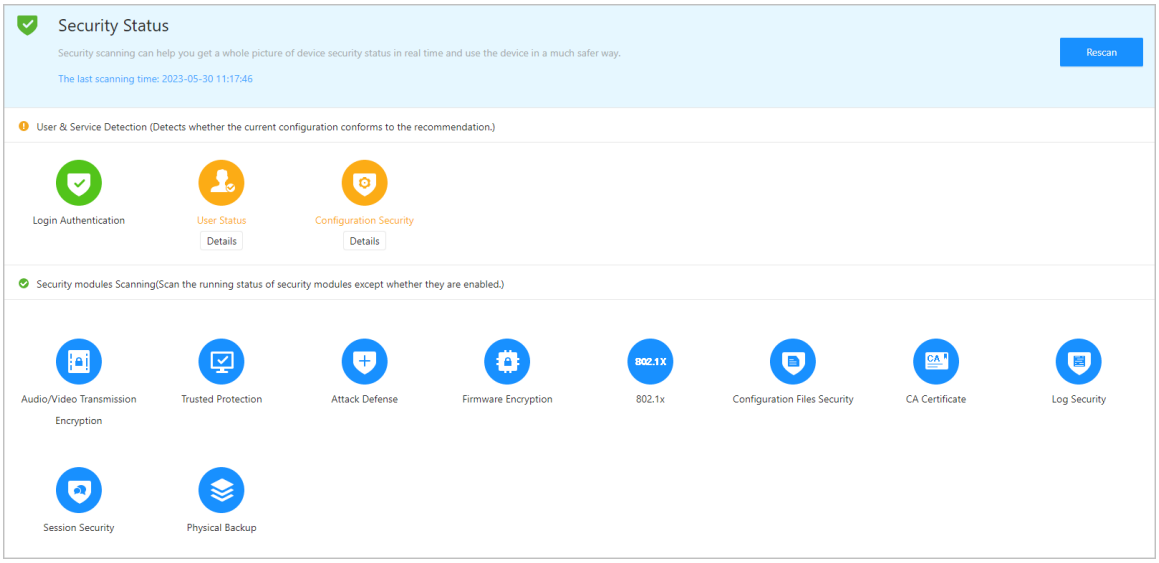
Procedure

Step 1 Select > **Security Status**.

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

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

Figure 3-64 Security Status



Related Operations

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

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

3.12.2 Configuring HTTPS

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

Procedure

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

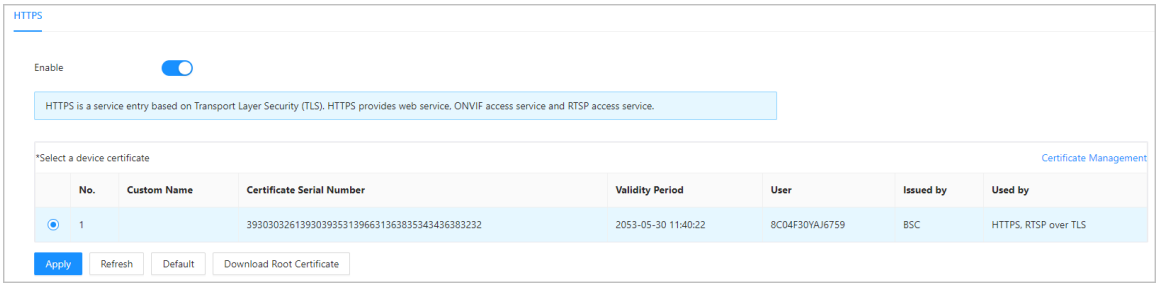
Step 2 Turn on the HTTPS service.

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

Step 3 Select the certificate.

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

Figure 3-65 HTTPS



Step 4 Click **Apply**.

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

3.12.3 Attack Defense

3.12.3.1 Configuring Firewall

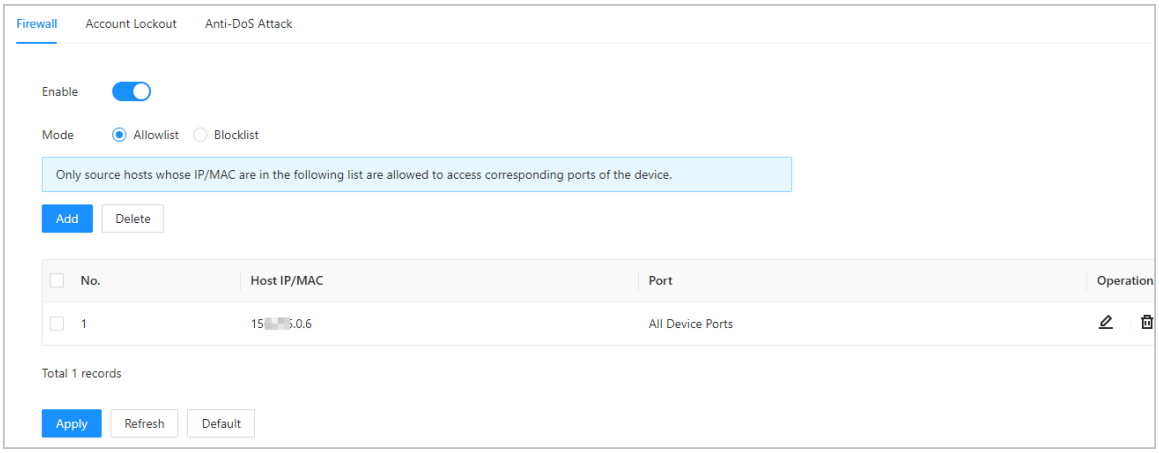
Configure firewall to limit access to the Device.

Procedure

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

Step 2 Click to enable the firewall function.

Figure 3-66 Firewall

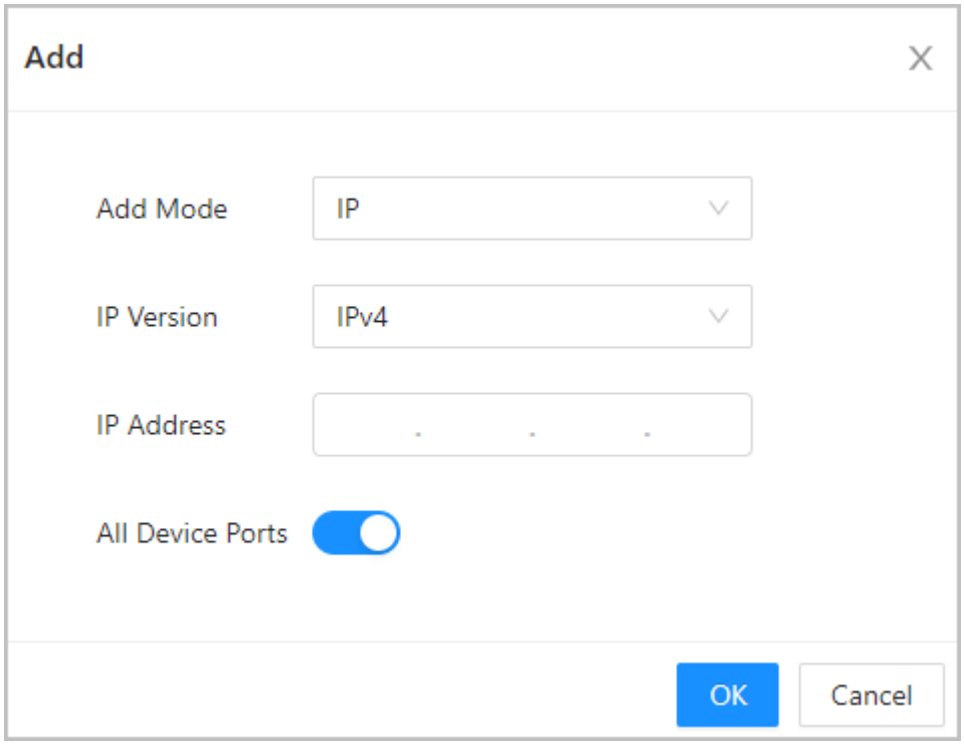


Step 3 Select the mode: **Allowlist** and **Blocklist**.

- **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 3-67 Add IP information



Step 5 Click **OK**.

Related Operations

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

3.12.3.2 Configuring Account Lockout

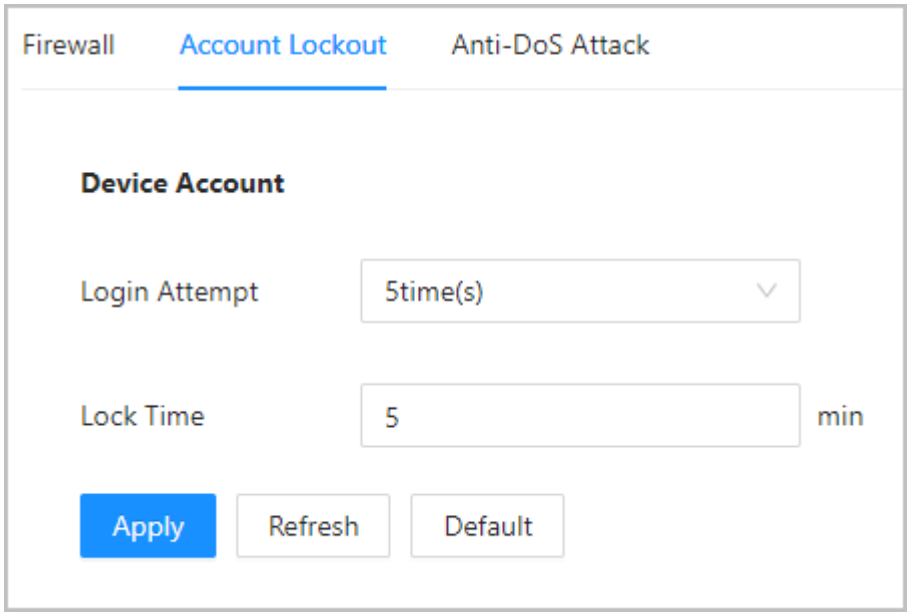
If the incorrect password is entered for a defined number of times, the account will be locked.

Procedure

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

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

Figure 3-68 Account lockout



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

Step 3 Click **Apply**.

3.12.3.3 Configuring Anti-DoS Attack

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

Procedure

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

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

Figure 3-69 Anti-DoS attack

Step 3 Click **Apply**.

3.12.4 Installing Device Certificate

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

3.12.4.1 Creating Certificate

Create a certificate for the Device.

Procedure

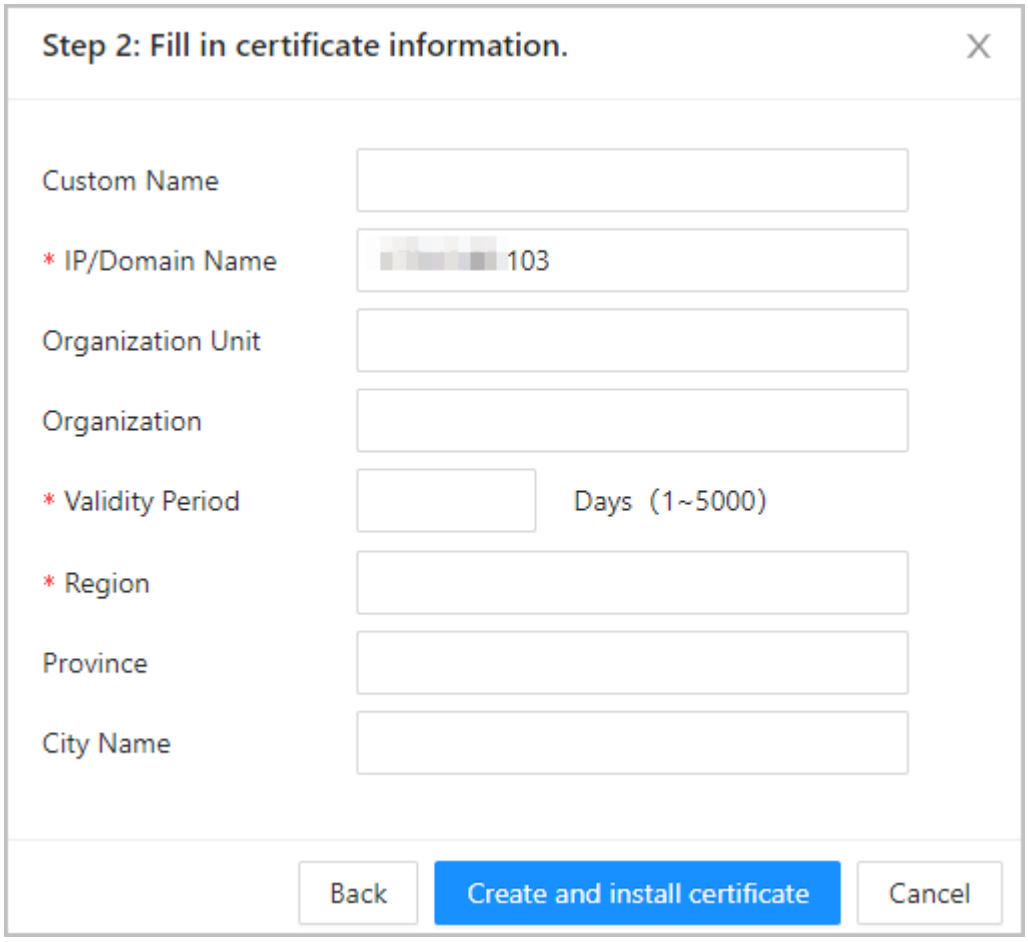
Step 1 Select > **CA Certificate** > **Device Certificate**.

Step 2 Select **Install Device Certificate**.

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

Step 4 Enter the certificate information.

Figure 3-70 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.

3.12.4.2 Applying for and Importing CA Certificate

Import the third-party CA certificate to the Device.

Procedure

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

Step 2 Click **Install Device Certificate**.

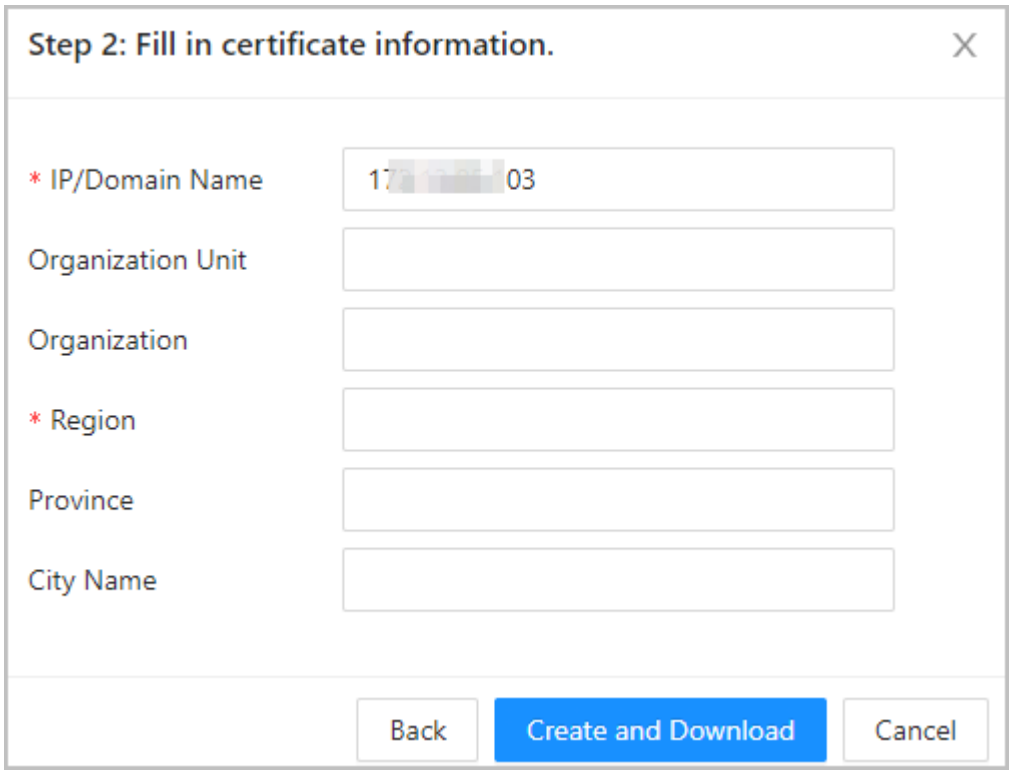
Step 3 Select **Apply for CA Certificate and Import (Recommended)** , and click **Next**.

Step 4 Enter the certificate information.

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

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

Figure 3-71 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.

3.12.4.3 Installing Existing Certificate

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

Procedure

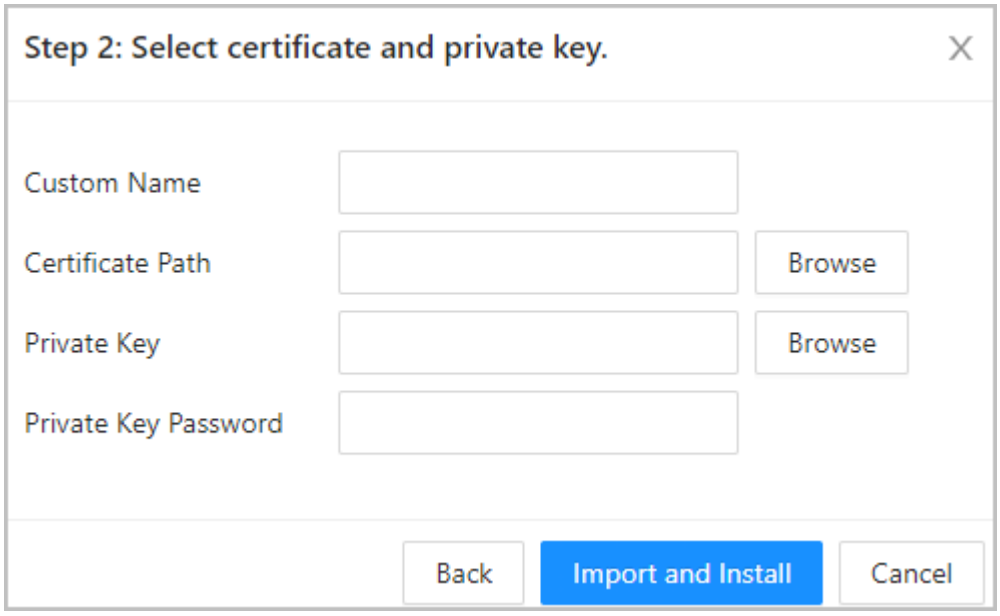
Step 1 Select **Security** > **CA Certificate** > **Device Certificate**.

Step 2 Click **Install Device Certificate**.

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

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

Figure 3-72 Certificate and private key



Step 5 Click **Import and Install**.

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

Related Operations

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

3.12.5 Installing the Trusted CA Certificate

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

Background Information

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

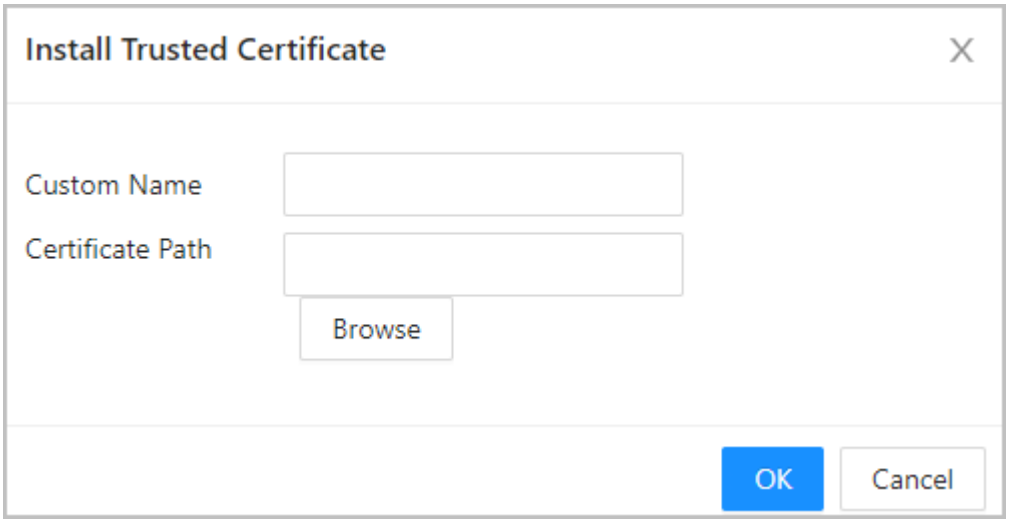
Procedure

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

Step 2 Select **Install Trusted Certificate**.

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

Figure 3-73 Install the trusted certificate



Step 4 Click **OK**.

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

Related Operations

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

3.12.6 Data Encryption

Procedure

Step 1 Select > **Data Encryption**.

Step 2 Configure the parameters.

Figure 3-74 Data encryption

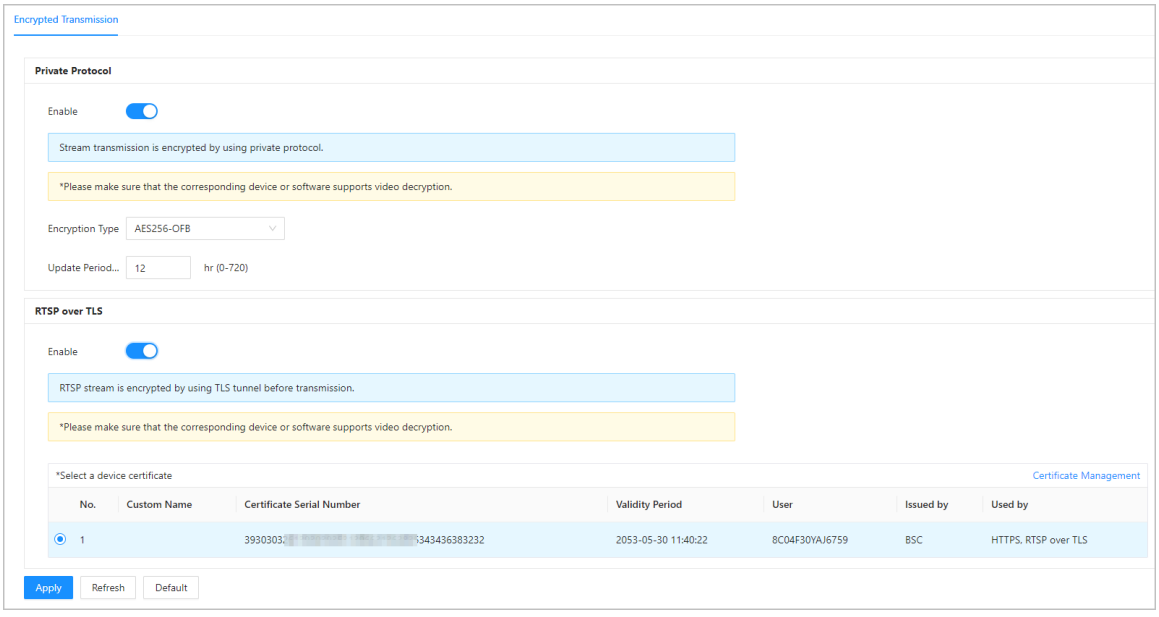


Table 3-39 Data encryption description

	Parameter	Description
Private Protocol	Enable	Streams are encrypted during transmission through private protocol.
	Encryption Type	Keep it as default.
	Update Period of Secret Key	Ranges from 0 h -720 h. 0 means never update the secret key.
RTSP over TLS	Enable	RTSP stream is encrypted during transmission through TLS tunnel.
	Certificate Management	Create or import certificate.

3.12.7 Security Warning

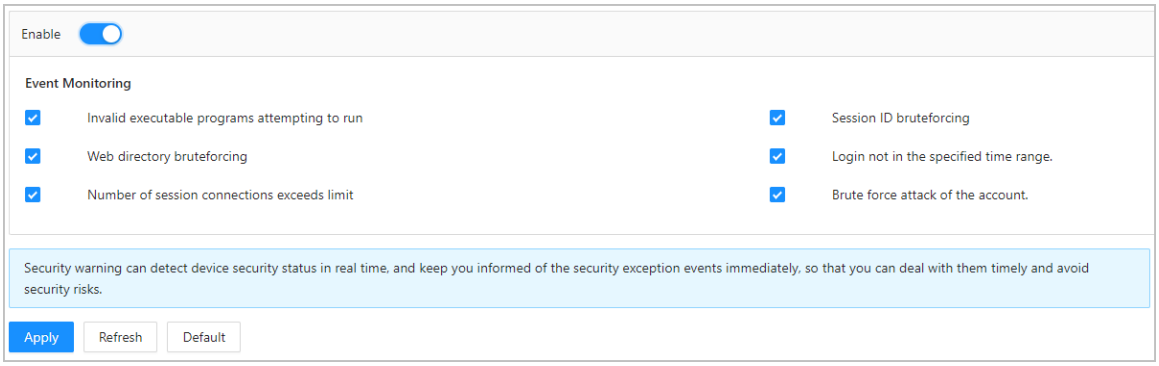
Procedure

Step 1 Select > **Security Warning**.

Step 2 Enable the security warning function.

Step 3 Select the monitoring items.

Figure 3-75 Security warning



Step 4 Click **Apply**.

3.12.8 Security Authentication

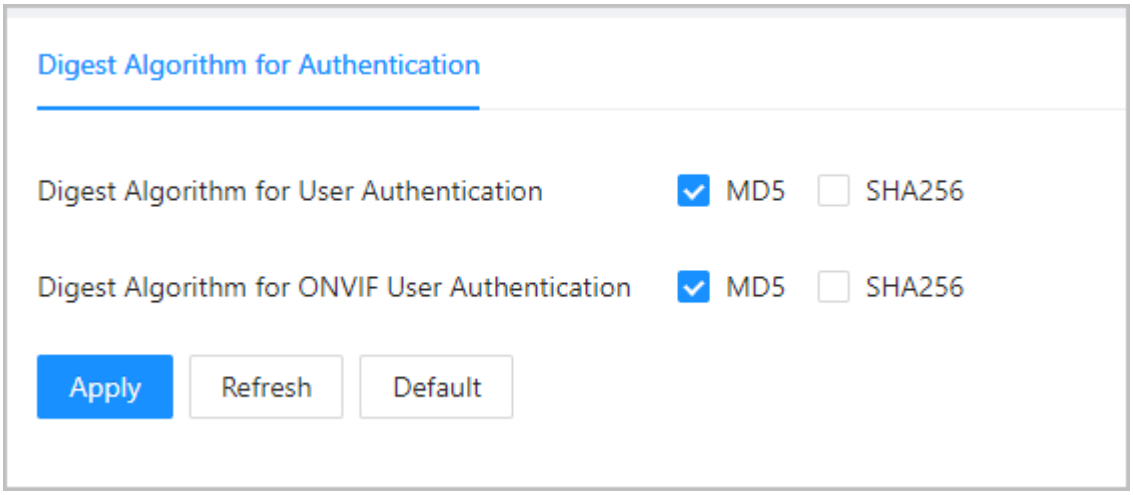
Procedure

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

Step 2 Select a message digest algorithm.

Step 3 Click **Apply**.

Figure 3-76 Security Authentication



4 Phone Operations

4.1 Initialization

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

Procedure

Step 1 Power on the Access Controller.

Step 2 The Wi-Fi hotspot is enabled by default when the device is not initialized. 30 minutes after the device enters the initialization screen, the Wi-Fi hotspot on your phone automatically turns off. The hotspot name is *DAP+product serial number*.

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

Step 4 Tap **Start Initialization**.

Step 5 Select the language.

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

- The password must consist of 8 to 32 non-blank characters and contain at least two types of the following characters: upper case, lower case, numbers, and special characters (excluding ' " ; : &). Set a high-security password by following the password strength prompt.
- Keep the password safe after initialization and change the password regularly to improve security.
- If you want to reset the administrator password by scanning the QR code, you need the linked email address to receive the security code.

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

4.2 Logging in to the Webpage

Prerequisites

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

Procedure

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

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

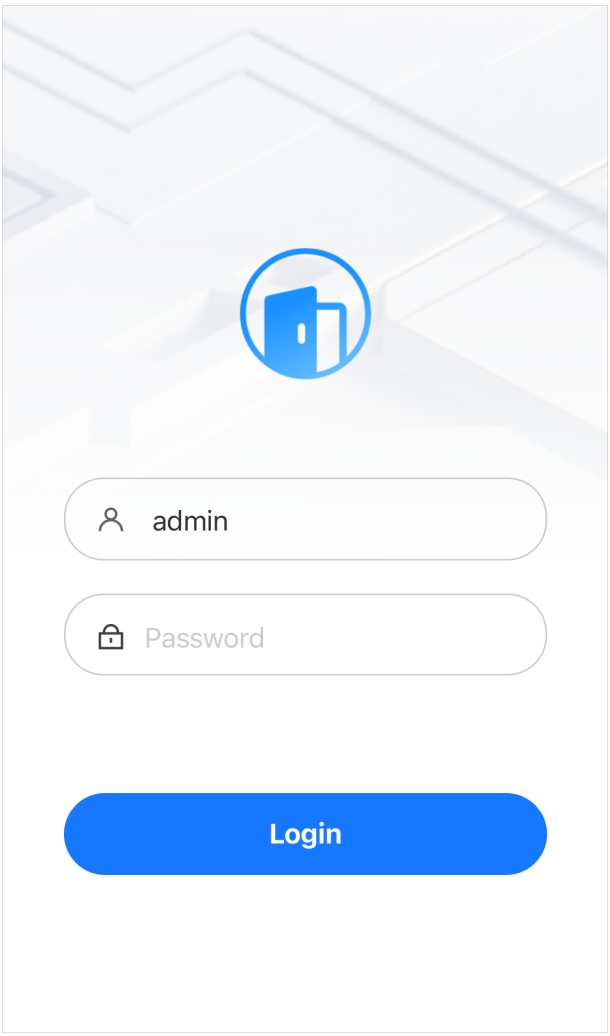
- The phone and the Device are in the same LAN. Open the browser on the phone, and then enter the IP address.
- The phone and the Device are in the same LAN. Scan the QR code through **Communication Settings** > **Network Settings** > **Wi-Fi** on the webpage of your phone.
- You can also select **Communication Settings** > **Network Settings** > **Wi-Fi AP** to go to the main menu.

Step 2 Enter the user name and password.

Click next to the password to view it.

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

Figure 4-1 Login page



Step 3 Tap **Login**.

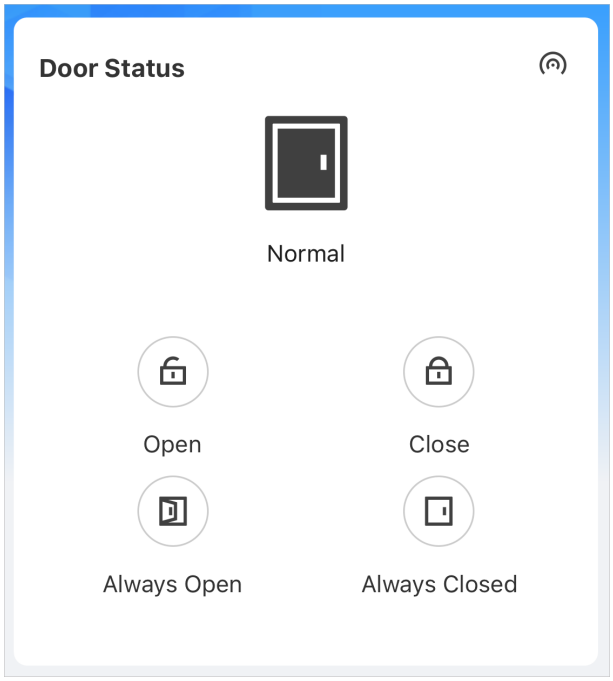
4.3 Home Page

The home page is displayed after you successfully log in.

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

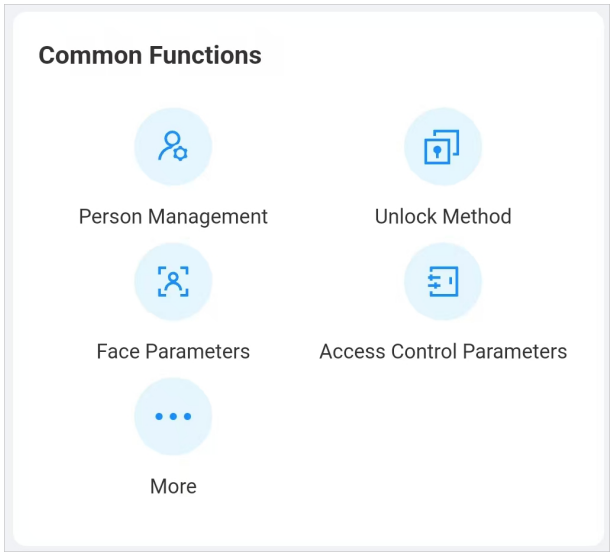
  The product document is available on select models.
- The **Door Status** area displays the status of the door. You can remotely open or close the door. You can also configure the door status as **Always Open** or **Always Closed**.

Figure 4-2 Door status



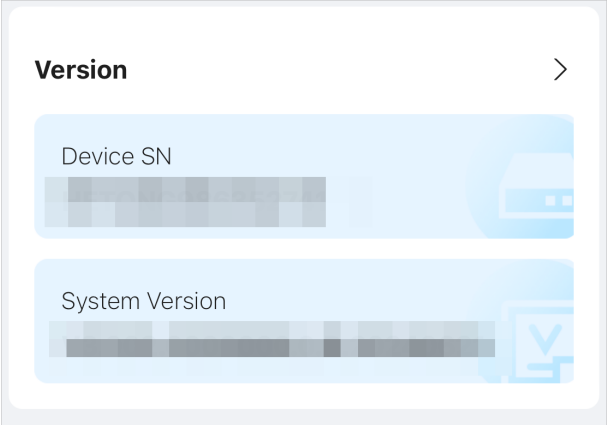
- The **Common Functions** area displays the configuration menu of the Device. Tap **More** to view all the configuration menus.

Figure 4-3 Common functions



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

Figure 4-4 Version



4.4 Person Management

Add the person and configure the permissions.

Procedure

Step 1 Log in to the webpage.

Step 2 Tap **Person Management** , and then tap **+**.

Step 3 Configure user information.

Figure 4-5 Add the person (1)

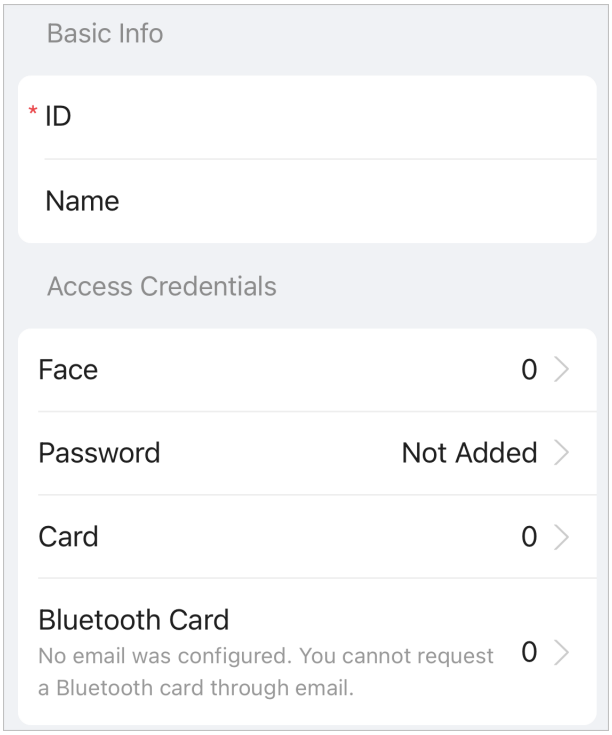


Figure 4-6 Add the person (2)

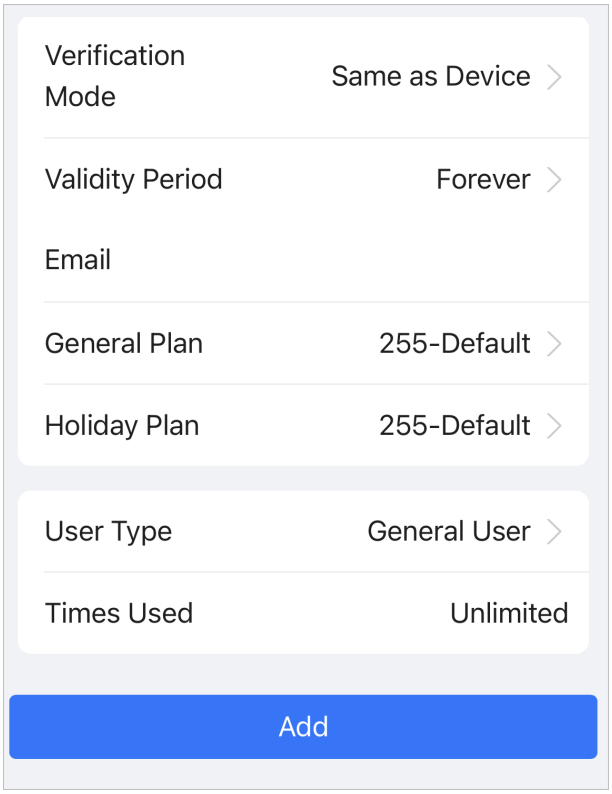


Table 4-1 Parameters description

Parameter	Description
ID	The user ID is like employee ID, which can be numbers, letters, and their combinations, and the maximum length of the number is 30 characters.
Name	The name can contain up to 32 characters (including numbers, symbols, and letters).
Face	Supports uploading the face image or take the photo. Each person can only add up to 2 face images. You can view or delete the face image after you upload it. The face image is in jpg, jpeg, png format.
Password	Configure the user password. The maximum length of the password is 8 digits. The duress password is the unlock password + 1. For example, if the user password is 12345, the duress password will be 12346. A duress alarm will be triggered when a duress password is used to unlock the door. You need to connect a external collector to use this function.

Parameter	Description
Card	Tap **Add**, manually enter the card number or swipe the card in the card swiping area of the Device. A user can register up to 5 cards at most. After adding successfully, tap the added card, you can change the card number, configure the card as the duress card or delete the card. If you turn on the duress alarm, an alarm will be triggered if a duress card is used to unlock the door. One user can only set one duress card.
Bluetooth Card	Bluetooth is only available on select models. You can select **Request through Email** or **Request through Registration Code**. • **Request through Email** : Suitable for the first time a Bluetooth card is requested. You can request up to 5 Bluetooth cards, and have to use the email that is registered to DMSS. You must have entered your reserved Email before you use the function. 1. Configure the Email that is registered to DMSS. 2. Click **Request through Email**, and then the Bluetooth cards can be requested. • **Request through Registration Code** : Suitable when you already have a Bluetooth card and want to reuse it on another access controller supporting Bluetooth function. 1. Copy the Bluetooth registration code from the DMSS. 2. Click **Request through Registration Code**, and then enter the code. 3. Click **OK**.
Verification Mode	Configure the verification mode for the person. You can use the mode that is the same as the device or customize the mode. • **Same as Device** : The mode is the same as the device. • **Custom** : After you select **Custom**, **Combination Method** and **Unlock Method** are displayed. Select the combination method and unlock methods as needed. ◇ Or: Use one of the selected unlock methods to open the door. ◇ And: Use all the selected unlock methods to open the door. ◇ The customized verification mode is only valid for the local device. It cannot be used in external card readers. ◇ When the customized verification mode is different from the mode of the device, the customized mode takes the priority.
Validity Period	Select from **Custom** and **Forever**. You need to set a date on which the door access permissions of the person will be expired if you select **Custom**.

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

Step 4 Tap **Add**.

4.5 Configuring the System

4.5.1 Viewing Version Information

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

4.5.2 Configuration Management

Procedure

Step 1 Log in to the webpage.

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

Step 3 Restore to the factory default settings if necessary.

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

4.5.3 Maintenance

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

Procedure

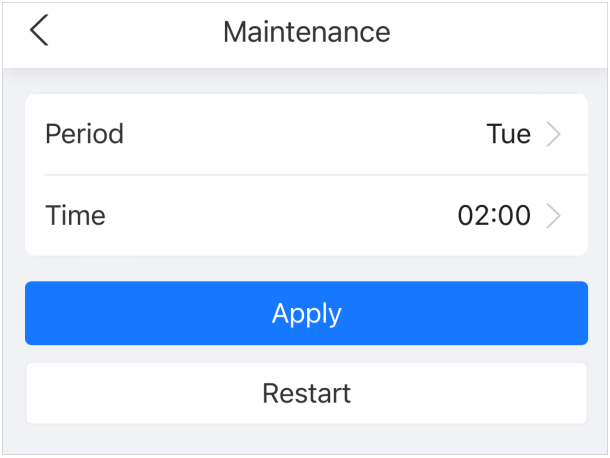
Step 1 Log in to the webpage.

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

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

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

Figure 4-7 Maintenance



4.5.4 Configuring Time

Procedure

Step 1 Log in to the webpage.

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

Step 3 Configure the time.

Figure 4-8 Configure the time parameters

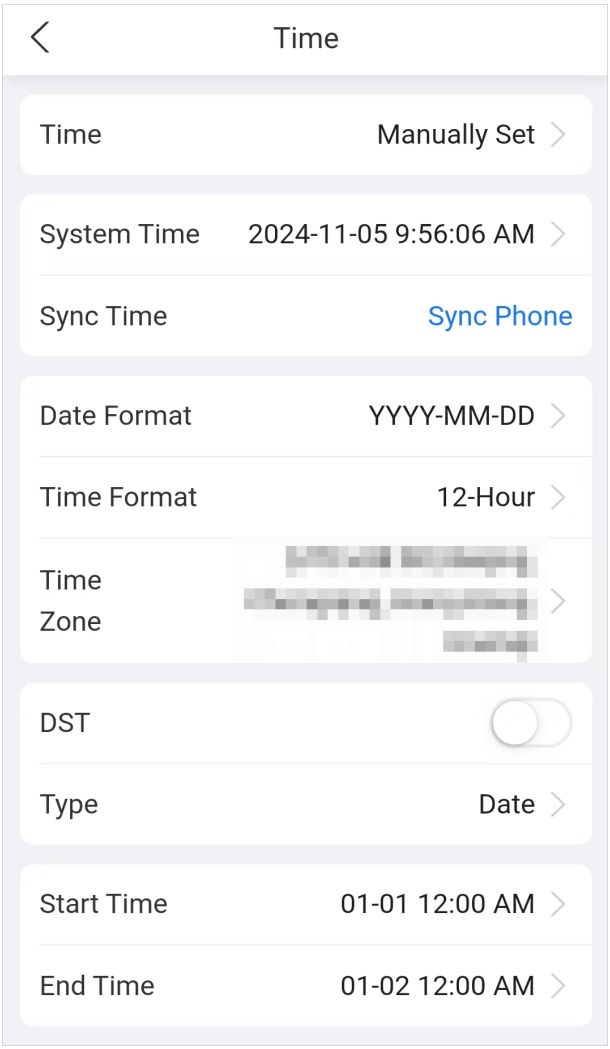


Table 4-2 Time settings description

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

Step 4 Tap **Apply**.

4.5.5 Data Capacity

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

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

4.5.6 Language

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

4.6 Configuring Access Control

4.6.1 Configuring Unlock Methods

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

Procedure

Step 1 Log in to the webpage.

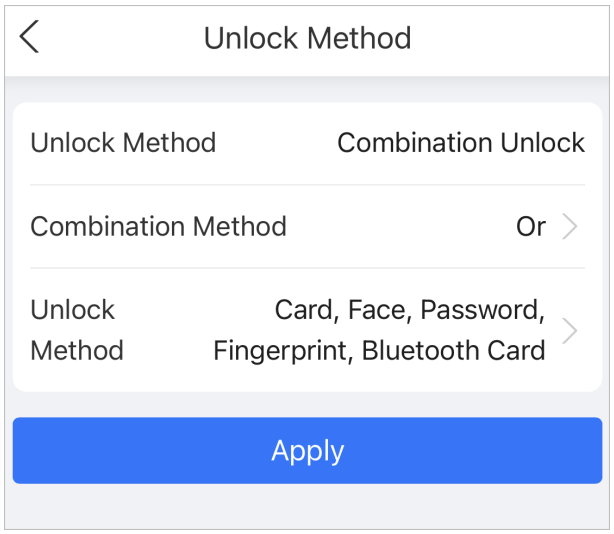
Step 2 Tap **Unlock Method** on the main menu, or select **More** > **Access Control** > **Unlock Method**.

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

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

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

Figure 4-9 Unlock method



4.6.2 Configuring Face Parameters

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

Procedure

Step 1 Log in to the webpage.

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

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

Figure 4-10 Configure the face parameters (1)

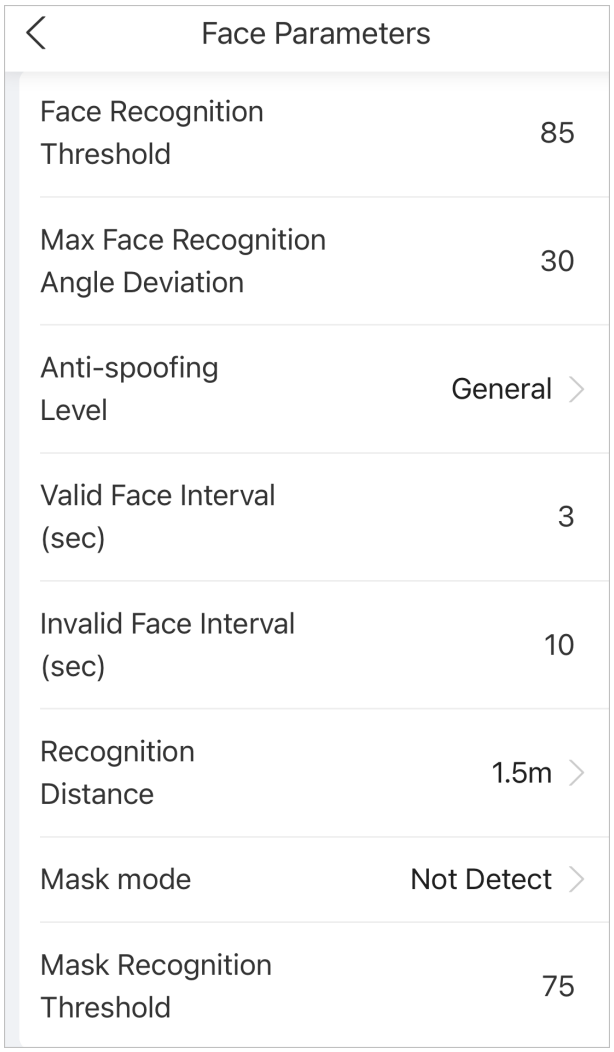


Figure 4-11 Configure the face parameters (2)

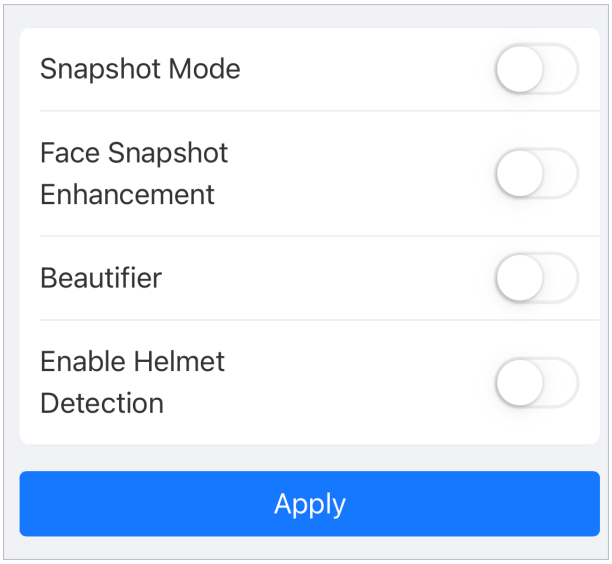


Table 4-3 Description of face parameters

Name	Description
Face Recognition Threshold	Adjust the accuracy level of face recognition. Higher threshold means higher accuracy and lower false recognition rate. When the threshold is too low such as 0, the false recognition rate will be extremely high. Please be advised.
Max Face Recognition Angle Deviation	Set the largest angle that a face can be posed in for face detection. The larger the value, the larger the range for the face angle. If the angle a face is positioned in is not within the defined range, it might not be detected properly.
Anti-spoofing Level	After the function is enabled, it prevents people from being able to use photos, videos, mask and other substitutes to gain unauthorized access. After the function is enabled, face frame is not displayed for non-living verification.
Valid Face Interval (sec)	When the same face remains in front of the lens after the first successful recognition, the Device will perform recognition again for the face after a defined interval.
Invalid Face Interval (sec)	When the same face remains in front of the lens after the first failed recognition, the Device will perform recognition again for the face after a defined interval. If you configure **0**, the face will not be captured and there is no unlock records.
Recognition Distance	The distance between the face and the lens.

Name	Description
Mask Mode	• **Not Detect** : Mask is not detected during face recognition. • **Mask Alert** : Mask is detected during face recognition. If the person is not wearing a mask, the system will remind them to wear a mask, but they will still be allowed access. • **Mask Required** : Mask is detected during face recognition. If a person is not wearing a mask, the system will remind them to wear masks, and access will be denied.
Mask Recognition Threshold	The higher the threshold, the more accurate face recognition will be when a person is wearing a mask, and there will be a lower false recognition rate.
Snapshot Mode	After the function is enabled, low-quality snapshots in the unlock records can be filtered out.
Face Snapshot Enhancement	After the function is enabled, the snapshots in the unlock records are beautified.
Beautifier	Beautify captured face images.
Enable Helmet Detection	Detects safety hats. The door will not unlock if a person does not wear a helmet.

4.6.3 Configuring Access Control Parameters

Procedure

Step 1 Log in to the webpage.

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

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

Figure 4-12 Access control parameters (1)

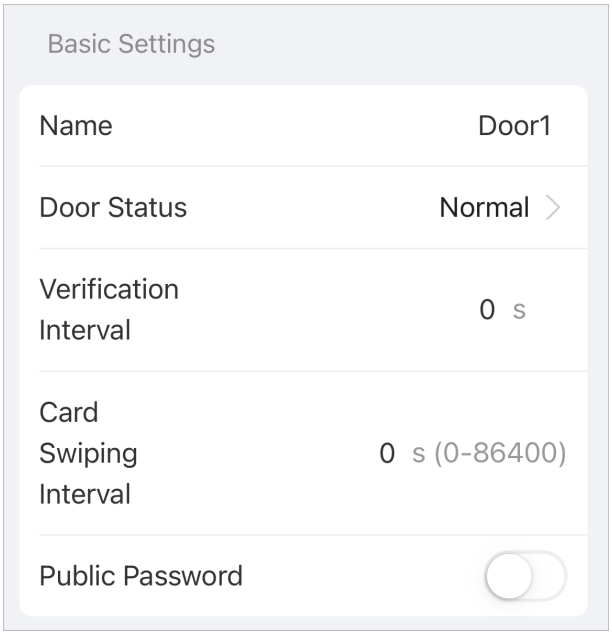


Figure 4-13 Access control parameters (2)

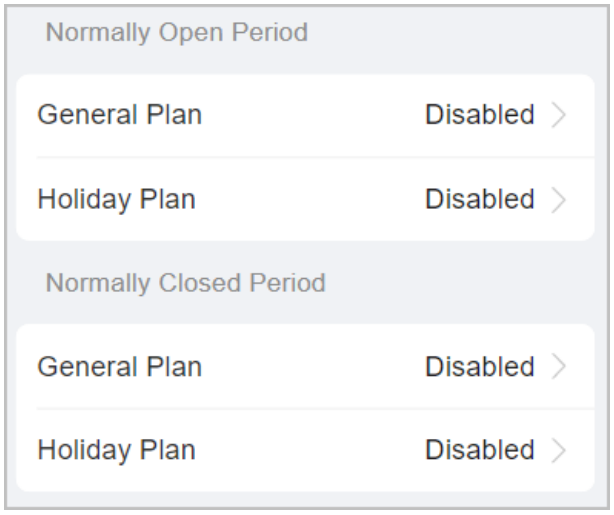


Figure 4-14 Access control parameters (3)

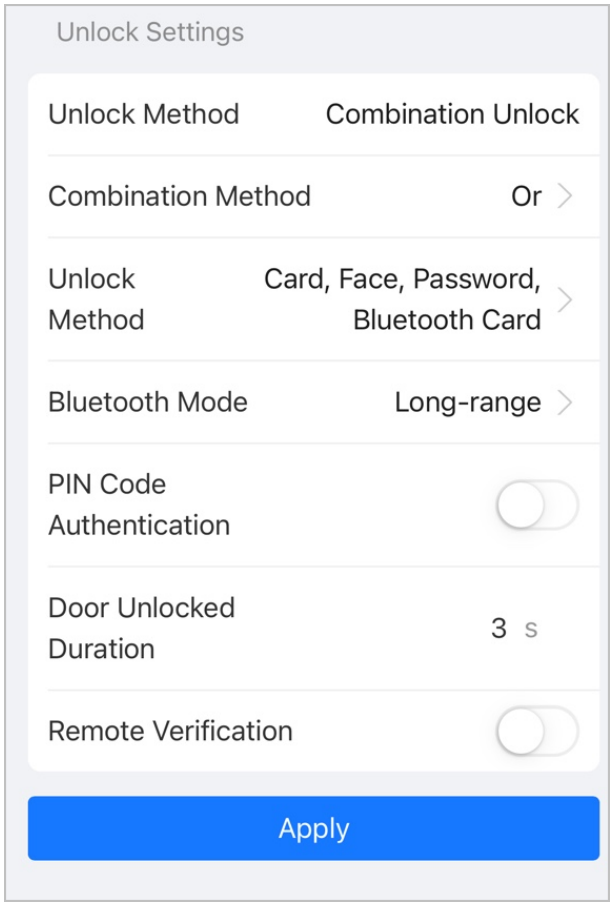


Table 4-4 Description of access control parameters

Parameter		Description
Basic Settings	Name	The name of the door.

Parameter		Description
	Door Status	Set the door status. • Normal: The door will be unlocked and locked according to your settings. • Always Open: The door remains unlocked all the time. • Always Closed: The door remains locked all the time.
	Verification Interval	If you verify your identity multiple times within a set period, only the earliest verification will be considered valid, and the door will not open after the second or later verifications. From the moment the door fails to open, you must wait for the configured verification time interval before attempting to verify your identity again.
	Card Swiping Interval	For first-time verification through card, you can normally unlock the door or perform attendance, and the records are generated. Within the configured period, if you swipe the card for verification again, you cannot unlock the door or perform attendance, and the records are not generated. Please verify the identification after the configured period. The **Card Swiping Interval** takes priority over **Verification Interval**.
	Public Password	After the public password is enabled, configure the password. You can use the public password without entering the user ID to unlock the door. Only one public password is supported for one device.
Normally Open Period	General Plan/ Holiday Plan	When you select **Normal**, you can select a time template from the drop-down list. The door remains open or closed during the defined time. • When normally open period conflicts with normally closed period, normally open period takes priority over normally closed period. • When the general plan conflict with the holiday plan, the holiday plan takes priority over the general plan.
Normally Closed Period	General Plan/ Holiday Plan	
Unlock Settings	Unlock Method	**Combination Unlock** by default.
	Combination Method	• Or: Use one of the selected unlock methods to open the door. • And: Use all the selected unlock methods to open the door.

Parameter		Description
	Unlock Method	Unlock methods might differ depending on the models of product.
	PIN Code Authentication	When PIN code authentication is enabled, you can open the door with just the password. You do not have to enter the user ID if this function is enabled. The remote verification is not supported.
	Bluebooth Mode	Select the Bluebooth mode according to your need.
	Door Unlocked Duration	After a person is granted access, the door will remain unlocked for a defined time for them to pass through. It ranges from 0.2 to 600 seconds.
	Remote Verification	Open the door remotely.

Step 4 Tap **Apply**.

4.6.4 Configuring Alarms

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

Procedure

Step 1 Log in to the webpage.

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

Step 3 (Optional) Select the door channel.

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

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

Figure 4-15 Alarm settings

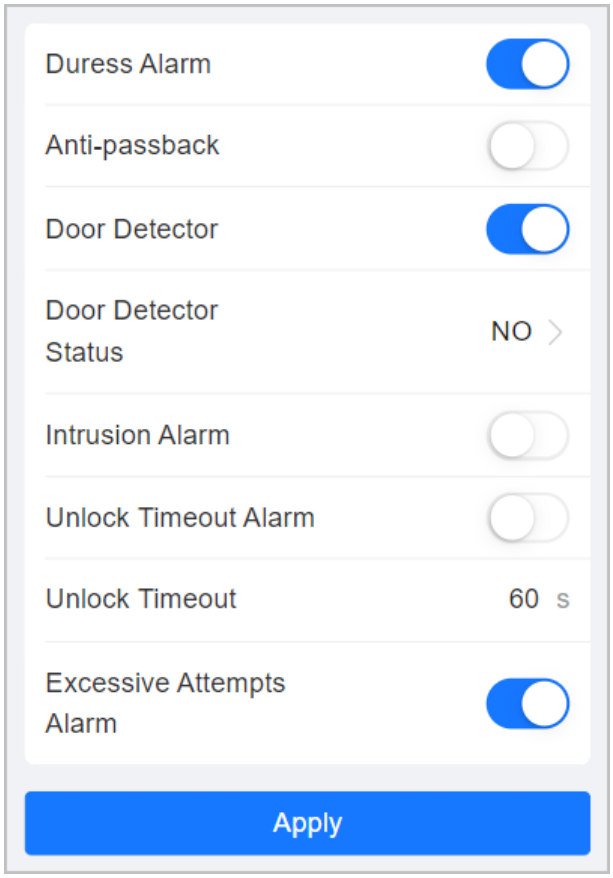


Table 4-5 Description of alarm parameters

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

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

4.6.5 Configuring Alarm Linkages (Optional)

You can configure alarm linkages.

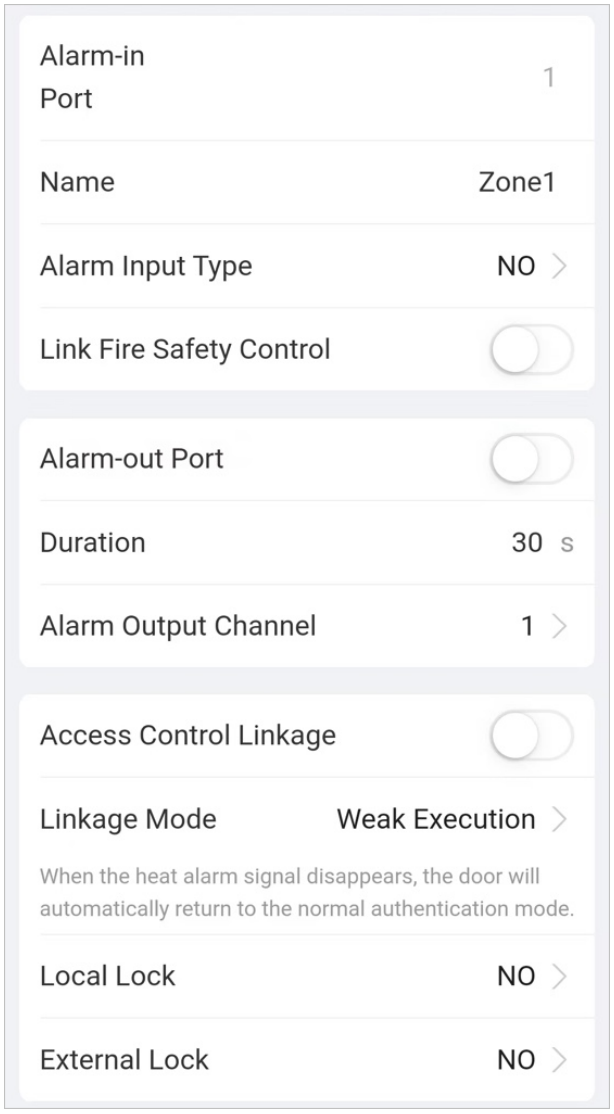
Procedure

Step 1 Log in to the webpage.

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

Step 3 Select the zone to configure alarm.

Figure 4-16 Alarm linkage



Step 4 Create a name for the alarm zone.

Step 5 Enable **Link Fire Safety Control**, and select a type for the alarm input device.

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

Step 6 If you want to link access control when the fire alarm is triggered, enable **Access Control Linkage**.

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

Step 7 Select a linkage mode.

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

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

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

Step 9 Tap **OK**.

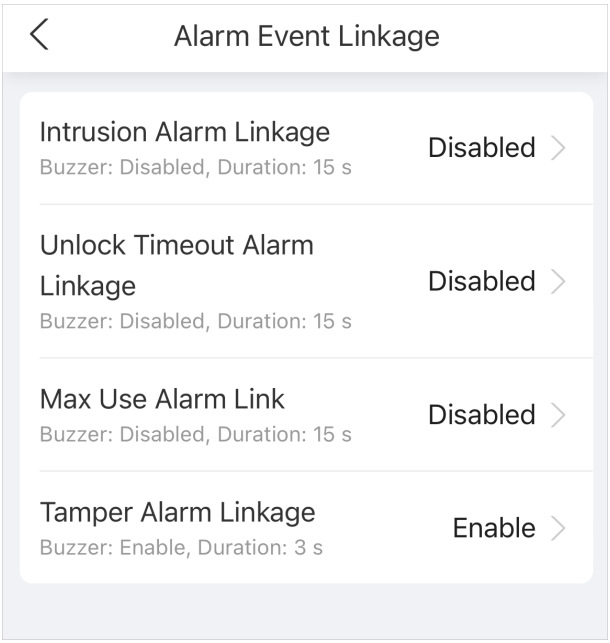
4.6.6 Configuring Alarm Event Linkage

Procedure

Step 1 Log in to the webpage.

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

Figure 4-17 Alarm event linkage



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

Table 4-6 Alarm event linkage

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

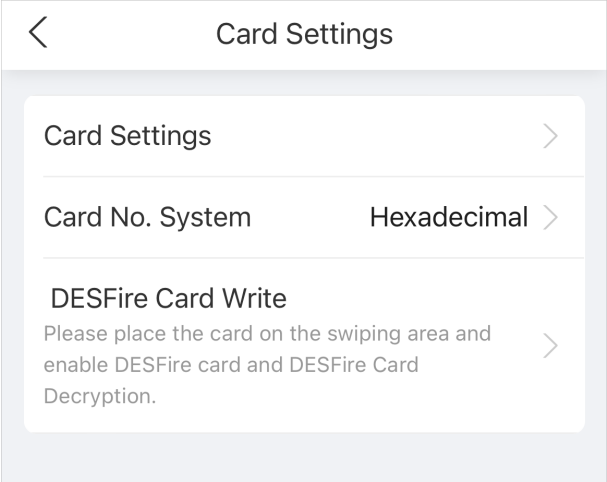
4.6.7 Configuring Card Settings

Procedure

Step 1 Log in to the webpage.

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

Figure 4-18 Card settings



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

Figure 4-19 Card parameters

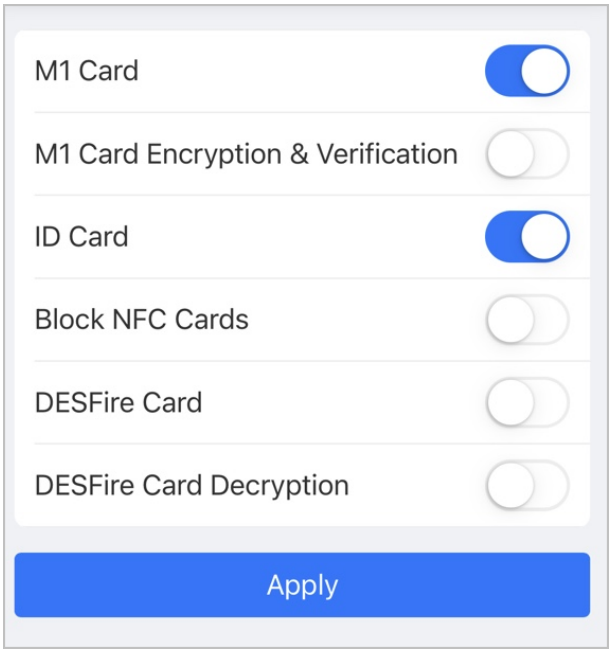


Table 4-7 Card parameters description

Parameter	Description
M1 Card	The M1 card can be read when this function is enabled.
M1 Card Encryption & Verification	Only the encrypted IC card can be read when this function is enabled. Make sure **M1 Card** is enabled.

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

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

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

Step 5 Tap **DESFire Card Write**.

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

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

4.6.8 Privacy Setting

Procedure

Step 1 Log in to the webpage.

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

Step 3 Enable the function as needed.

- Verification snapshot: Face images will be captured automatically when people unlock the door.
- Alarm snapshot: When enabled, snapshots will be captured upon triggering anti-passback, duress, blocklist and unauthorized excessive attempts. It is turned off by default.
- Night IR snapshot: Clear images can be captured in low-light or complete darkness.

- When **Verification Snapshot** is enabled, **Night IR Snapshot** will be automatically enabled. During daytime, **Verification Snapshot** uses white light capture, while at night, it uses IR capture. If only **Night IR Snapshot** is disabled, **Verification Snapshot** will use white light capture in both daytime and nighttime scenarios.
- When **Alarm Snapshot** is enabled, **Night IR Snapshot** will be automatically enabled. During daytime, **Alarm Snapshot** uses white light capture, while at night, it uses IR capture. If only **Night IR Snapshot** is disabled, **Alarm Snapshot** will use white light capture in both daytime and nighttime scenarios.
- When **Verification Snapshot** , **Alarm Snapshot**, and **Night IR Snapshot** are all enabled, and both **Verification Snapshot** and **Alarm Snapshot** are disabled, the **Night IR Snapshot** will be automatically hidden.

Step 4 Tap **Apply**.

4.6.9 Configuring Output Port Functions

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

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

Procedure

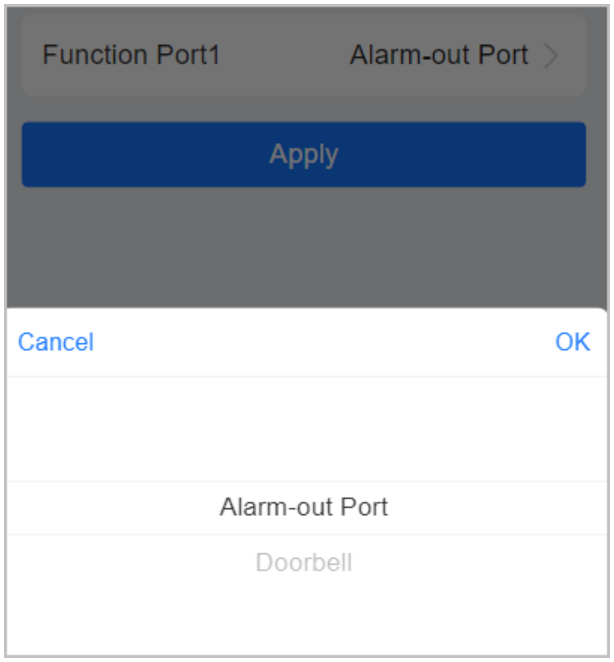
Step 1 Log in to the webpage.

Step 2 Select **More** > **Access Control** > **Output Port Config**.

Step 3 Select the type of the port.

When the alarm cable and the doorbell cable are shared, configure the interface to **Doorbell** to make sure the doorbell will ring.

Figure 4-20 Configure ports



Step 4 Tap **Apply**.

4.7 Communication Settings

4.7.1 Configuring TCP/IP

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

Procedure

Step 1 Log in to the webpage.

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

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

Figure 4-21 TCP/IP

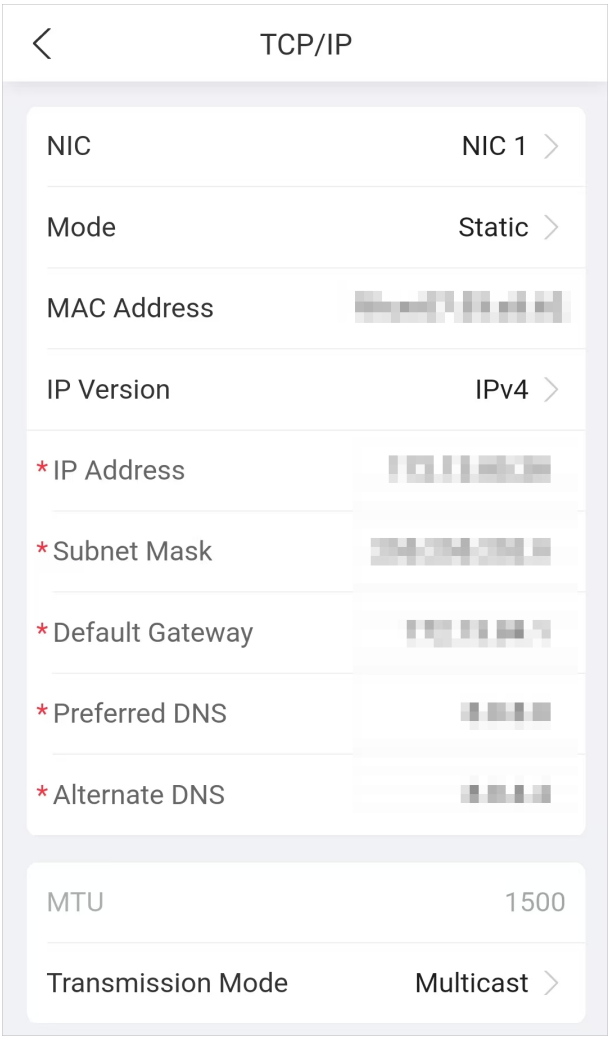


Table 4-8 Description of TCP/IP

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

Parameter	Description
Preferred DNS	Set IP address of the preferred DNS server.
Alternate DNS	Set IP address of the alternate DNS server.
MTU	MTU (Maximum Transmission Unit) refers to the maximum size of data that can be transmitted in a single network packet in computer networks. It is 1500 by default.
Transmission Mode	• Multicast: Ideal for video talk. • Unicast: Ideal for group call.

4.7.2 Configuring Wi-Fi

Procedure

Step 1 Log in to the webpage.

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

Step 3 Turn on Wi-Fi.

All available Wi-Fi are displayed.

- The Wi-Fi function is available only on select models.
- Wi-Fi and Wi-Fi AP can be enabled at the same time, and Wi-Fi function is enabled by default.

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

The Wi-Fi is connected.

Related Operations

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

4.7.3 Configuring Wi-Fi AP

- The Wi-Fi function is available only on select models.
- The Wi-Fi and Wi-Fi AP can be enabled at the same time.

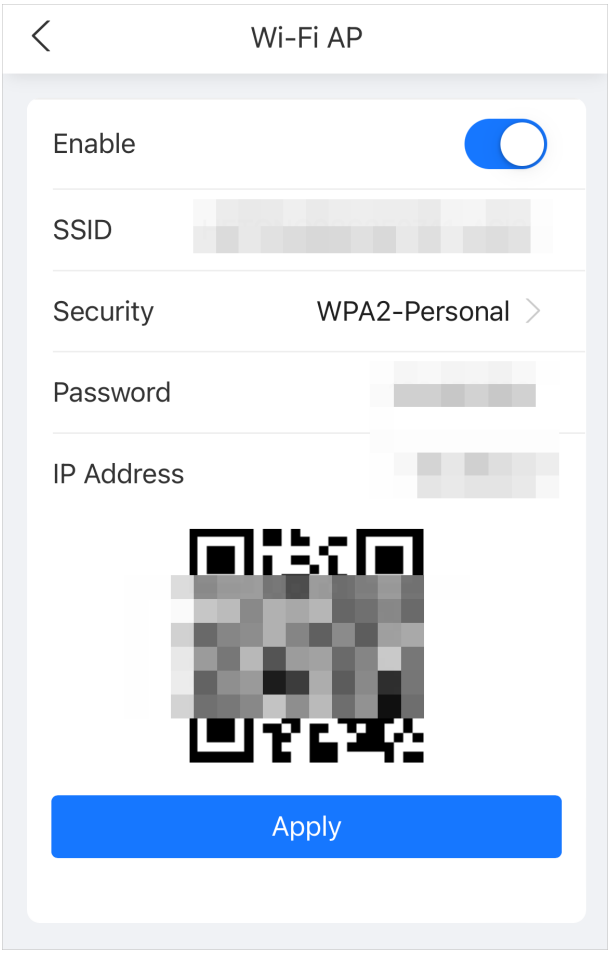
Procedure

Step 1 Log in to the webpage.

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

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

Figure 4-22 Wi-Fi AP



4.7.4 Configuring Cloud Service

Procedure

Step 1 Log in to the webpage.

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

Step 3 Turn on the cloud service function.

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

Step 4 Tap **Apply**.

4.7.5 Configuring Auto Registration

Procedure

Step 1 Log in to the webpage.

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

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

Figure 4-23 Auto registration

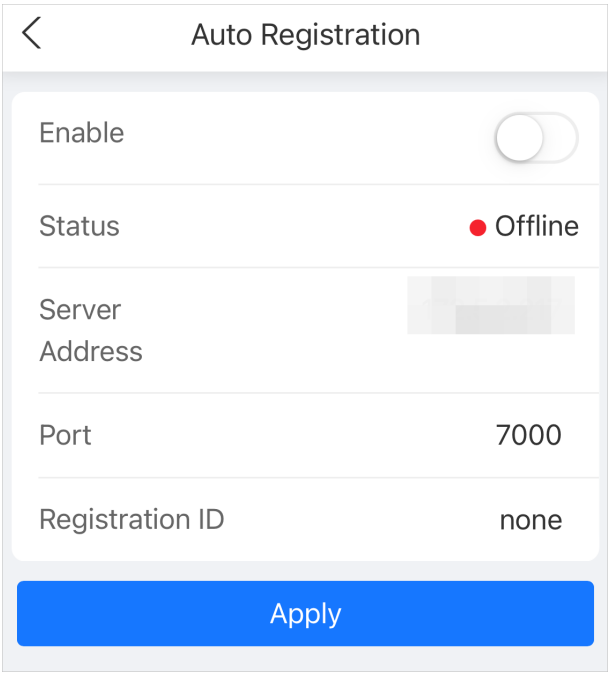


Table 4-9 Automatic registration description

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

4.7.6 Bluetooth Settings

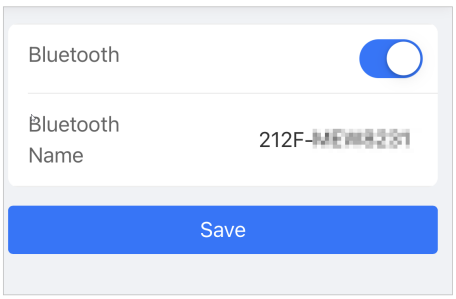
Procedure

Step 1 Log in to the webpage.

Step 2 Select **Communication** > **Bluetooth Settings**.

Step 3 Enable or turn off **Bluetooth**.

Figure 4-24 Bluetooth



Step 4 Tap **Save**.

Results

You can unlock the door through the Bluetooth through the DMSS app. For details, see "2.2.5 Unlocking by Bluetooth" .

4.7.7 Configuring Wiegand

Procedure

Step 1 Log in to the webpage.

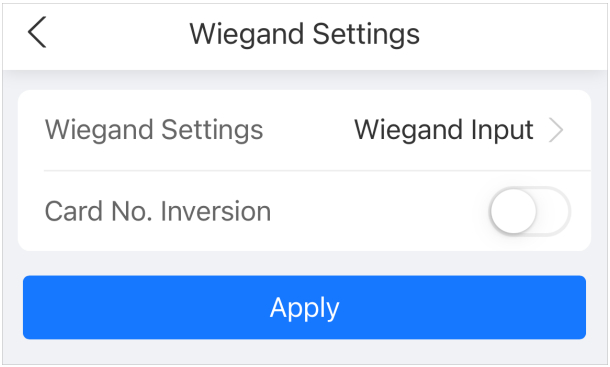
Step 2 Select **More** > **Communication Settings** > **Wiegand**.

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

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

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

Figure 4-25 Wiegand input



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

Figure 4-26 Wiegand output

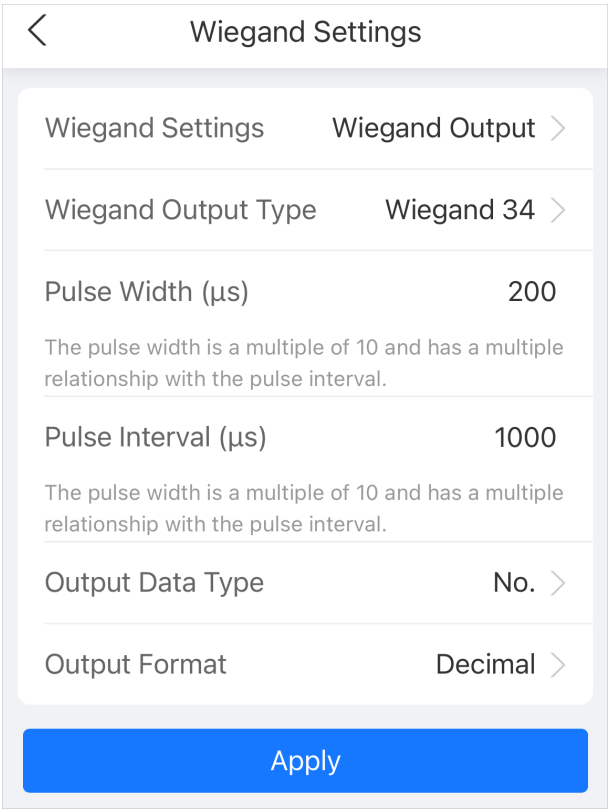


Table 4-10 Description of Wiegand output

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

4.7.8 Configuring RS-485

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

Procedure

Step 1 Log in to the webpage.

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

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

The parameters might differ according to different external device types. The following figure uses **Access Controller** as the example.

Figure 4-27 RS-485 settings

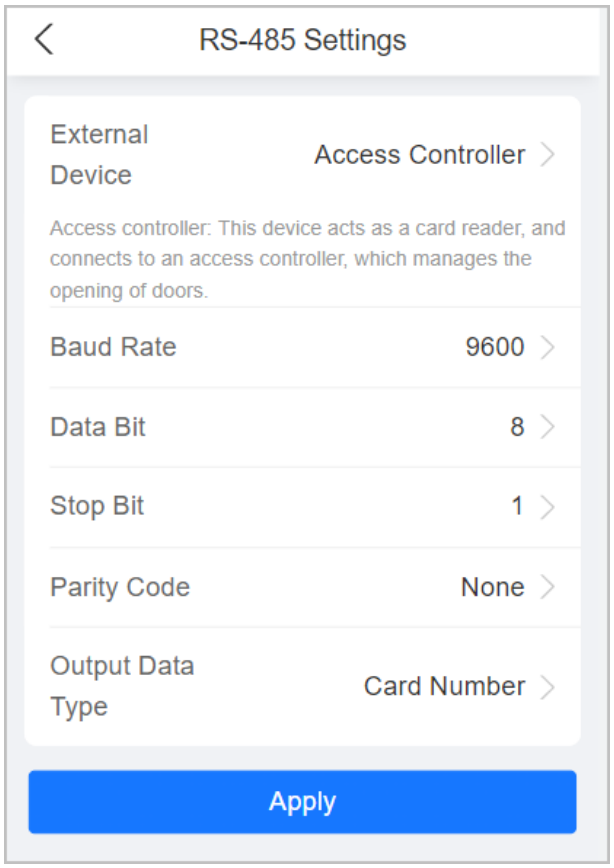


Table 4-11 Configure the RS-485 parameters

Parameter	Description
External Device	• Access Controller Select **Access Controller** when the Device functions as a card reader, and sends data to other external access controllers to control access. Output Data type: ◇ Card Number: Outputs data based on card number when users swipe card to unlock door; outputs data based on user's first card number when they use other unlock methods. ◇ No.: Outputs data based on the user ID. • Card Reader: The Device functions as an access controller, and connects to an external card reader. • Reader (OSDP): The Device is connected to a card reader based on OSDP protocol. • Door Control Security Module: The door exit button, lock and fire linkage is not effective after the security module is enabled. • Turnstile: When the Device connects to a turnstile, and the access controller board of the turnstile connects to an external QR code module or card swiping module, the board will transmit the verification data to the turnstile. • Lock extension mode: When the Access Controller is connected to external lock extension module, if you select **Lock Extension Module**, the local lock is unlocked after you verify the identification on the local device, and the extension lock is unlocked after you verify the identification on the external card reader. After you select **Lock Extension Module** , you can select channel 2 on the **Access Control Parameters** and **Alarm** page on the webpage of the Access Controller.
Data Bit	The number of bits used to transmit the actual data in a serial communication. It represents the binary digits that carry the information being transmitted.
Stop Bit	A bit sent after the data and optional parity bits to indicate the end of a data transmission. It allows the receiver to prepare for the next byte of data and provides synchronization in the communication protocol.
Parity Code	An additional bit sent after the data bits to detect transmission errors. It helps verify the integrity of the transmitted data by ensuring a specific number of logical high or low bits.

4.8 Configuring Audio Prompts

Set audio prompts during identity verification.

Procedure

Step 1 Log in to the webpage.

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

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

Figure 4-28 Configure the audio parameters

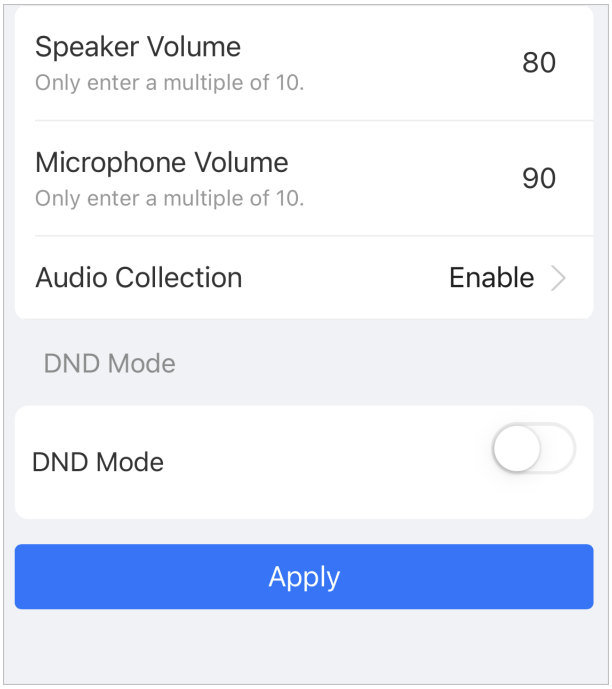


Table 4-12 Parameters description

Parameters	Description
Speaker Volume	Set the volume of the speaker.
Microphone Volume	Set the volume of the microphone.
Audio Collection	If this function is enabled, the sound from the device mic will be captured during live view and recording.
DND Mode	No voice prompts during the set time when you verify your identity on the Device. You can set up to 4 periods.

4.9 Viewing Logs

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

4.9.1 System Logs

View and search for system logs.

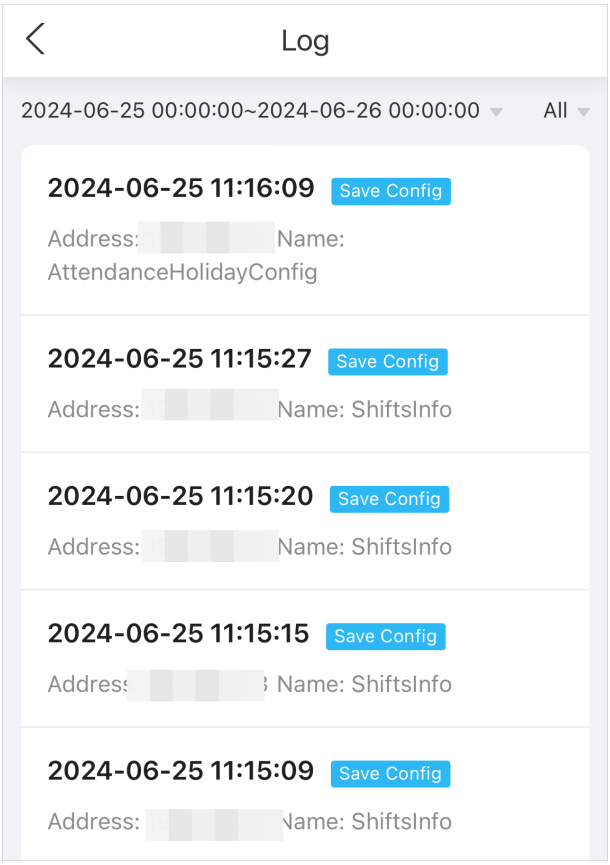
Procedure

Step 1 Log in to the webpage.

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

Step 3 Select the time and the record type.

Figure 4-29 Logs



4.9.2 Unlock Records

Search for unlock records.

Procedure

Step 1 Log in to the webpage.

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

Step 3 Select the time and the record type.

Step 4 Tap a record to view the details.

4.9.3 Call History

Search for the call history.

Procedure

Step 1 Log in to the webpage.

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

4.9.4 Alarm Logs

View alarm logs.

Procedure

Step 1 Log in to the webpage.

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

Step 3 Select the time and the log type.

5 Smart PSS Lite Configuration

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

5.1 Installation

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

5.2 Initialization and Logging In

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

Procedure

Step 1 Double-click SmartPSSLite.exe.

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

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

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

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

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

Step 6 Click **I have read and agree to the terms of software license agreement** to agree **SOFTWARE LICENSE AGREEMENT**.

Step 7 Click **I have read and agree to the terms of software privacy policy** to agree **Product Privacy Policy**.

Step 8 Set password on the **Initialize** page, and then click **Next**.

Table 5-1 Parameters of setting password

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

Step 9 Set security questions, and then click **Complete**.

Step 10 Double-click SmartPSSLite.exe.

Step 11 Enter user name and password, and then click **Login**.

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

5.3 Adding Devices

There are 3 available methods of adding devices.

- Automatically search
- Manually adding
- Import in batches

5.3.1 Adding Device by Searching

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

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

Procedure

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

Step 2 Select a search method.

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

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

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

The devices will be added to the platform.

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

Related Operations

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

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

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

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

5.3.2 Adding Device One by One

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

Procedure

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

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

Step 3 Click **Add**.

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

Appendix 1 Important Points of Face Registration

Before Registration

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

During Registration

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

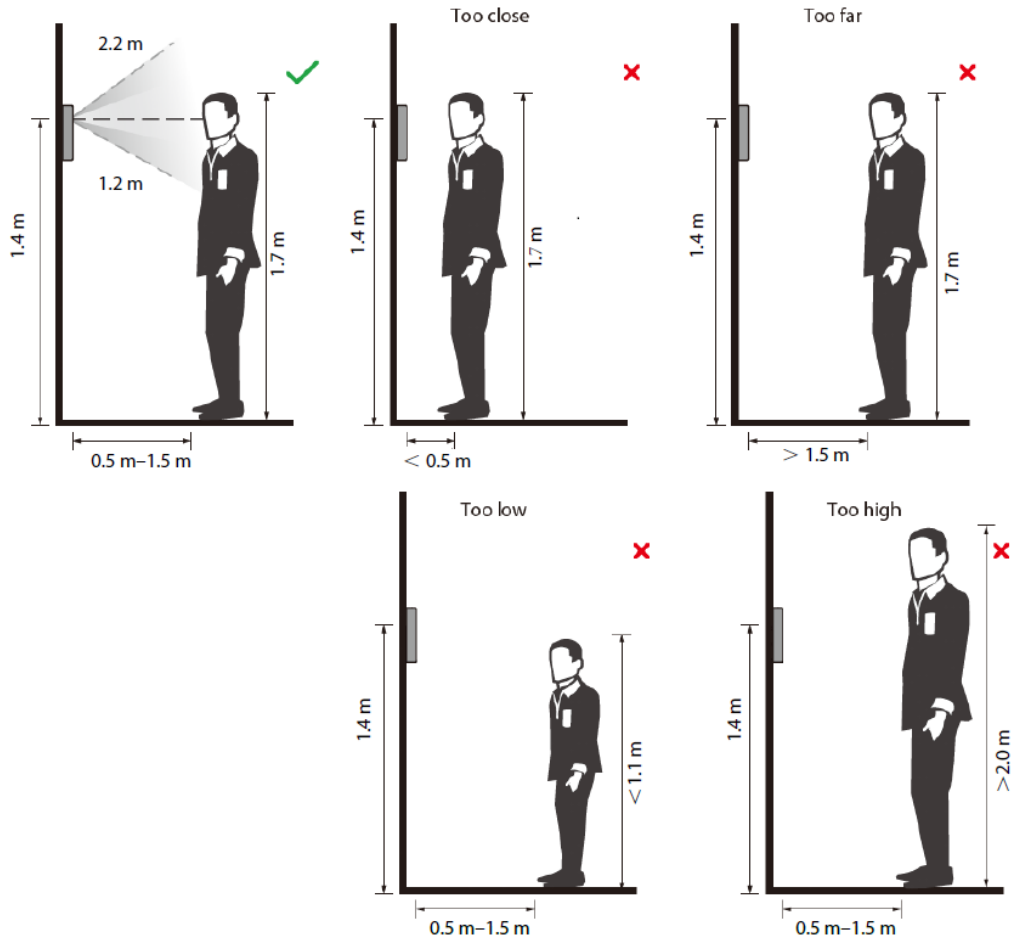
- Do not shake your head or body, otherwise the registration might fail.
- Avoid 2 faces appear in the capture frame at the same time.

Face Position

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

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

Appendix Figure 1-1 Appropriate face position



Requirements of Faces

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

Appendix Figure 1-2 Head position

Appendix Figure 1-3 Face distance

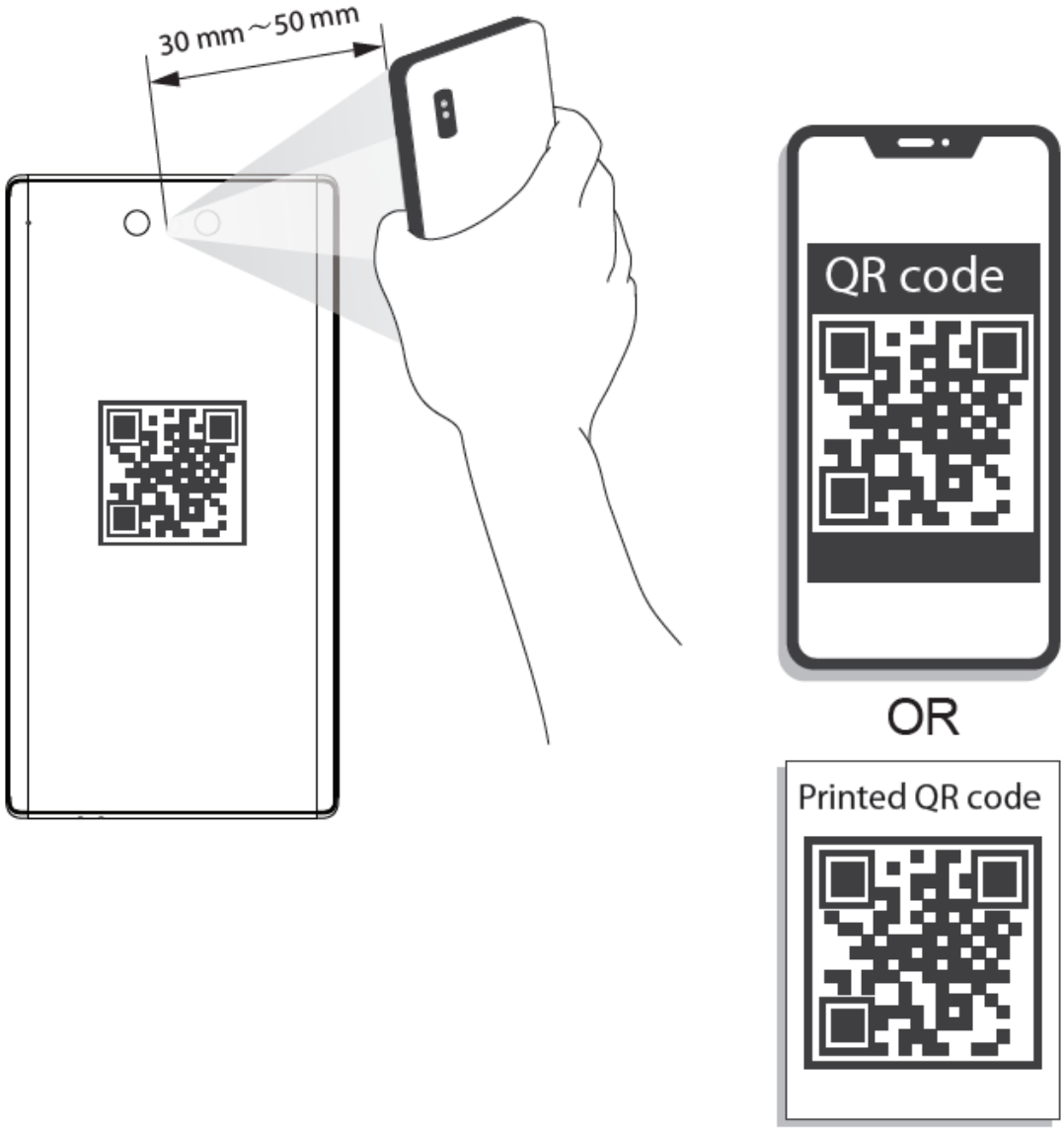
- When importing face images through the management platform, make sure that image resolution is within the range from 150 × 300 pixels to 600 × 1200 pixels. It is recommended that the resolution be greater than 500 × 500 pixels, the image size be less than 100 KB, and the image name and person ID be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

Appendix 2 Important Points of QR Code Scanning

Place the QR code on your phone at a distance of 30 mm–50 mm away from the QR code scanning lens. It supports QR code that is larger than 30 mm × 30 mm and less than 128 bytes in size.

- QR code detection distance differs depending on the bytes and size of QR code.
- Make sure the QR code is aligned with the lens, and avoid direct sunlight.

Appendix Figure 2-1 QR code scanning



Appendix 3 Security Recommendation

Account Management

1. **Use complex passwords**

   Please refer to the following suggestions to set passwords:

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

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

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

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

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

Service Configuration

1. **Enable HTTPS**

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

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

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

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

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

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

Network Configuration

1. **Enable 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;
   - Stablish 802.1x access authentication system to reduce the risk of illegal terminal access to the private network.

Security Auditing

1. **Check online users**

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

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

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

Software Security

1. **Update firmware in time**

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

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

Physical Protection

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

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