Access Controller

User's Manual



ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD. V1.0.5

Foreword

General

This manual introduces the functions and operations of the Access Controller. 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
V1.0.5	Updated the password unlock descriptions.	November 2023
V1.0.4	Updated adding users and configuring permissions.	June 2023
V1.0.3	Updated the description on adding users.	April 2023
V1.0.2	Updated the unlock methods.	March 2023
V1.0.1	Updated the wiring.	September 2022
V1.0.0	First release.	September 2022

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, fingerprints, and license plate number. You need to be in compliance with your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by

implementing measures which include but are not limited: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

About the Manual

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

Important Safeguards and Warnings

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

Transportation Requirement



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

Storage Requirement



Store the Access Controller under allowed humidity and temperature conditions.

Installation Requirements



- Do not connect the power adapter to the Access Controller 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 Access Controller.
- Do not connect the Access Controller to two or more kinds of power supplies, to avoid damage to the Access Controller.
- Improper use of the battery might result in a fire or explosion.



- Personnel working at heights must take all necessary measures to ensure personal safety including wearing a helmet and safety belts.
- Do not place the Access Controller in a place exposed to sunlight or near heat sources.
- Keep the Access Controller away from dampness, dust, and soot.
- Install the Access Controller on a stable surface to prevent it from falling.
- Install the Access Controller 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 power supply must conform to the requirements of ES1 in IEC 62368-1 standard and be no higher than PS2. Please note that the power supply requirements are subject to the Access Controller label.
- The Access Controller is a class I electrical appliance. Make sure that the power supply of the Access Controller is connected to a power socket with protective earthing.

Operation Requirements



- Check whether the power supply is correct before use.
- Do not unplug the power cord on the side of the Access Controller while the adapter is powered on.
- Operate the Access Controller within the rated range of power input and output.
- Use the Access Controller under allowed humidity and temperature conditions.
- Do not drop or splash liquid onto the Access Controller, and make sure that there is no object filled with liquid on the Access Controller to prevent liquid from flowing into it.
- Do not disassemble the Access Controller without professional instruction.

Table of Contents

Foreword I
Important Safeguards and Warnings III
1 Product Overview 1
1.1 Product Introduction 1
1.2 Main Features 1
1.3 Application Scenarios 1
2 Main Controller-Sub Controller 3
2.1 Networking Diagram 3
2.2 Configurations of Main Controller 3
2.2.1 Configuration Flowchart 3
2.2.2 Initialization 4
2.2.3 Logging In 5
2.2.4 Dashboard 10
2.2.5 Home Page 11
2.2.6 Adding Devices 12
2.2.7 Adding Users 14
2.2.8 Adding Weekly Plans 30
2.2.9 Adding Holiday Plans (Optional) 31
2.2.10 Adding Areas 33
2.2.11 Adding Permission Rules 33
2.2.12 Viewing Authorization Progress 36
2.2.13 Configuring Access Control (Optional) 37
2.2.14 Configuring the Password Unlock 41
2.2.15 Configuring Global Alarm linkages (Optional) 41
2.2.16 Configuring First Card Unlock 43
2.2.17 Configuring Multi-person Unlock 45
2.2.18 Configuring Anti-passback 47
2.2.19 Configuring Multi-door Interlock 49
2.2.20 Access Monitoring (Optional) 51
2.2.21 Local Device Configurations (Optional) 52
2.2.22 Viewing Records 69
2.2.23 Security Settings(Optional) 70
2.3 Configurations of Sub Controller 80
2.3.1 Initialization 80
2.3.2 Logging In 80
2.3.3 Home Page 80
3 Smart PSS Lite-Sub Controllers 81

3.1 Networking Diagram 81
3.2 Configurations on SmartPSS Lite 81
3.3 Configurations on Sub Controller 81
Appendix 1 Cybersecurity Recommendations 82

1 Product Overview

1.1 Product Introduction

Flexible and convenient, the Access Controller has a user friendly system that allows you to access controllers on the webpage through IP address. It comes with a professional access management system, and makes the networking of main and sub control modes quick and easy, meeting the needs of small and advanced systems.

1.2 Main Features

- Built of flame-retardant PC and ABS material, it is both sturdy and elegant with an IK06 rating.
- Supports TCP and IP connection, and standard PoE.
- Accesses card readers through Wiegand and RS-485 protocols.
- Supplies power to the lock through its 12 VDC output power supply, which has a maximum output current of 1000 mA.
- Supports 1000 users, 5000 cards, 3000 fingerprints, and 300,000 records.
- Multiple unlock methods including card, password, fingerprint and more. You can also combine these methods to create your own personal unlock methods.
- Multiple types of alarms events are supported, such as duress, tampering, intrusion, unlock timeout, and illegal card.
- Supports a wide range of users including general, patrol, VIP, guest, blocklisted, and more users.
- Manual and automatic time synchronization.
- Retains stored data even while powered off.
- Offers a variety of functions and the system can be configured. Devices can also be updated through the webpage.
- Features main and sub control modes. The main control mode offers user management, access control device management and configuration, and more options. Devices under sub-control modes can be added to multiple platforms.
- A main controller can connect with and manage up to 19 sub controllers.
- Watchdog protects the system to allow the device to be stable and perform efficiently.
- Sub controllers can be added to SmartPSS Lite and DSS Pro.

1.3 Application Scenarios

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

The Access Controller can be set to the main access controller (herein referred to as main controller) or the Sub Access Controller (herein referred to as sub-controller). 2 different networking methods are available for the Access Controller. You can select a networking method based on your needs.

Table 1-1 Networking methods of access controller

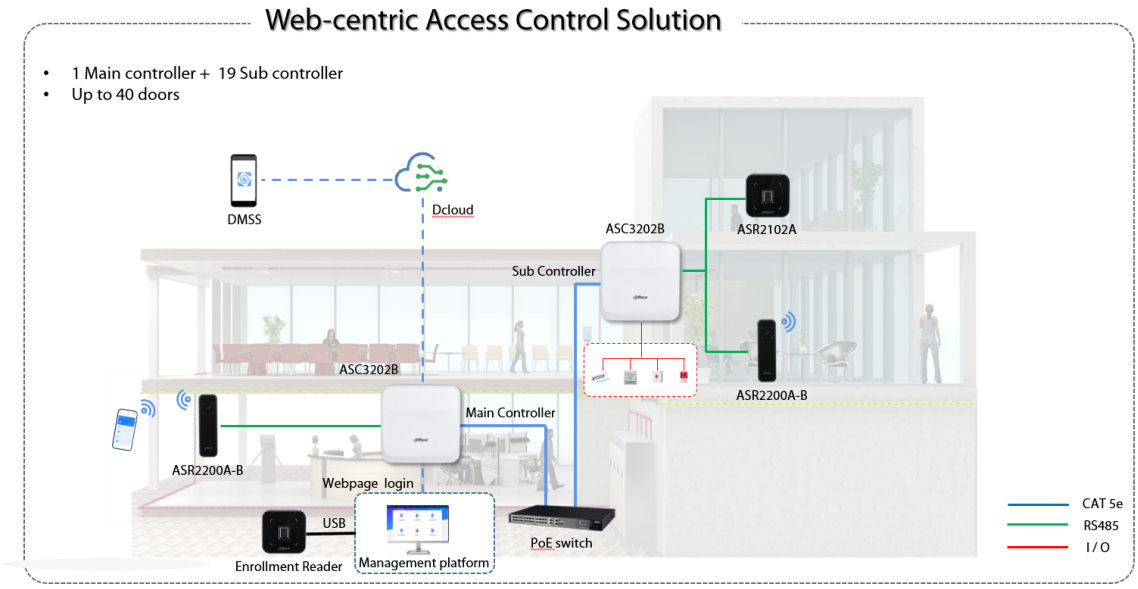
Networking methods	Description
Main Controller—Sub Controller	The main controller comes with a management platform (herein referred to as the Platform). Sub-controllers must be added to the Platform of the main controller. The main controller can manage up to 19 sub controllers. For details, see "2 Main Controller-Sub Controller". We do not recommend you add other management platforms in this networking method.
SmartPSS Lite—Sub Controller	Sub controllers needs to be added to a standalone management platform, such as SmartPSS Lite. The platform can manage up to 64 doors if each sub controller connects 2 doors. For details, see "3 Smart PSS Lite-Sub Controllers".

2 Main Controller-Sub Controller

2.1 Networking Diagram

The main controller comes with a management platform (herein referred as the platform). Sub controller needs to be added to the management platform of the main controller. The main controller can manage up to 19 sub controllers.

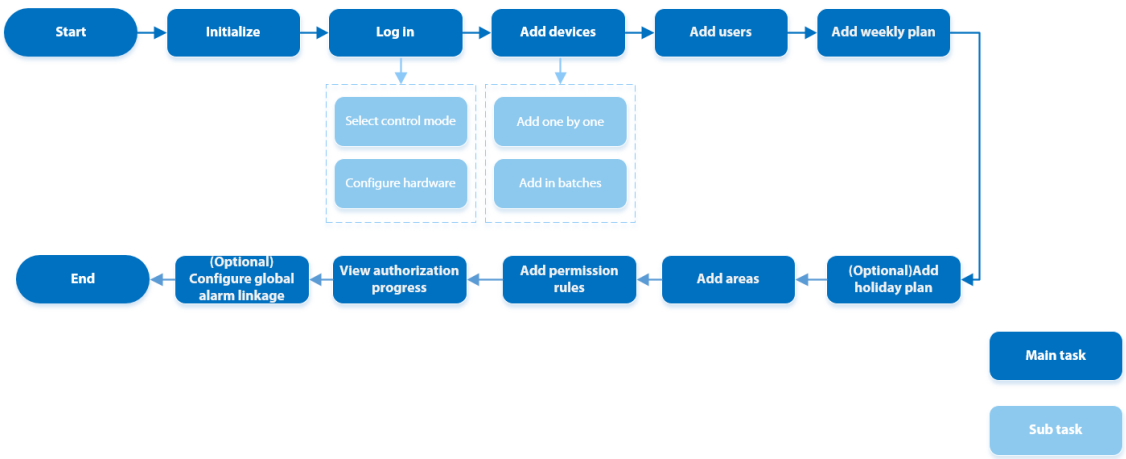
Figure 2-1 Networking diagram



2.2 Configurations of Main Controller

2.2.1 Configuration Flowchart

Figure 2-2 Configuration flowchart



2.2.2 Initialization

Initialize the main controller when you log in to the webpage for the first time or after it is restored to its factory defaults.

Prerequisites

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

Procedure

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

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

Step 2 Select a language, and then click **Next**.

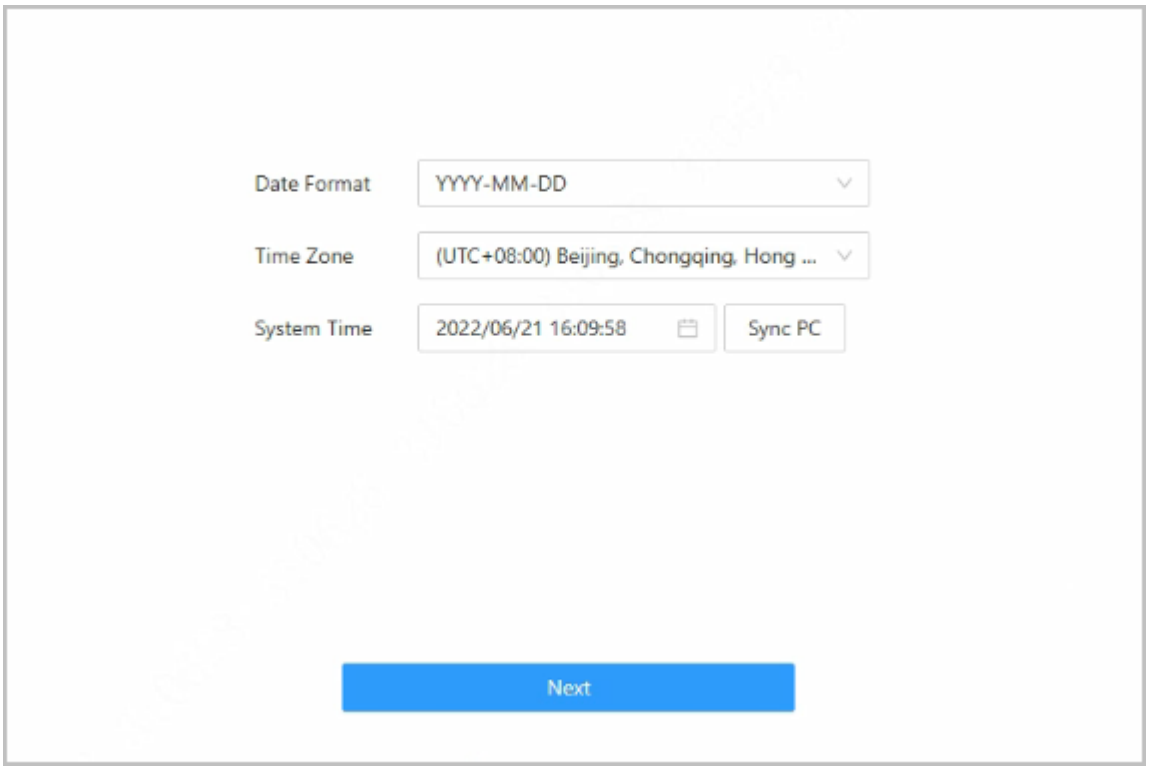
Step 3 Read the software license agreement and privacy policy carefully, select **I have read and agree to the terms of the Software License Agreement and Privacy Policy.** , and then click **Next**.

Step 4 Set the password and email address.

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

Step 5 Configure the system time, and then click **Next**.

Figure 2-3 Configure the time



Step 6 (Optional) Select **Auto Check for Updates** , and then click **Completed**.

The system automatically check is there any higher version available, and inform the user to update the system. The system automatically checks for new updates, and informs you when a new update is available.

Step 7 Click **Completed**.

The system automatically goes to the login page after initialization is successful.

2.2.3 Logging In

For first-time login during initialization, you need to follow the login wizard to configure the type of main controller and its hardware.

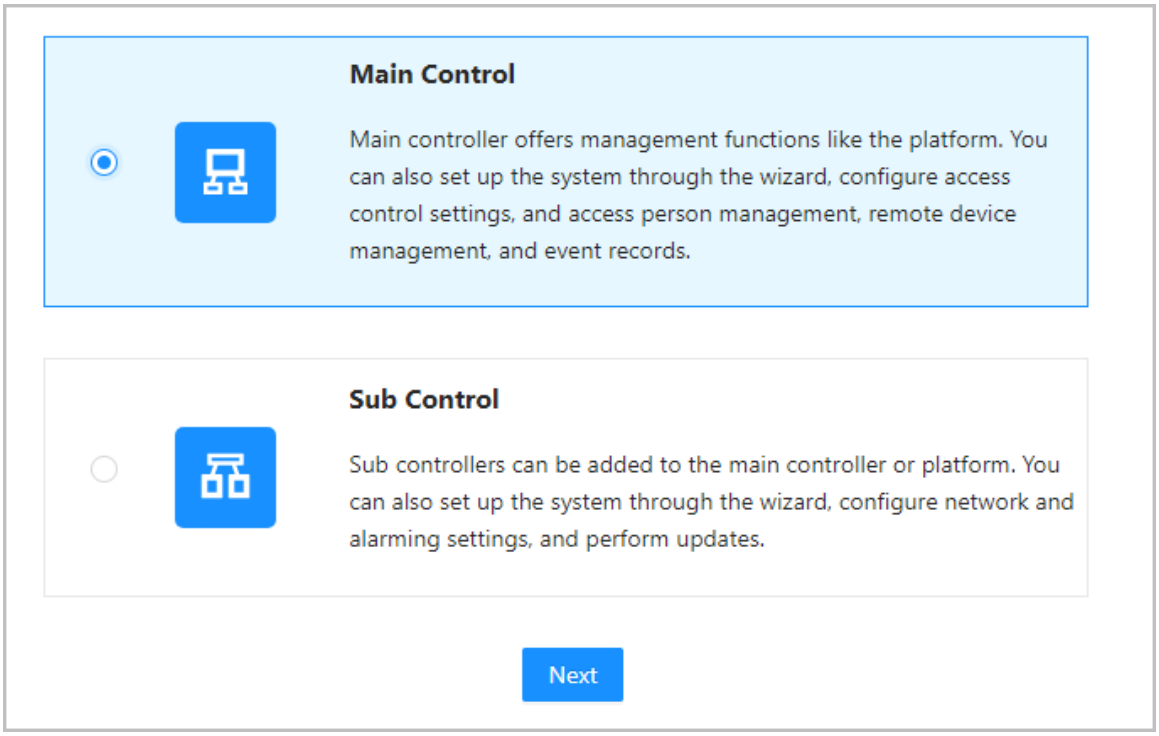
Procedure

Step 1 On the login page, enter the username and password.

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

Step 2 Select **Main Control** , and then click **Next**.

Figure 2-4 Type of access controller



- Main Control: The main controller comes with a management platform. You can manage all sub-controllers, configure access control, access personal management on the platform, and more.
- Sub Control: Sub controllers needs to be added to the management platform of the main controller or other management platforms such as DSS Pro or SmartPSS Lite. You can perform the configurations on the webpage of the sub-controller.

Step 3 Select the number of doors, and then enter the name of the door.

Step 4 Configure the parameters of the doors.

Figure 2-5 Configure door parameters

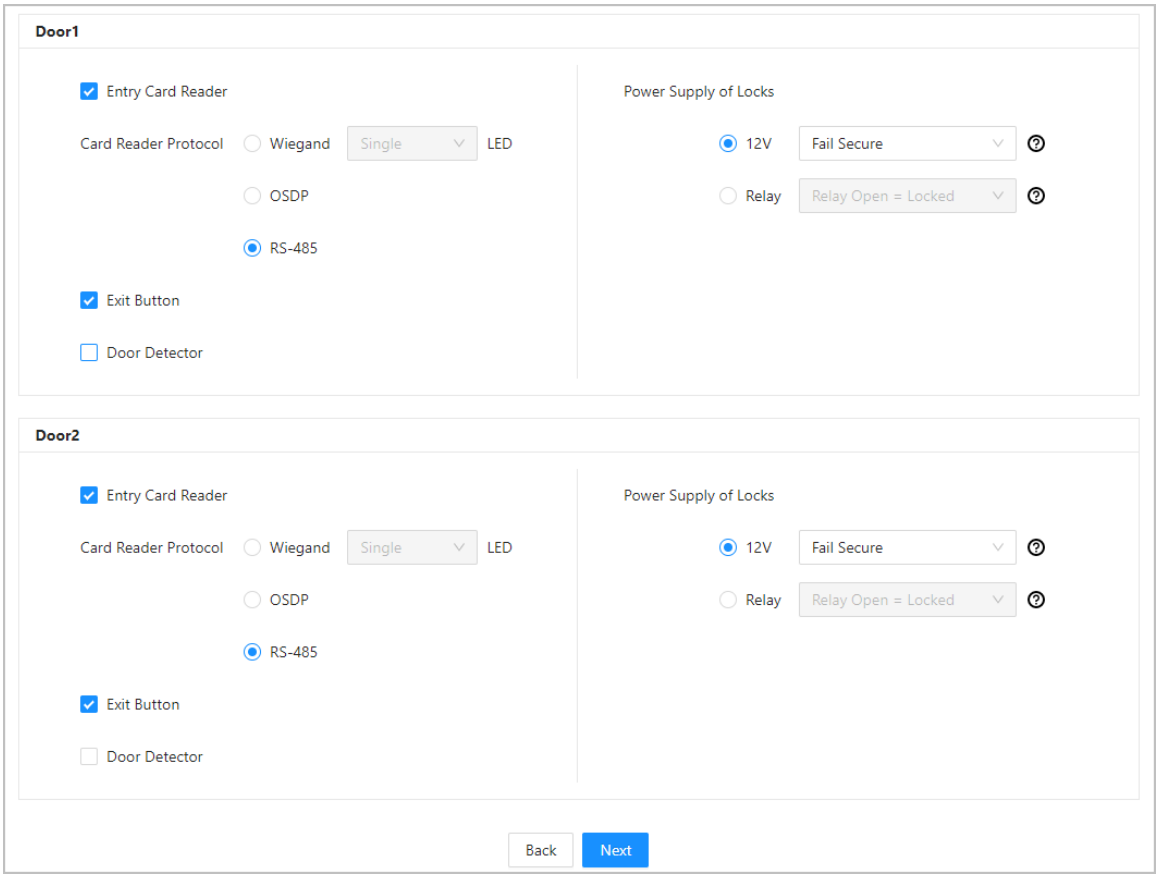


Table 2-1 Parameter description

Parameter	Description
Entry Card Reader	Select the card reader protocol. • Wiegand: Connects to a Wiegand reader. You can connect the LED wire to the LED port of the controller, and the reader will beep and flash when the door unlocks. • OSDP: Connects to an OSDP reader. • RS-485: Connects to a RS-485 reader.
Exit Button	Connects to an exit button.
Door Detector	Connects to a door detector.

Parameter	Description
Power Supply of Locks	• 12 V: The controller provides power to the lock. ◇ Fail secure: When the power is interrupted or fails, the door stays locked. ◇ Fail safe: When the power is interrupted or fails, the door automatically unlocks to let people leave. • Relay: The relay supplies power for the lock. ◇ Relay open = locked: Sets the lock to remain locked when the relay is open. ◇ Relay open = unlocked: Sets the lock to unlock when the relay is open. The electromagnetic lock unlocks in a instant and locks again immediately when the Access Controller is in the soft reboot.

Step 5 Configure access control parameters.

Step 6 In **Unlock Settings** , select **Or** or **And** from **Combination Method**.

- Or: Use one of the selected unlock methods to authorize opening the door.
- And: Use all of the selected unlock methods to authorize opening the door.

Bluetooth card can not be selected when you set the combination method to **And**.

Step 7 Select the unlock methods, and then configure the other parameters.

Figure 2-6 Unlock settings

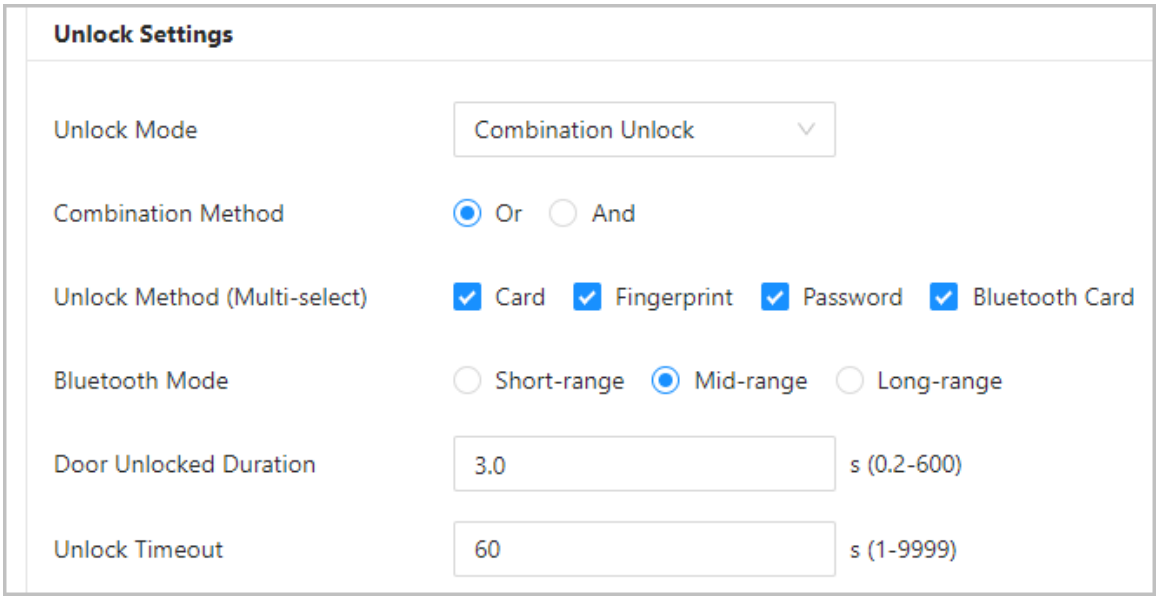


Table 2-2 Unlock settings description

Parameter	Description
Unlock Method (Multi-select)	Supports unlocking through card, fingerprint, password or Bluetooth card. The Bluetooth card function is turned off by default.

Parameter	Description
Bluetooth Mode	The Bluetooth card must be a certain distance away from the access control device to exchange data and unlock the door. Following are the ranges that are most suitable for it. • Short-range: The Bluetooth unlock range is less than 0.2 m. • Mid-range: The Bluetooth unlock range is less than 2 m. • Long-range: The Bluetooth unlock range is less than 10 m. ⚠ The Bluetooth unlock range might differ depending on models of your phone and the environment.
Door Unlock Duration	After a person is granted access, the door will remain unlocked for a defined time for them to pass through. It ranges from 0.2 s to 600 s.
Unlock Timeout	A timeout alarm is triggered when the door remains unlocked for longer than the defined value.

Step 8 In **Alarm Settings**, configure the alarm parameters.

Figure 2-7 Alarm

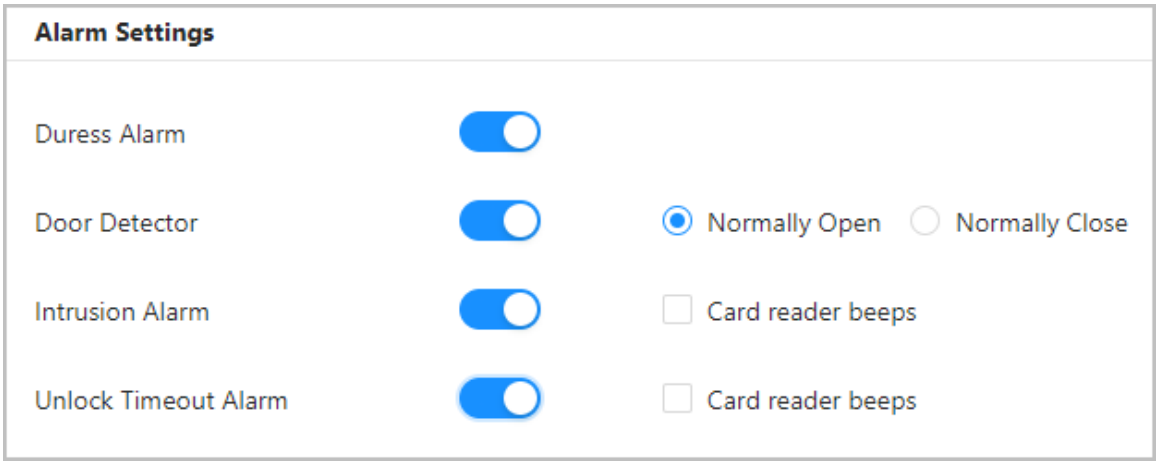


Table 2-3 Description of alarm parameters

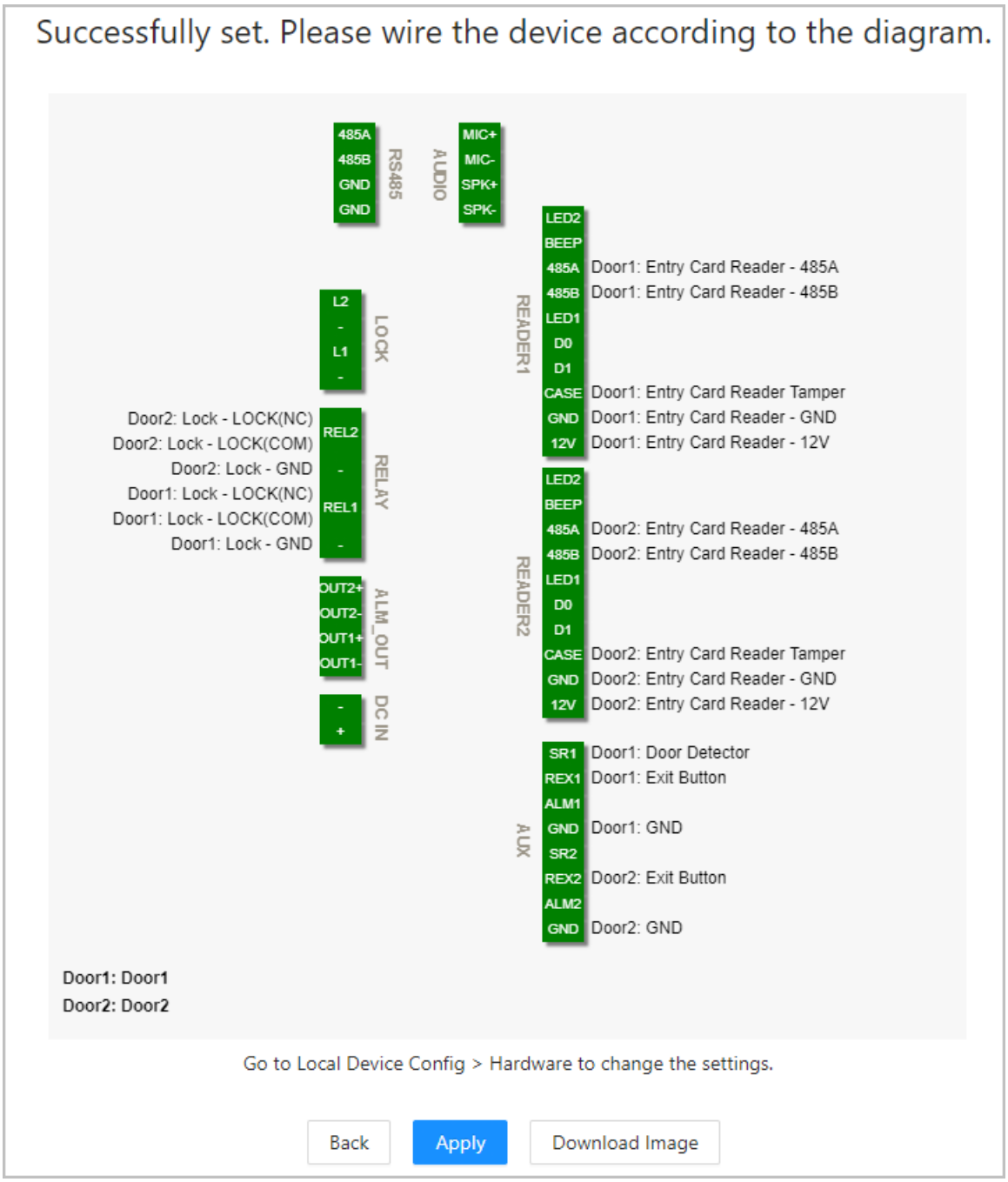
Parameter	Description
Duress Alarm	An alarm will be triggered when a duress card, duress password or duress fingerprint is used to unlock the door.
Door Detector	Select the type of door detector.
Intrusion Alarm	• When the door detector is enabled, an intrusion alarm will be triggered if the door is opened abnormally. • A timeout alarm will be triggered when the door remains unlocked for longer than the defined unlock time. • When **Card reader beeps** is enabled, the card reader beeps when the intrusion alarm or timeout alarm is triggered.
Unlock Timeout Alarm	

Step 9 Click **Next**.

A wiring diagram is generated based on your configurations. You can wire the device according to the diagram.

The image below is for reference only.

Figure 2-8 Wiring diagram



Step 10 Click **Apply**.

- You can go to **Local Device Config** > **Hardware** to change the settings after you successfully log in to the platform.
- Click **Download Image** to download the diagram to your computer.

Related Operations

If you want to change the settings of the hardware, go to **Local Device Config** > **Hardware**.

2.2.4 Dashboard

After you successfully log in, the dashboard page of the platform is displayed. The dashboard is displayed showing visualized data.

Figure 2-9 Dashboard

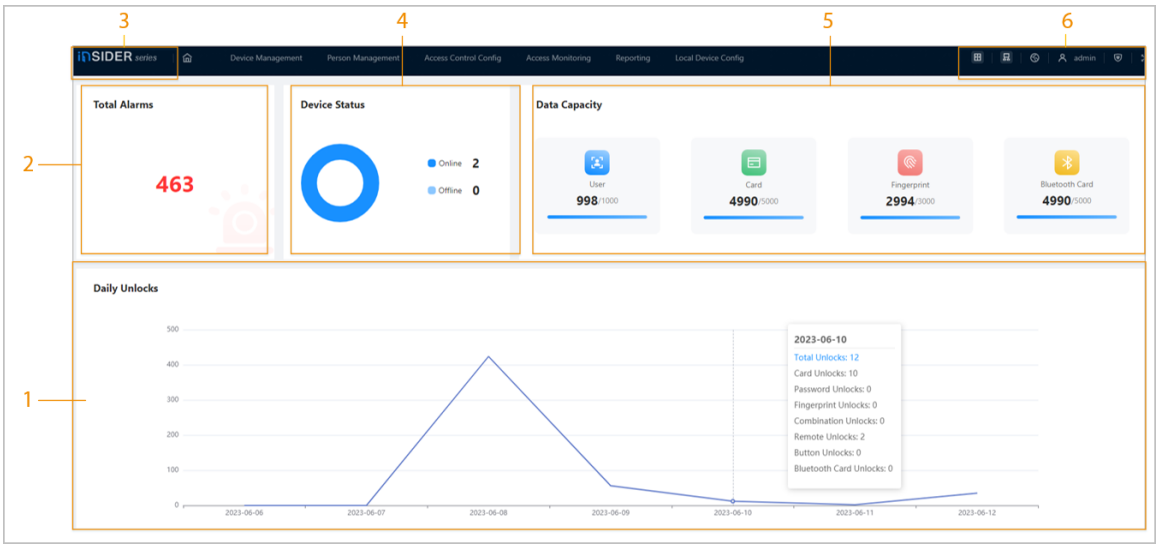


Table 2-4 Home page description

No.	Description
1	Displays the unlock methods used for the day. Hover over a day to see the type of unlocks used for that day.
2	Displays the total number of alarms.
3	• Click to go to the dashboard page. • Click to go to the dashboard page. • Click to go to the home page of the platform.
4	Displays the status of devices, including offline devices and online devices.
5	Displays the data capacity of cards, fingerprints and Bluetooth cards.

No.	Description
6	• The number of doors of the controller. ◇ : Double door ◇ : Single door • The type of the controller. ◇ : Main controller. ◇ : Sub controller. • : Select the language of the platform. • : Go to the **Security** page directly. • : Restart or log out of the platform. • : Display the webpage in full screen.

2.2.5 Home Page

After you successfully log in, the home page of the main controller is displayed.

Figure 2-10 Home page

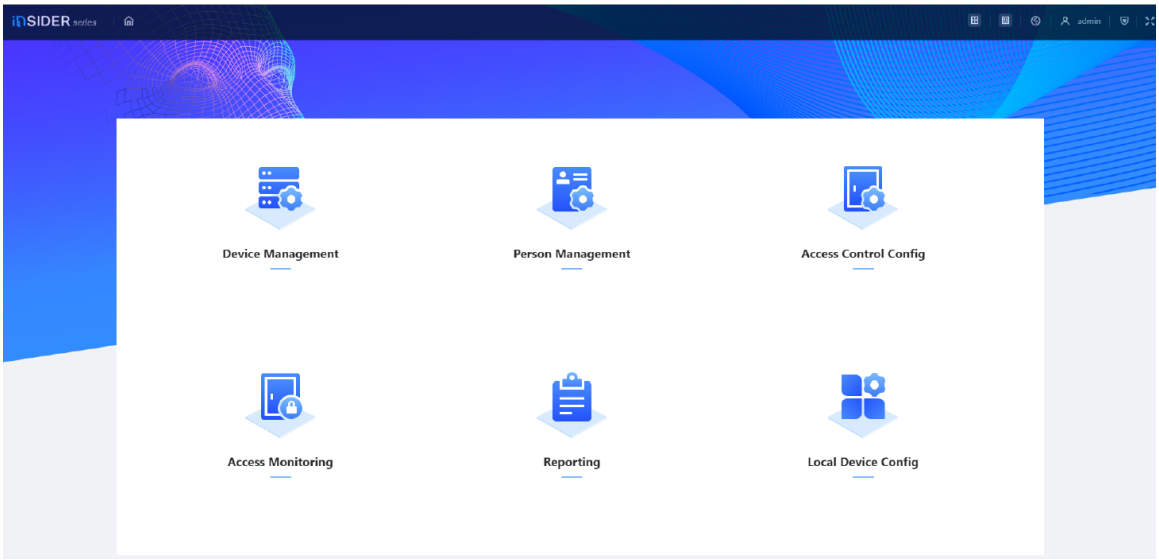


Table 2-5 Home page description

Menu	Description
Device Management	Add devices to the platform of the main controller.
Person Management	Add personnel and assign area permissions to them.
Access Control Config	Add time templates, create and assign area permissions, configure door parameters and global alarm linkages, and view the permission authorization progress.
Access Monitoring	Remotely control the doors and view event logs.
Reporting	View and export alarm records and unlock records.

Menu	Description
Local Device Config	Configure parameters for the local device, such as network and local alarm linkage.

2.2.6 Adding Devices

You can add devices to the management platform of the main controller in batches or one by one. If the controller was set to the main controller while you were going through the login wizard, you can add and manage sub controllers through the Platform.

Only the main controller comes with a management platform.

2.2.6.1 Adding Device One by One

You can add sub controllers to the main controller one by one.

Procedure

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

Step 2 Enter the device information.

Figure 2-11 Device information

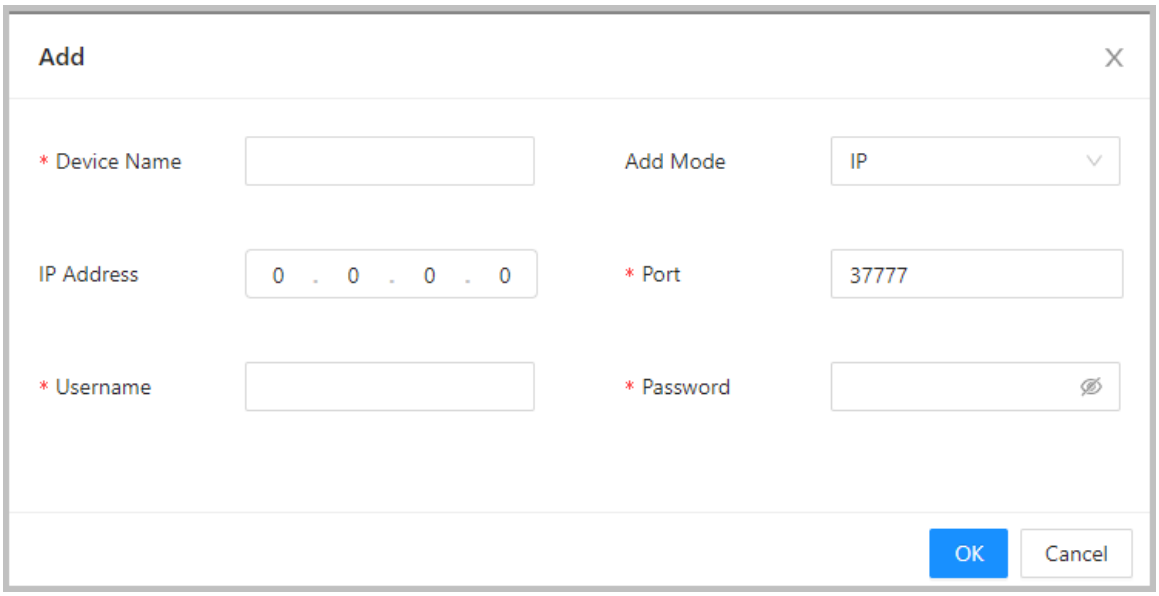


Table 2-6 Device parameters Description

Parameter	Description
Device Name	Enter the name of the Controller. We recommend you name it after its installation area.
Add Mode	Select **IP** to add the Access Controller by entering its IP address.
IP Address	Enter the IP address of the controller.
Port	The port number is 37777 by default.
Username/Password	Enter the username and password of the Controller.

Step 3 Click **OK**.

The added controllers are displayed on the **Device Management** page.

Figure 2-12 Successfully add devices



If the controller was set as the main controller while you were going through the login wizard, the controller will be added to the management platform automatically and function as both the main controller and sub controller.

Related Operations

- : Edit the information on the device.

  Only sub controllers support the below operations.
- : Go to the webpage of the sub controller.
- : Log out of the device.
- : Delete the device.

2.2.6.2 Adding Devices in Batches

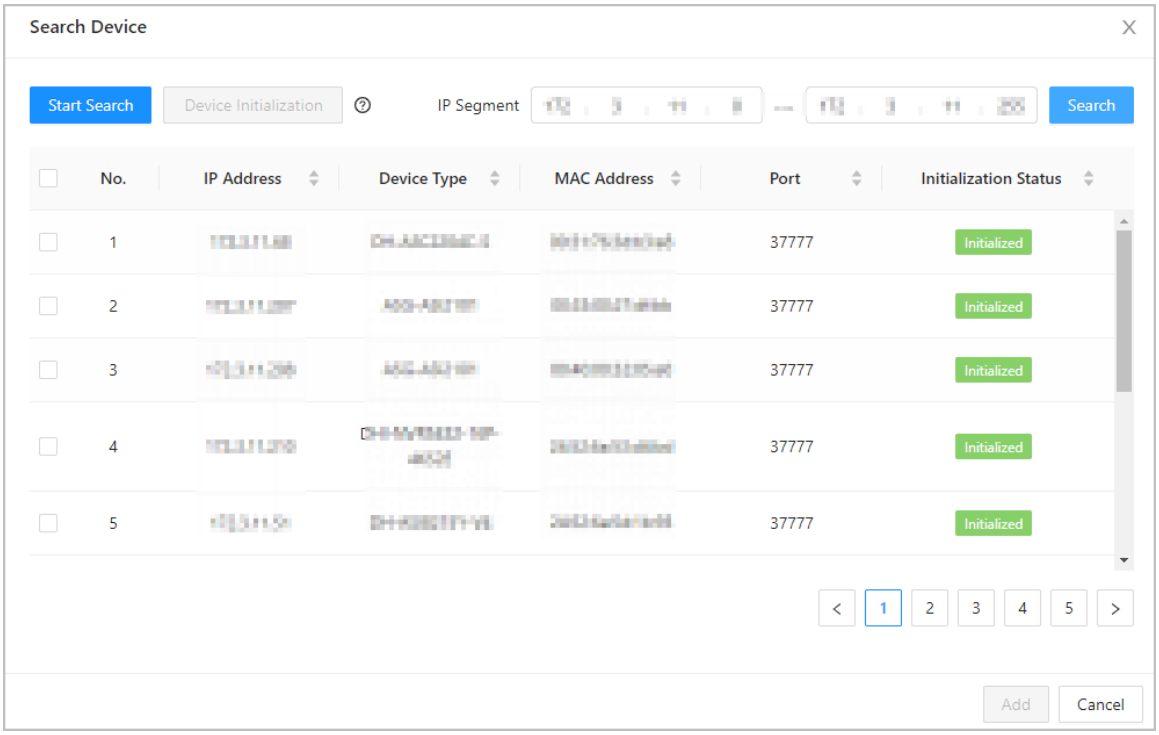
We recommend you use the auto-search function when you add sub controllers in batches. Make sure the sub controllers you want to add are on the same network segment.

Procedure

Step 1 On the home page, Click **Device Management** , and then click **Search Device**.

- Click **Start Search** to search for devices on the same LAN.
- Enter a range for the network segment, and then click **Search**.

Figure 2-13 Auto search



All devices that were searched for will be displayed.

You can select devices from the list, and click **Device Initialization** to initialize them in batches.

To ensure the security of devices, initialization is not supported for devices on different segments.

Step 2 Select the Controllers that you want to add to the Platform, and then click **Add**.

Step 3 Enter the username and password of the sub controller, and then click **OK**.

The added sub controllers are displayed on the **Device Management** page.

Related Operations

- Modify IP: Select added devices, and then click **Modify IP** to change their IP addresses.
- Sync Time: Select added devices, and then click **Sync Time** to sync the time of the devices with the NTP server.
- Delete: Select the devices, and then click **Delete** to delete them.

2.2.7 Adding Users

Add users to departments. Enter basic information for users and set verification methods to verify their identities.

Related Operations

- Export all the users to Excel: On the **Person Management** page, click **Export** to export all users. You can also import the exported user information to other controllers.

To prevent data loss caused by force majeure damage to the equipment, it is recommended to regularly export user data for backup purposes.

- Import users: On the **Person Management** page, click **Download Template**, enter user information in the template, and then click **Import** to import all users.
- Extract all the users: On the **Person Management** page, click **More** > **Extract Person Info**, and select a device to extract all the users from the sub controller and send them to them the Platform of the main controller.

2.2.7.1 Adding Departments

Procedure

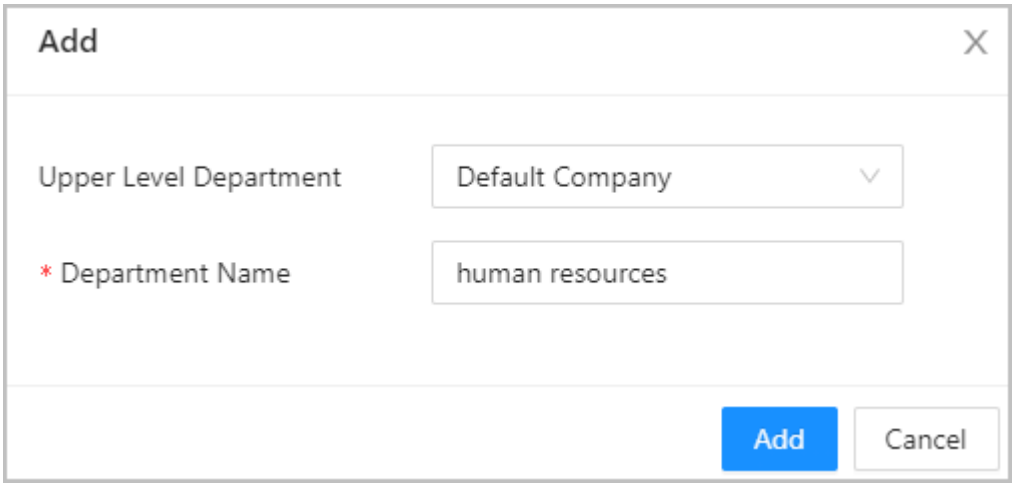
Step 1 On the home page, select **Person Management**.

Step 2 Create a department.

1. Click +.
2. Enter the name of the department, and then click **Add**.

The default department cannot be deleted.

Figure 2-14 Add department



Step 3 Click **OK**.

2.2.7.2 Adding Roles

Procedure

Step 1 On the home page, select **Person Management**.

Step 2 Create roles.

- The following roles already exist and cannot be modified or deleted: Default, Manager, Administrator, Visitor and Employee.
- The only general user type with manager role has the highest authority and it is not limited by advanced access rules, such as first card unlock, multi-person unlock, anti-passback, always closed door and unlock methods.

1. Click +.
2. Enter the name of the role, and then click **Add**.

2.2.7.3 Configuring Basic User Information

Procedure

Step 1 On the home page, select **Person Management**.

Step 2 Add users.

- Add users one by one.
  1. Click **Add**, and then enter the basic information for the user.

Figure 2-15 Basic information on the user

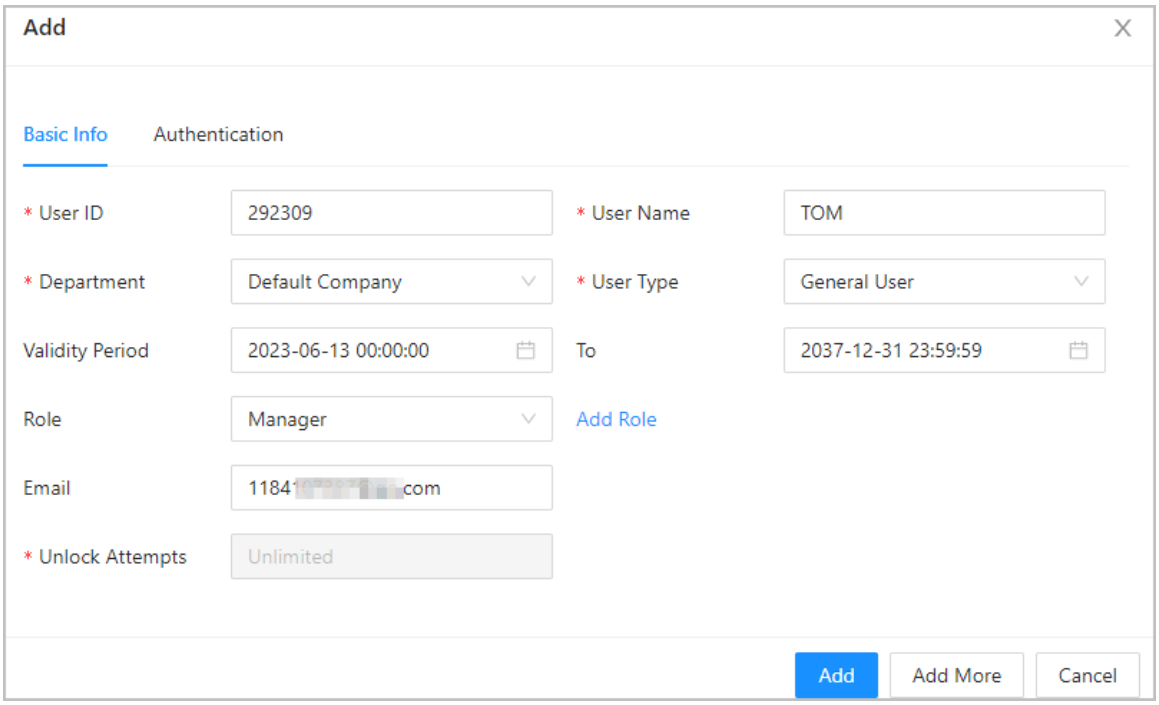


Table 2-7 Parameters description

Parameter	Description
User ID	The ID of the user.
Department	The department that the user belongs to. For details on how to create departments, see "2.2.7.1 Adding Departments".
Validity Period	Set a date on which the access permissions of the person will become effective.
Role	Assign an existing role to the user. You can also click **Add Role** to create a new role.
Email	The email address must be the same as the one that was used to sign up for DMSS.
To	Set a date on which the access permissions of the person will expire.
User Name	The name of the user.

Parameter	Description
User Type	The type of user. ◇ **General User** : General users can unlock the door. ◇ **VIP User** : When the VIP unlocks the door, service personnel will receive a notice. ◇ **Guest User** : Guests can unlock the door within a defined period or for a set number of times. After the defined period expires or the number of times for unlocking runs out runs out, they cannot unlock the door. ◇ **Patrol User** : Patrol users will have their attendance tracked, but they have no permission to unlock the door. ◇ **Blocklist User** : When users in the blocklist unlock the door, service personnel will receive a notification. ◇ **Other User** : When they unlock the door, the door will stay unlocked for 5 more seconds.
Unlock Attempts	The number of times a guest user can unlock the door.

2. Click **Add**.

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

- Add users through importing the template.

  1. Click **Import** > **Download Template** to download the user template.
  2. Enter user information in the template, and then save it.
  3. Click **Import**, and upload the template to the Platform.

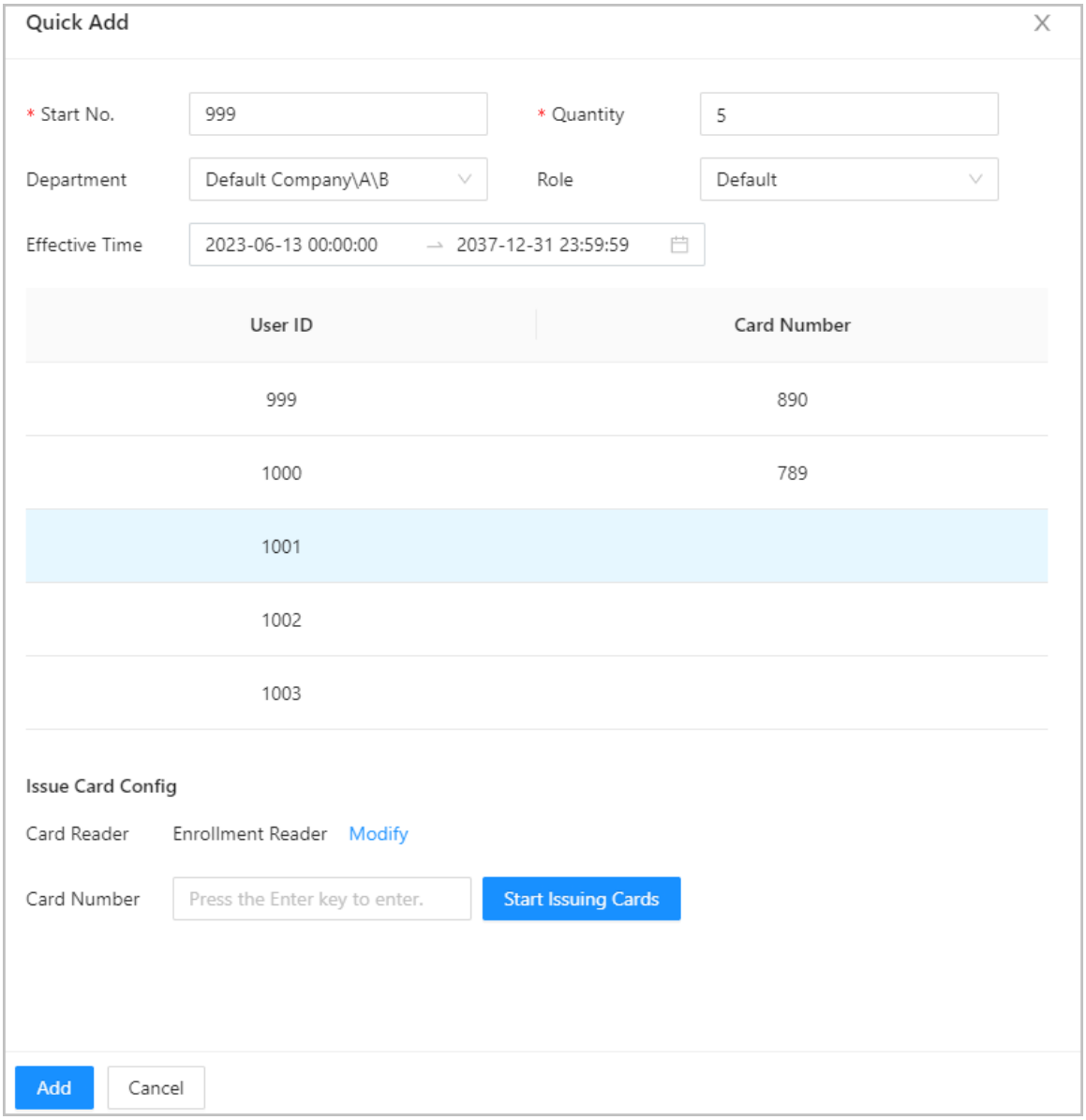
     The users are added to the Platform automatically.

- Use **Quick Add** to easily add users.

  1. Click **Quick Add**.
  2. Enter the start number of the user ID, and the quantity.

     The platform will generate a sequence of numbers starting from the defined start number. For example, if the start number is 999, and the quantity is 5, the system will generate a sequence of numbers from 999 to 1003.

Figure 2-16 Quick add



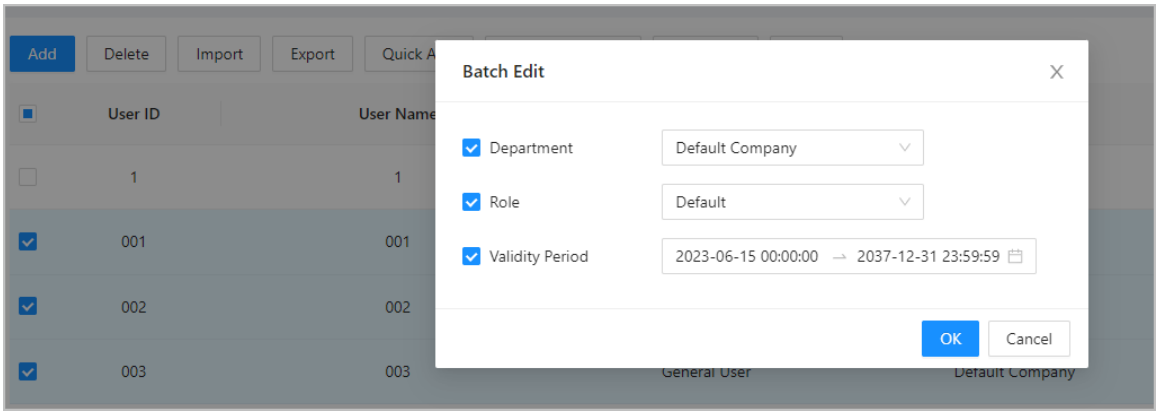
3. Select the department, role and the effective time.
4. Issue cards to the users in batches.

   You can manually enter the card number, or use the enrollment reader or card reader to read the card number. For details, see "2.2.7.4.2 Adding Cards".

Related Operations

Batch Edit: Edit personal information in batches.

Figure 2-17 Batch edit



2.2.7.4 Adding Authentication Methods

Add password, cards, fingerprint or Bluetooth cards to users, so that users can unlock the door through authentication. Each user can have up to 1 password, 5 IC/ID cards, 3 fingerprints, and 5 Bluetooth cards.

2.2.7.4.1 Adding Passwords

Add passwords to users for them to gain access by entering their password.

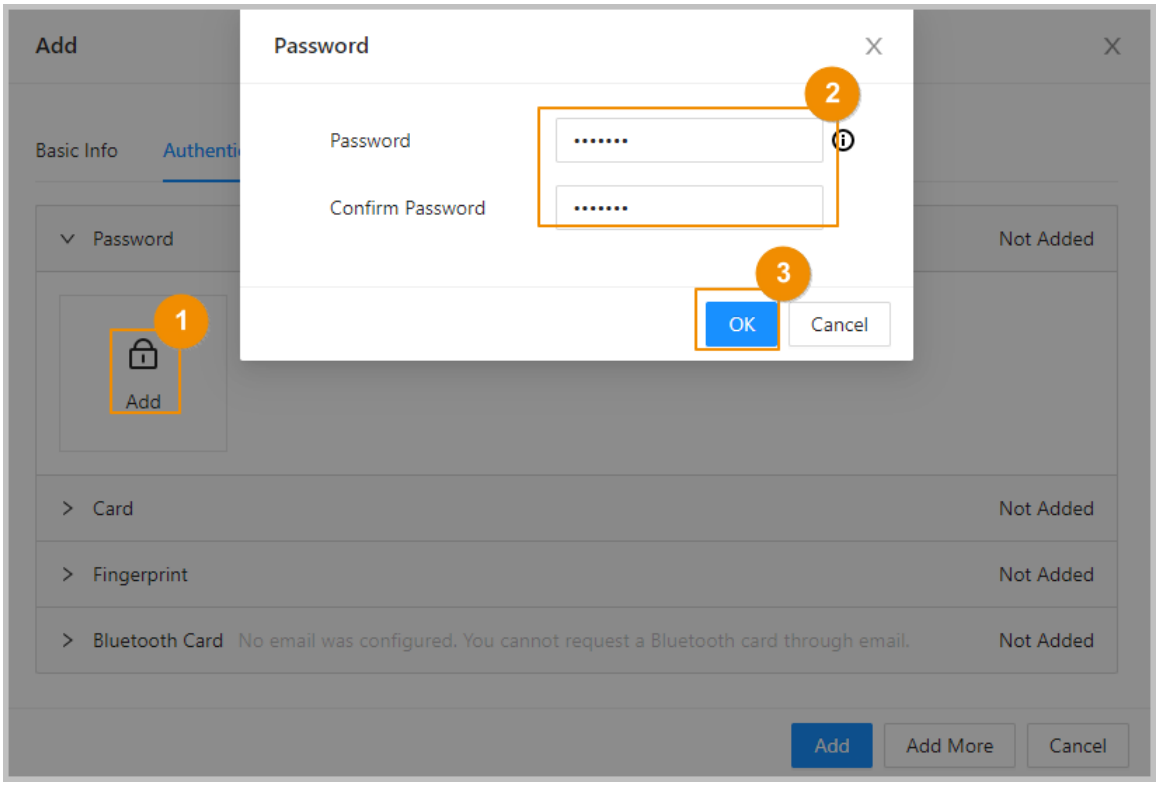
Procedure

Step 1 On the **Authentication** tab, click **Add**

Step 2 Enter and confirm the password.

Step 3 Click **OK**.

Figure 2-18 Add the password



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

2.2.7.4.2 Adding Cards

Add IC cards or ID cards to users for them to gain access by swiping their cards

Procedure

Step 1 (Optional) Before you assign cards to users, set the card type and the type of card number.

1. On the **Person Management** page, select **More** > **Card Type**.
2. If you plan on issuing cards through using enrollment reader, select a card type, and then click **OK**.

Make sure that the card type is the same as the card type that will be issued when you plan on issuing cards through using enrollment reader. For details, see Click Add. Click Modify, and then select Enrollment Reader. Make sure that the card enrollment reader is connected to your computer. Follow the on-screen instructions to download and install the plug-in. Click Read Card, and then swipe the cards on the enrollment reader. A 60-second countdown is displayed to remind you to swipe the card, and the system

will read the card number automatically. If the 60-second countdown expires, click Read Card again to start a new countdown. Click Add. .

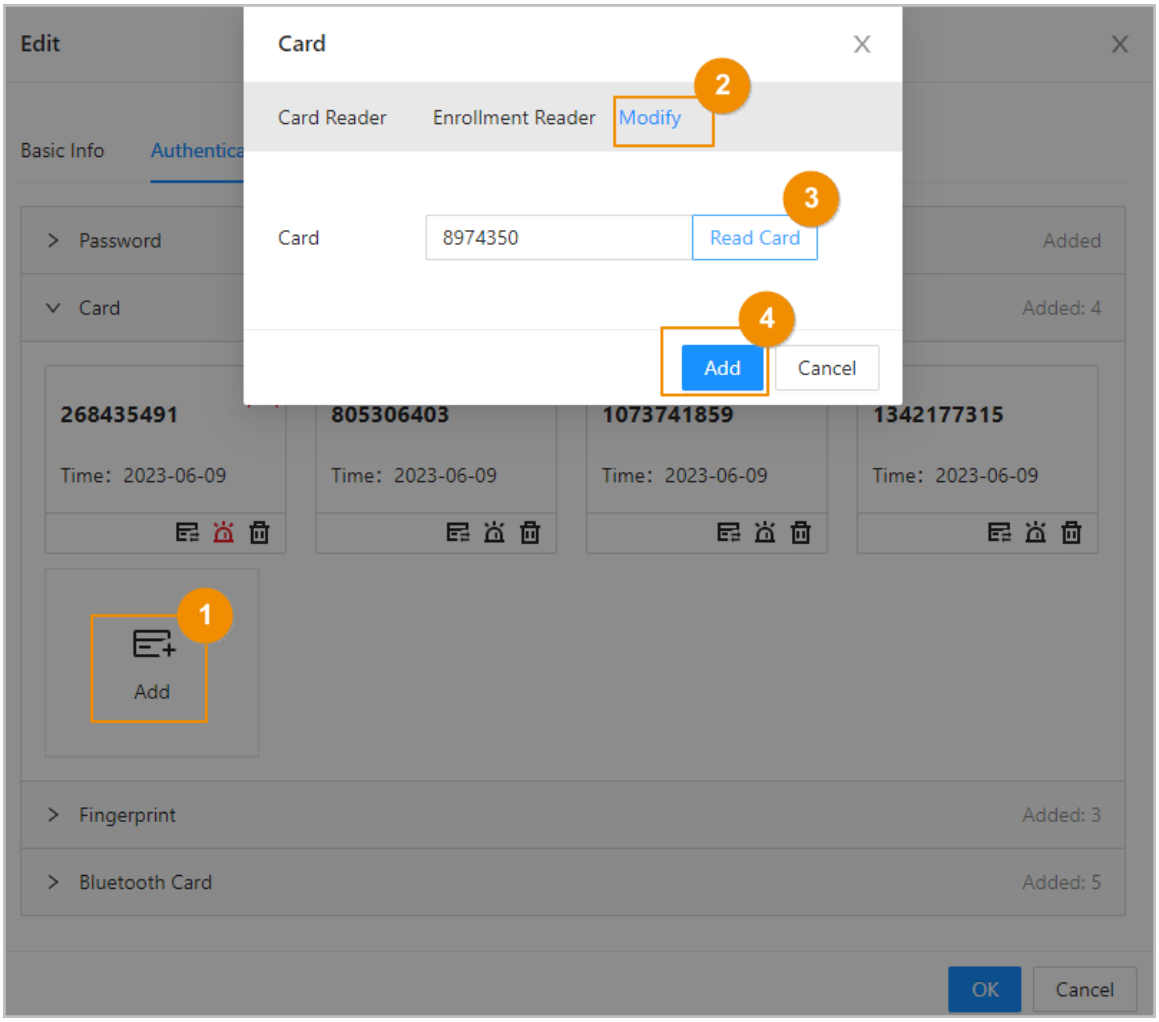
3. Select **More** > **Card No. System**.
4. Select decimal format or hexadecimal format for the card number.

Step 2 On the **Authentication** tab, click **Card** to add cards.

4 methods are available to add cards.

- Enter the card number manually.
  1. Click **Add**.
  2. Enter the card number, and then click **Add**.
- Use the enrollment reader to read the card number.

Figure 2-19 Use the enrollment reader to read the card number



1. Click **Add**.
2. Click **Modify** , and then select **Enrollment Reader**.

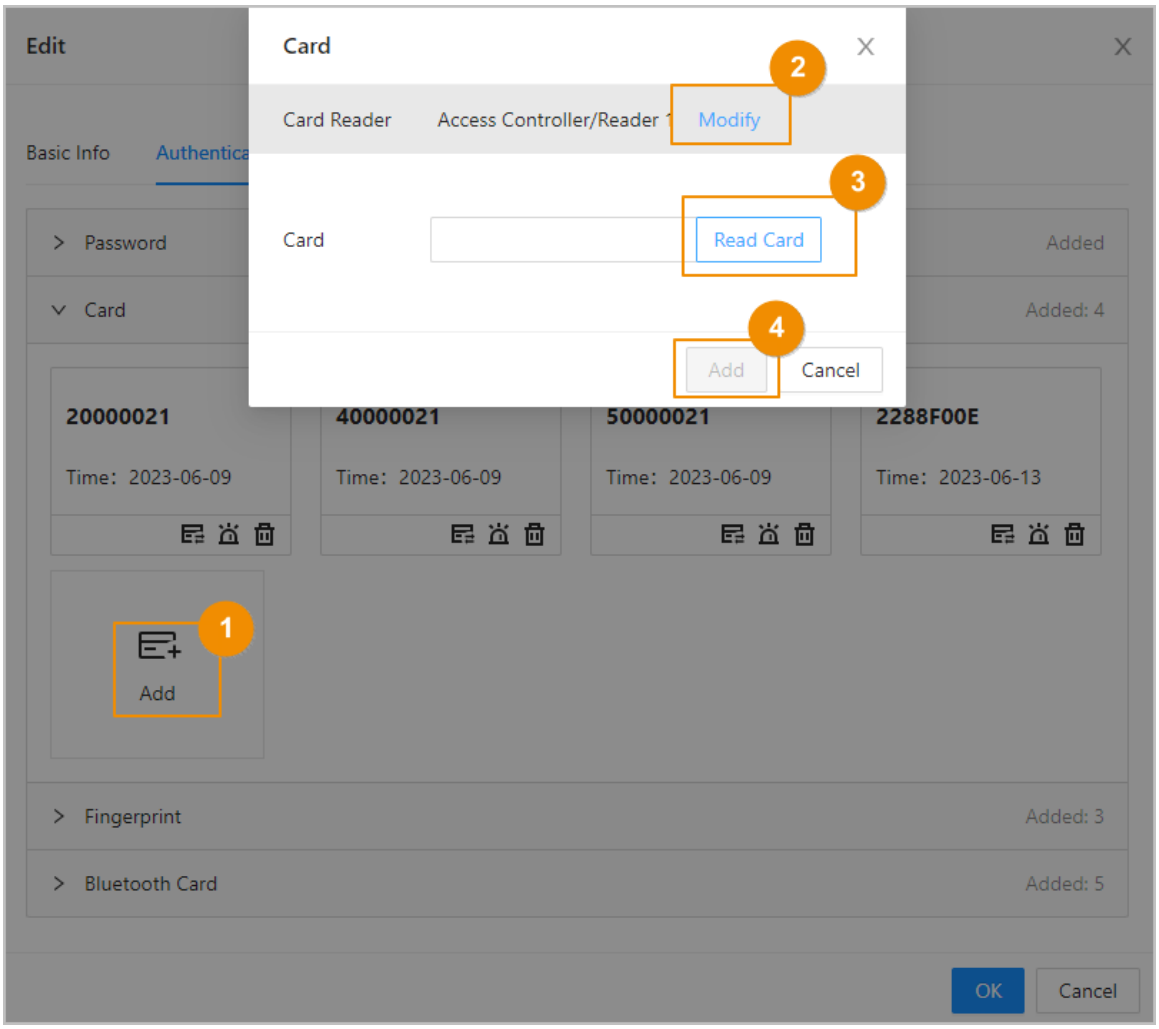
   Make sure that the card enrollment reader is connected to your computer.
3. Follow the on-screen instructions to download and install the plug-in.
4. Click **Read Card**, and then swipe the cards on the enrollment reader.

   A 60-second countdown is displayed to remind you to swipe the card, and the system will read the card number automatically. If the 60-second countdown expires, click **Read Card** again to start a new countdown.

5. Click **Add**.

- Use the card reader to read the card number.

Figure 2-20 Use the card reader to read the card number



1. Click **Modify**, and then select a card reader.

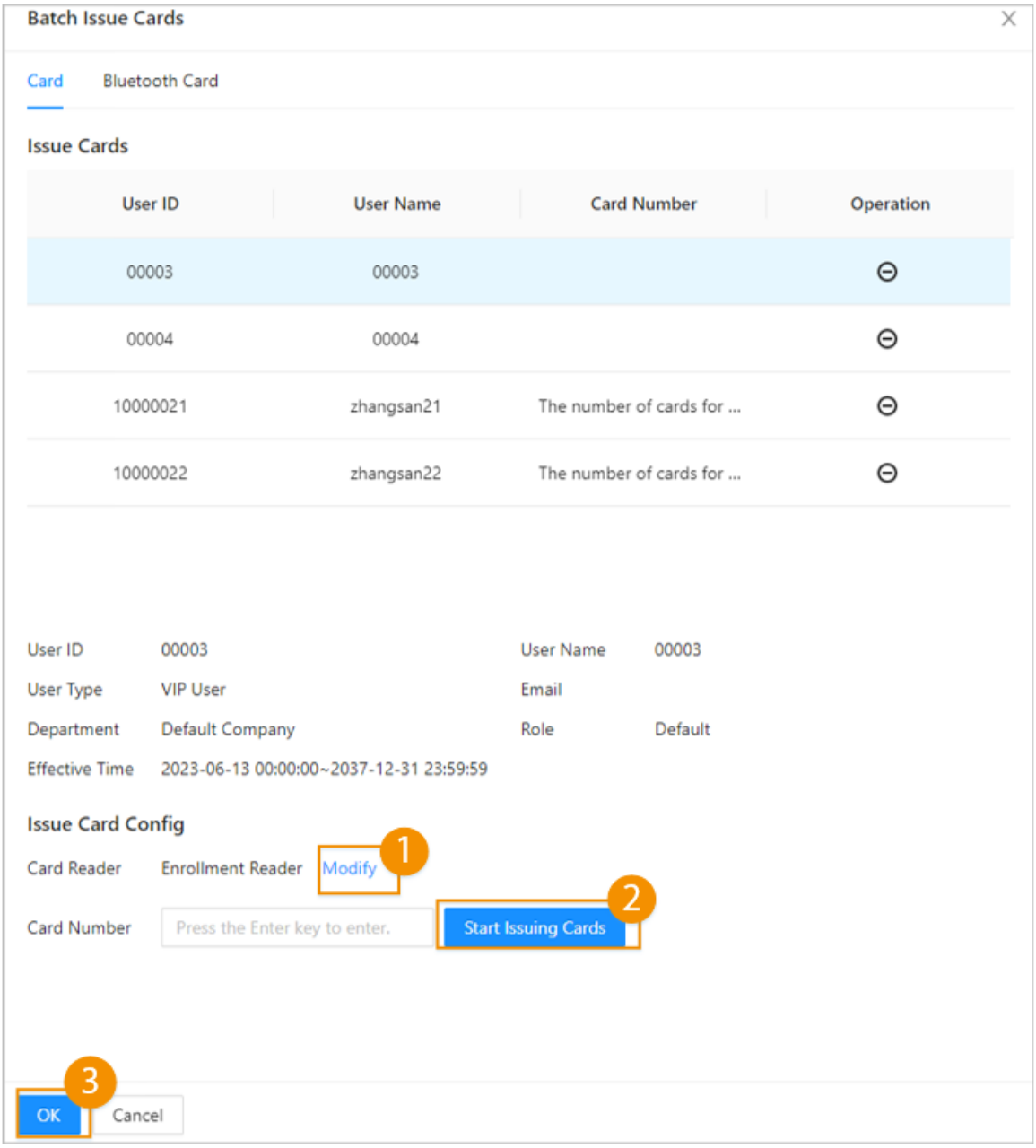
   Make sure that the card reader is connected to the Access Controller.
2. Click **Read Card**, and then swipe the cards on the card reader.

   A 60-second countdown is displayed to remind you to swipe the card, and the system will read the card number automatically. If the 60-second countdown expires, click **Read Card** again to start a new countdown.
3. Click **Add**.

- Add cards in batches: Issue cards to users in batches.

1. Click **Batch Issue Cards** , and then select **Issue Cards to Selected Users** or **Issue Cards to All Users**.
2. You can manually enter the card number, or click **Modify** to issue cards through the enrollment reader or card reader.

Figure 2-21 Issue cards through the enrollment reader or card reader



Related Operations

- : Change the number of the card.
- : Set the card to duress card.

  An alarm is triggered when people use the duress card to unlock the door.
- : Delete the card.

2.2.7.4.3 Adding Fingerprints

Add fingerprints to users for them to use their fingerprint to unlock doors.

Procedure

Step 1 On the **Authentication** tab, click **Fingerprint**.

Step 2 Connect a fingerprint scanner to the computer, and follow the on-screen instructions to register the fingerprint.

Step 3 Click **Add**.

2.2.7.4.4 Adding Bluetooth Cards

Add Bluetooth cards to users for them to gain access through Bluetooth cards.

Prerequisites

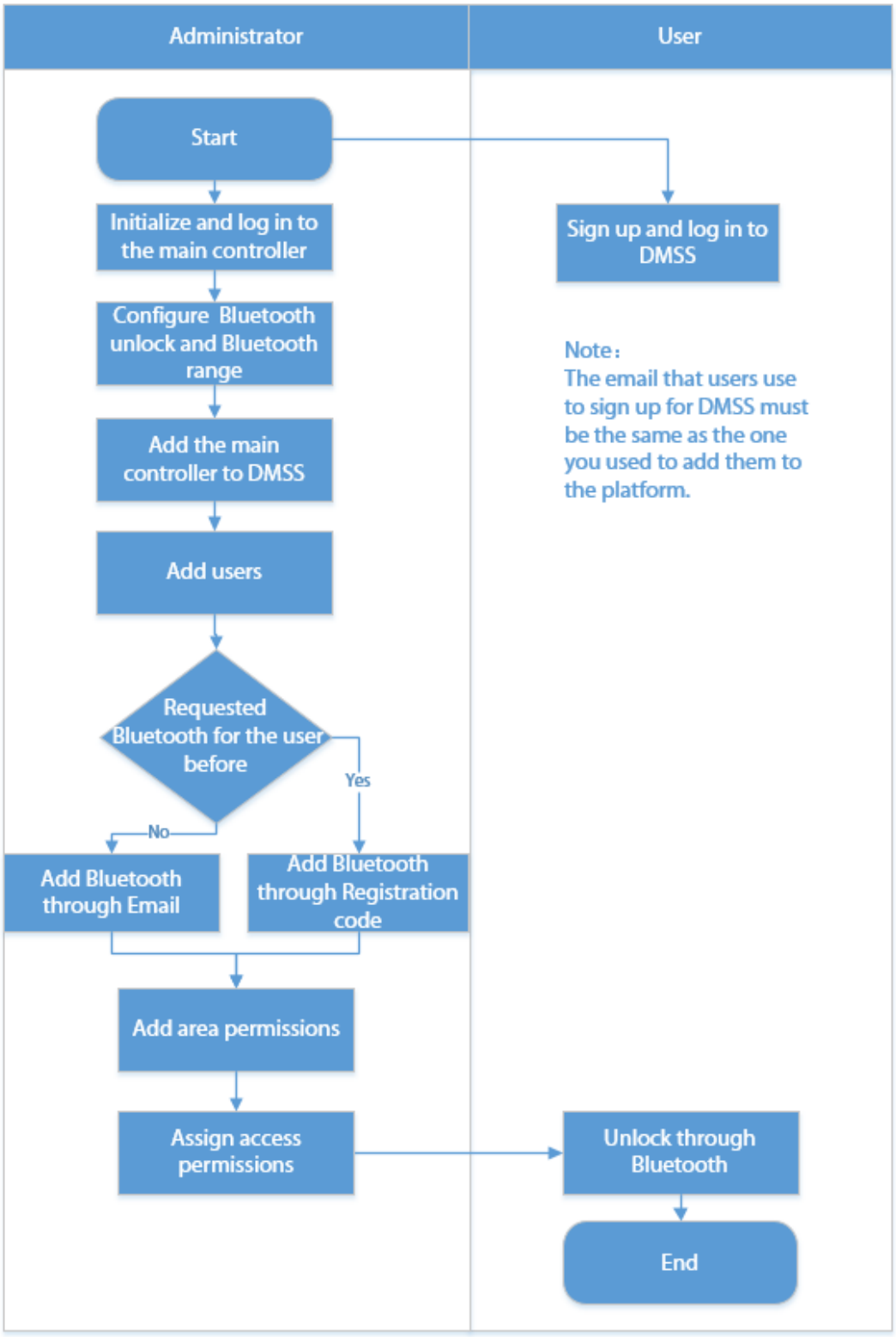
- The Bluetooth unlock function has been turned on.
- The main controller has been added to DMSS. For details, see "2.2.21.4.3 Configuring Cloud Service".
- Users have been added to the Platform of the Access Controller. For details, see "2.2.7.3 Configuring Basic User Information".
- General users, such as company employees, have installed and signed up for DMSS with their email.

The email that users use to sign up for DMSS must be the same as the one you used to add them to the access controller.

Background Information

Refer to the flowchart for configuring Bluetooth unlock. Administrator and general users need to perform different operations to complete the process. General users, like company employees, only need to sign up and log in to DMSS with their email to unlock doors using Bluetooth cards that were issued to them.

Figure 2-22 Flowchart for configuring Bluetooth unlock



Procedure

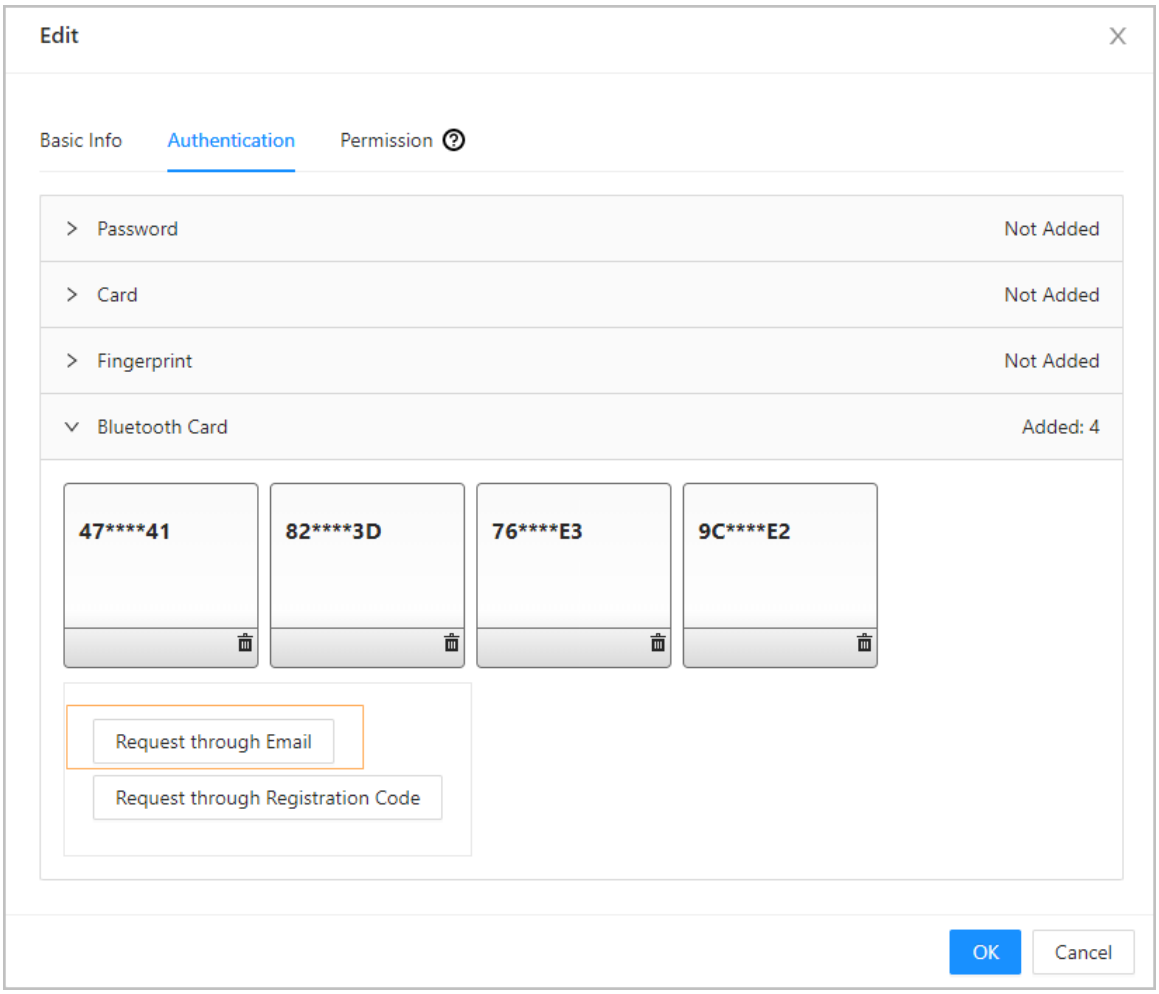
Step 1 On the tab, click **Bluetooth Card**.

3 methods are available to add Bluetooth cards.

- Request through Email one by one: Click **Request through Email**.

  A Bluetooth card is generated automatically. You can generate up to 5 cards for each user.

Figure 2-23 Request through Email



- Request through Email in batches.

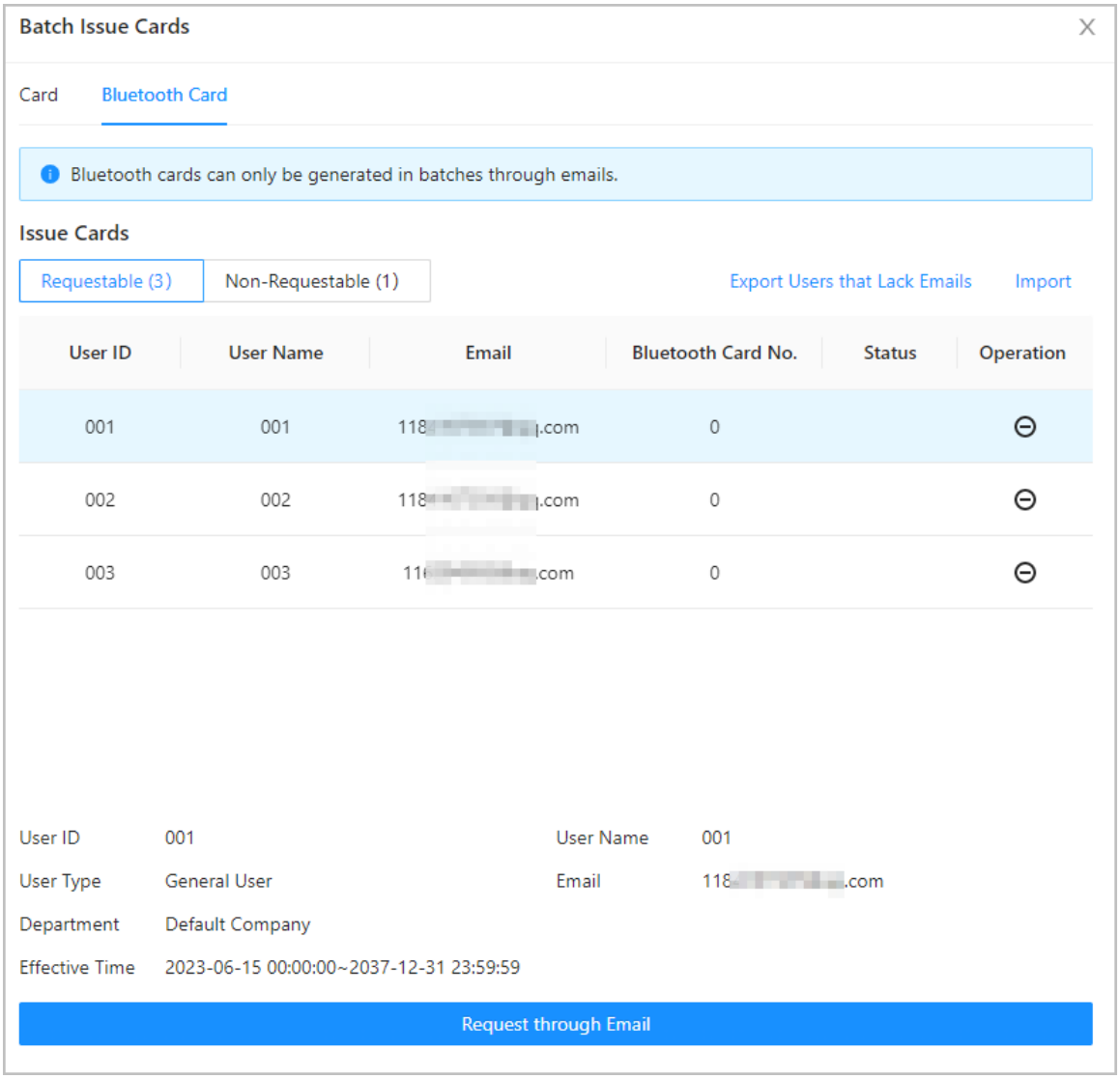
  1. On the **Person Management** page, click **Batch Issue Cards**.

     Batch issue cards only supports requesting through Email.

     - Issue Bluetooth cards to all the users on the list: Click **Issue Cards to All Users**.
     - Issue Bluetooth cards to selected users: Select users, and then click **Issue Cards to Selected Users**.
  2. Click **Bluetooth Card**.
  3. Click **Request through Email**.

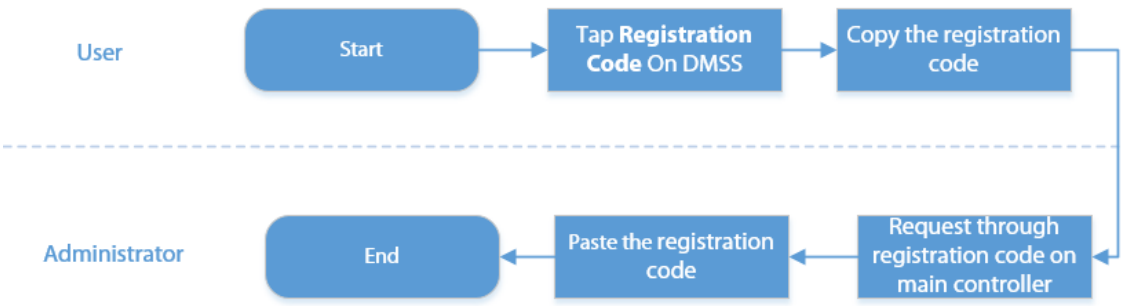
     - Users who do not have an email or already have 5 Bluetooth cards will be displayed on the non-requestable list.
     - Export users that lack emails: Click **Export** , enter the emails in the correct format, and then click **Import**. They will be moved to the requestable list.

Figure 2-24 Batch issue cards



- If you have requested Bluetooth cards for the user before, you can add the Bluetooth cards through registration code. using registration codes.

  Figure 2-25 The flowchart for requesting through registration code

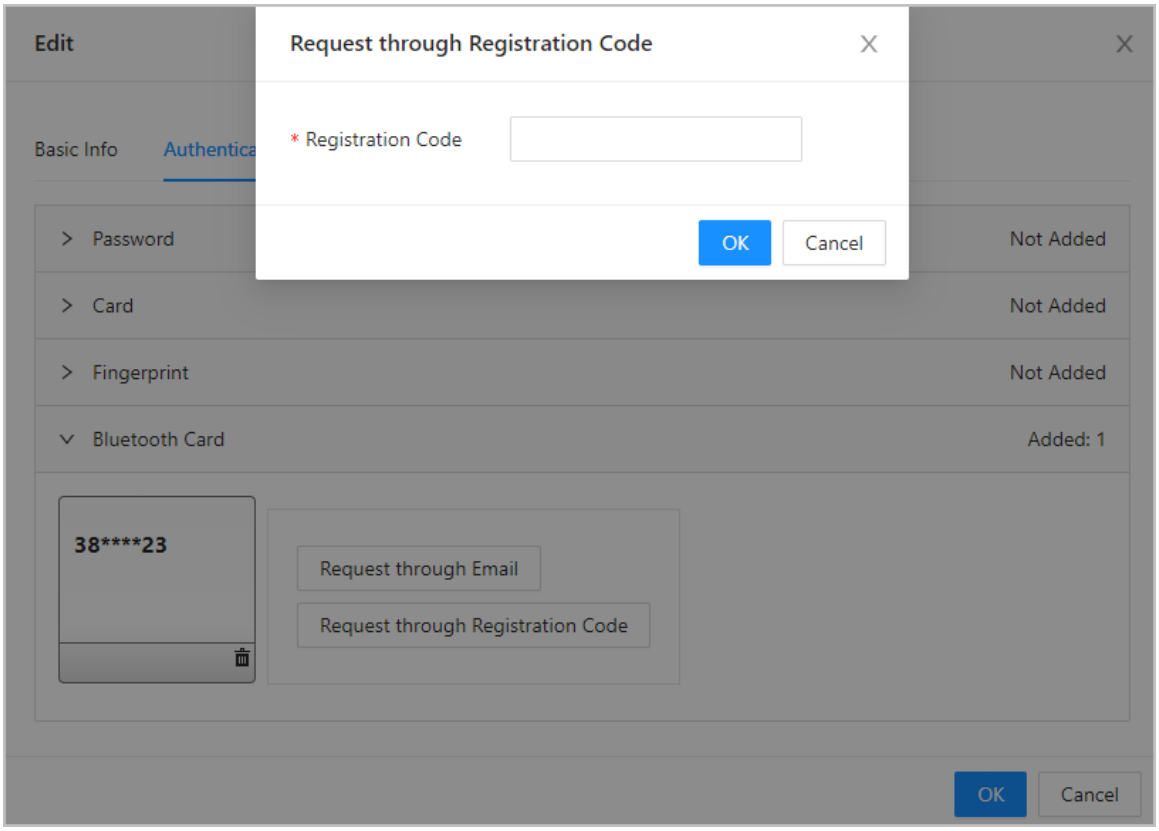


1. On DMSS, tap **Registration Code** of a Bluetooth card.

   The registration code is automatically generated by DMSS.
2. Copy the registration code.

3. On the **Bluetooth Card** tab, click **Request through Registration Code**, paste the registration code, and then click **OK**.

Figure 2-26 Request through registration code



4. Click **OK**.

   The Bluetooth card is added.

Step 2 Click **OK**.

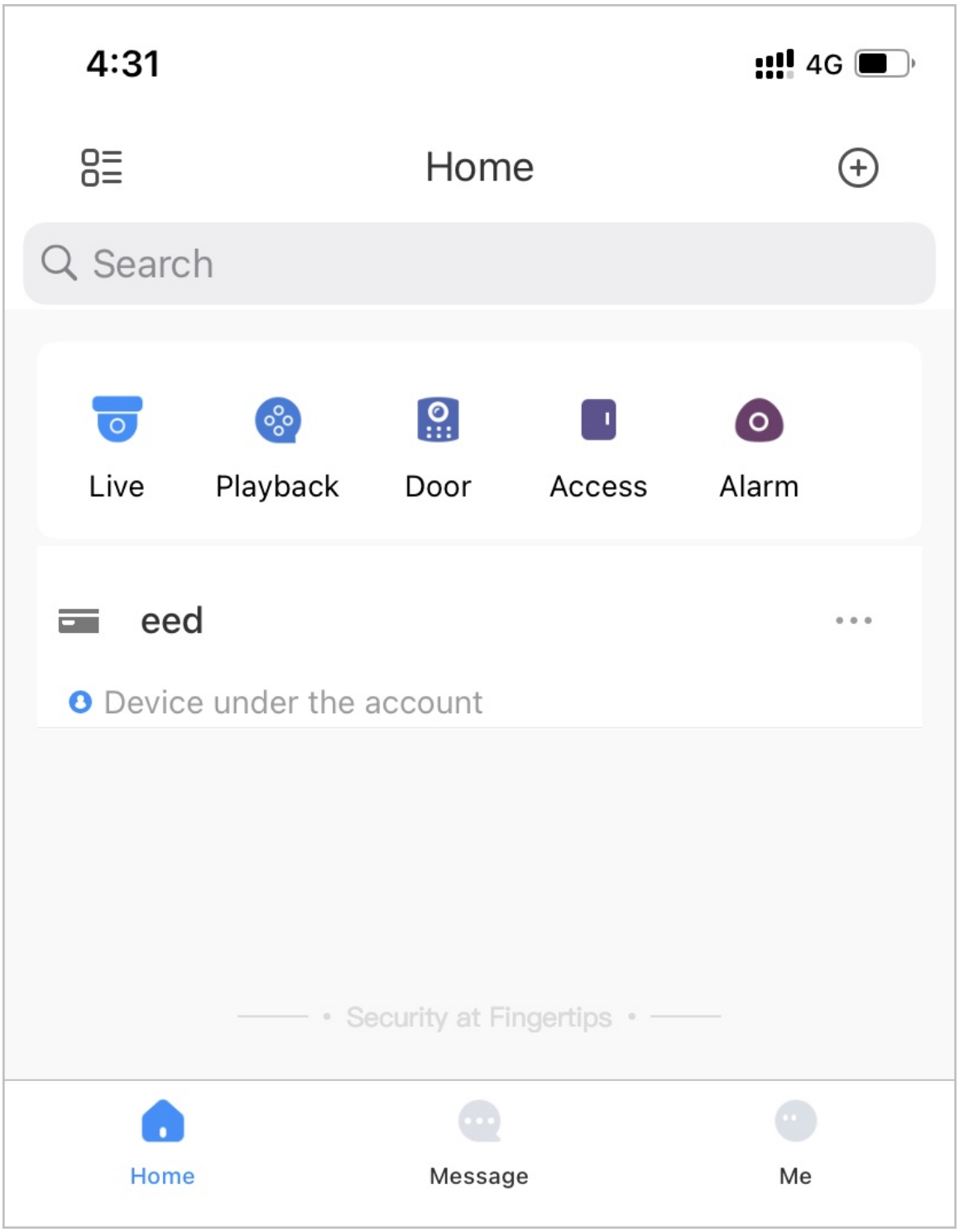
Results

After users sign up and log in to DMSS with the Email address, they can open DMSS to unlock the door through Bluetooth cards. For details, see the user's manual of DMSS.

- Auto Unlock: The door automatically unlocks when you are in the defined Bluetooth range, which allows the Bluetooth card to transmit signals to the card reader.

  In auto unlock mode, the Bluetooth card might continuously unlock the door when you are within the Bluetooth range for a long time until a failure occurs. Please turn off Bluetooth on the phone and then turn it on again.
- Shake to Unlock: The door unlocks when you shake your phone to allow the Bluetooth card to transmit signals to the card reader.

Figure 2-27 Unlock the door through Bluetooth cards

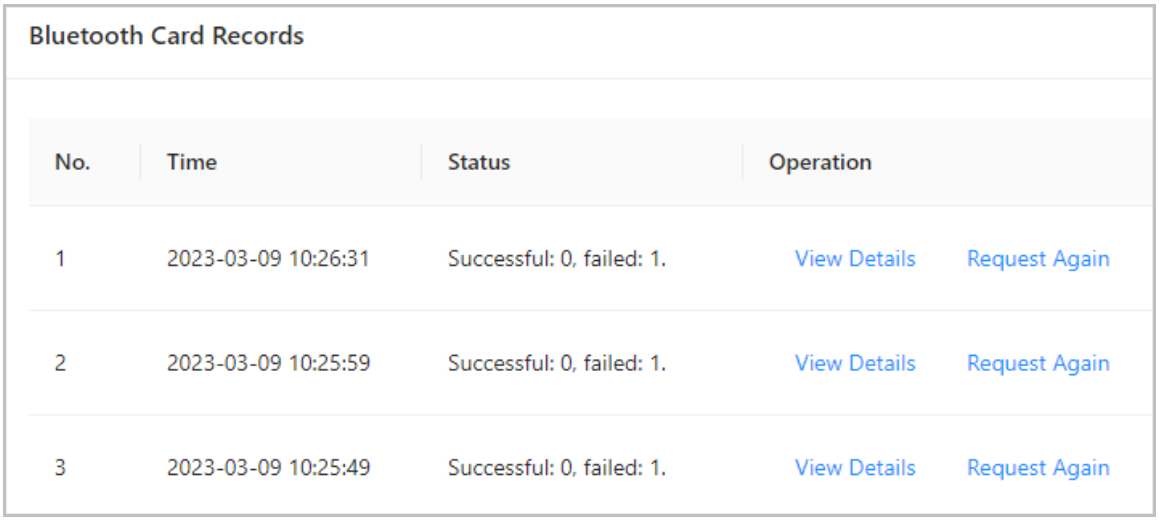


Related Operations

- Users can manage Bluetooth cards on DMSS.
  - Move to the Top: If multiple Bluetooth cards have been added, you can move cards to the top that are currently in use.
  - Rename: Rename the Bluetooth card.
  - Delete: Delete the Bluetooth card.
- Export users that lack emails: Click **Export**, enter the emails in the correct format and then click Import. They will be moved to the requestable list.

- View the request records: On the **Person Management** page, click **More** > **Bluetooth Card Records** to view the request status.

Figure 2-28 Request status



  - ◇ View Details: View the details of the request, including user information, reasons for failed requests and more. You can also request again for failed users.
  - ◇ Request Again: Request again for failed users.

2.2.8 Adding Weekly Plans

The weekly plan is used to set the unlock schedule for the week. The platform offers a default template with a full daytime schedule. You can also create your own templates.

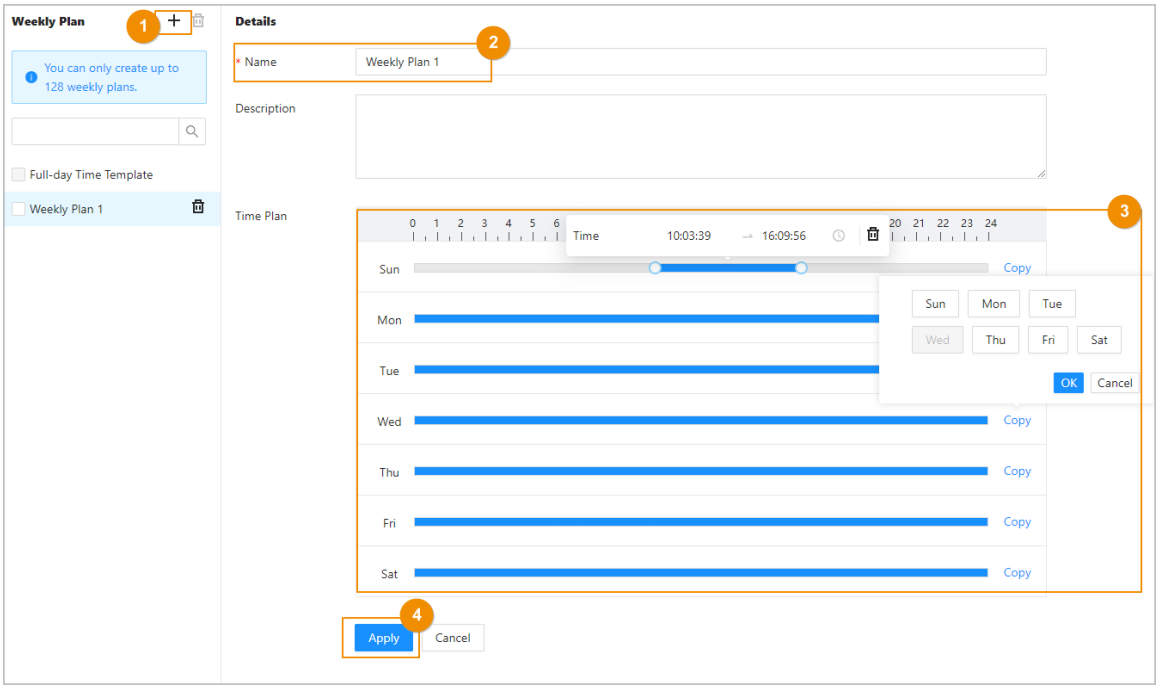
Procedure

Step 1 On the home page, select **Access Control Config** > **Weekly Plan**, and then click +.

- The default full-day time template cannot be modified.
- You can create up to 128 weekly plans.

Step 2 Enter the name of the time template.

Figure 2-29 Create the weekly plan



Step 3 Drag the slider to adjust the time period for each day.

You can also click **Copy** to apply the configured time period to other days.

You can only configure up to 4 time sections for each day.

Step 4 Click **Apply**.

2.2.9 Adding Holiday Plans (Optional)

The holiday plan is used to set the unlock schedule for holidays.

Procedure

Step 1 On the home page, select **Access Control Config** > **Holiday Plan**, and then click +.

You can create up to 128 holiday plans.

Step 2 Enter the name of the holiday plan.

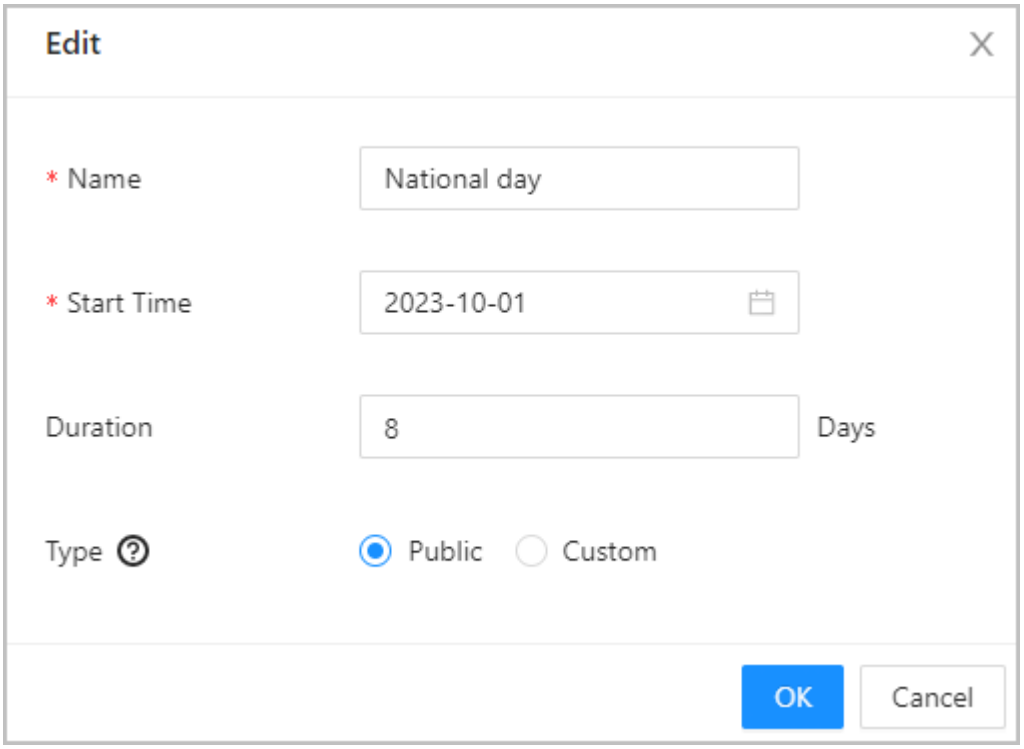
Step 3 Drag the slider to adjust the time period for each day.

You can only configure up to 4 time sections for each day.

Step 4 Click **Add** to add holidays to the holiday plan, and then click **OK**.

- Public: The holiday will be shared with all your holiday plans.
- Custom: The holiday is only used on the current holiday plan.

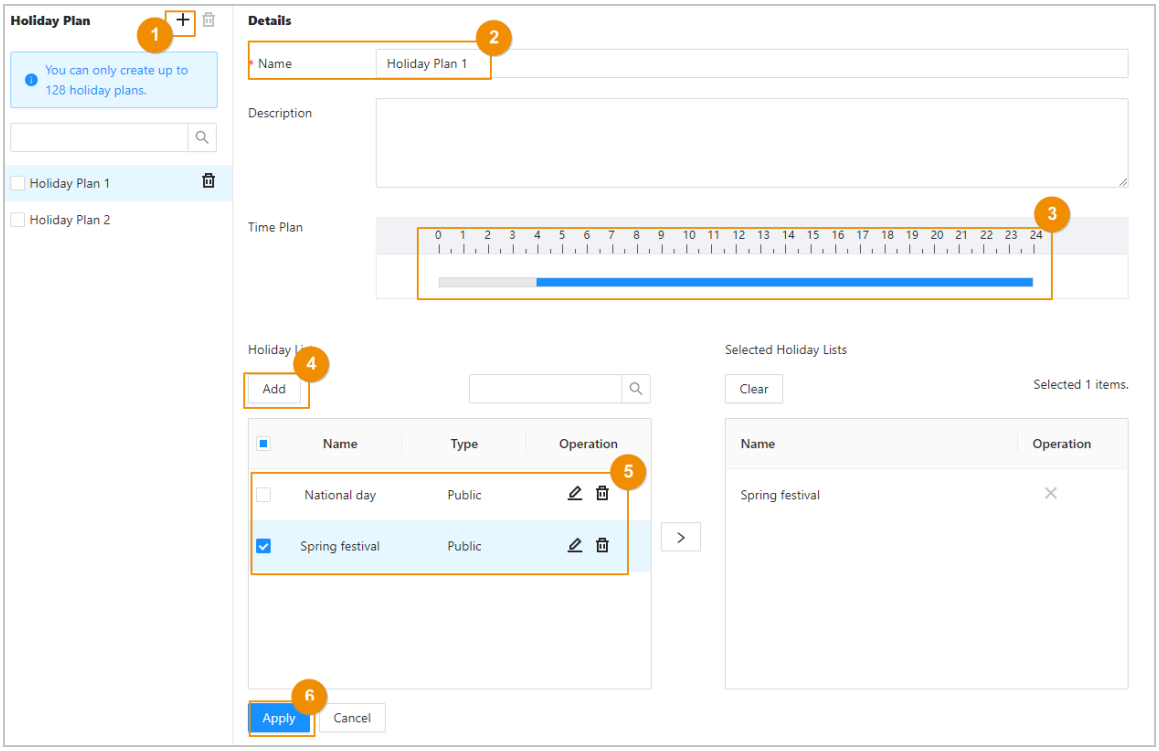
Figure 2-30 Add holidays



Step 5 Select holidays.

Step 6 Click **Apply**.

Figure 2-31 Create holiday plan



2.2.10 Adding Areas

An area is a collection of door access permissions. Create an area, and then link users to the area so that they can gain access permissions set for the area.

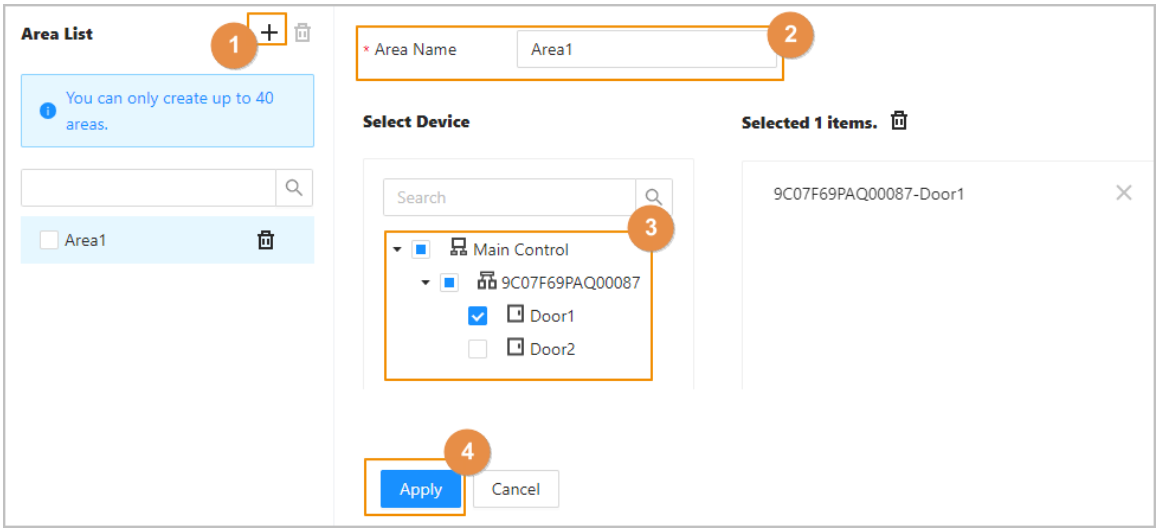
Procedure

Step 1 Click **Access Control Config** > **Area Settings**.

Step 2 Click + to add areas.

You can add up to 40 area permissions.

Figure 2-32 Add areas



Step 3 Enter the name of the area.

Step 4 Select doors.

Step 5 Click **Apply**.

2.2.11 Adding Permission Rules

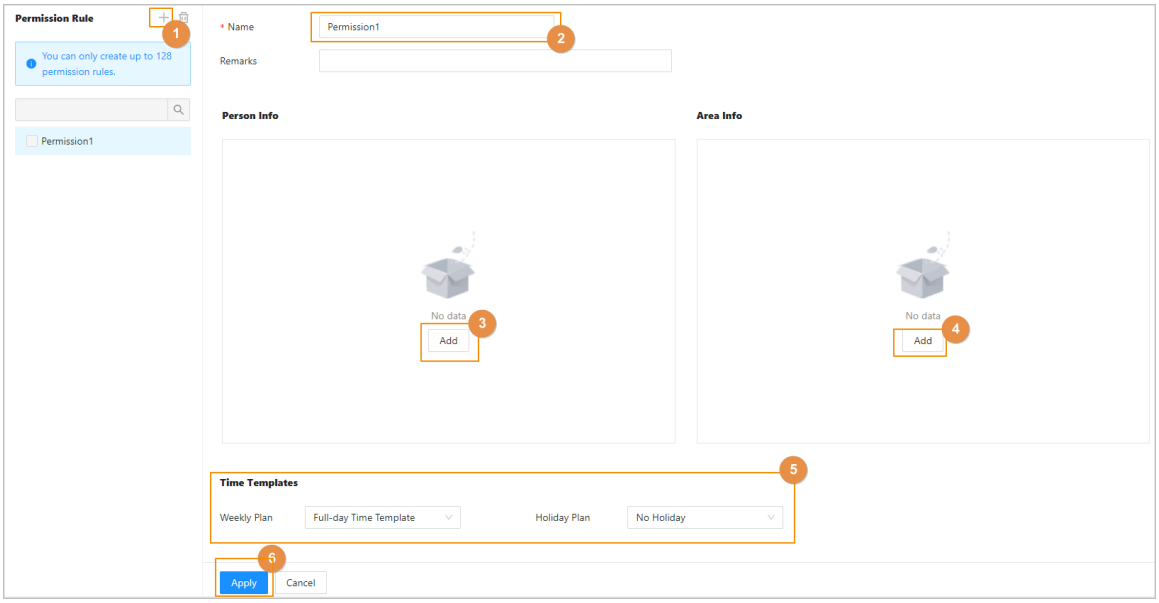
By creating permissions rules, you can assign access permissions to users by linking them to the areas. This will allow authorized personnel to gain access to secure areas.

Procedure

Step 1 On the home page, select **Access Control Config** > **Permission Settings**.

Step 2 Click + to add a permission rule.

Figure 2-33 Assign permissions in batches



Step 3 Enter the name of the permission rule.

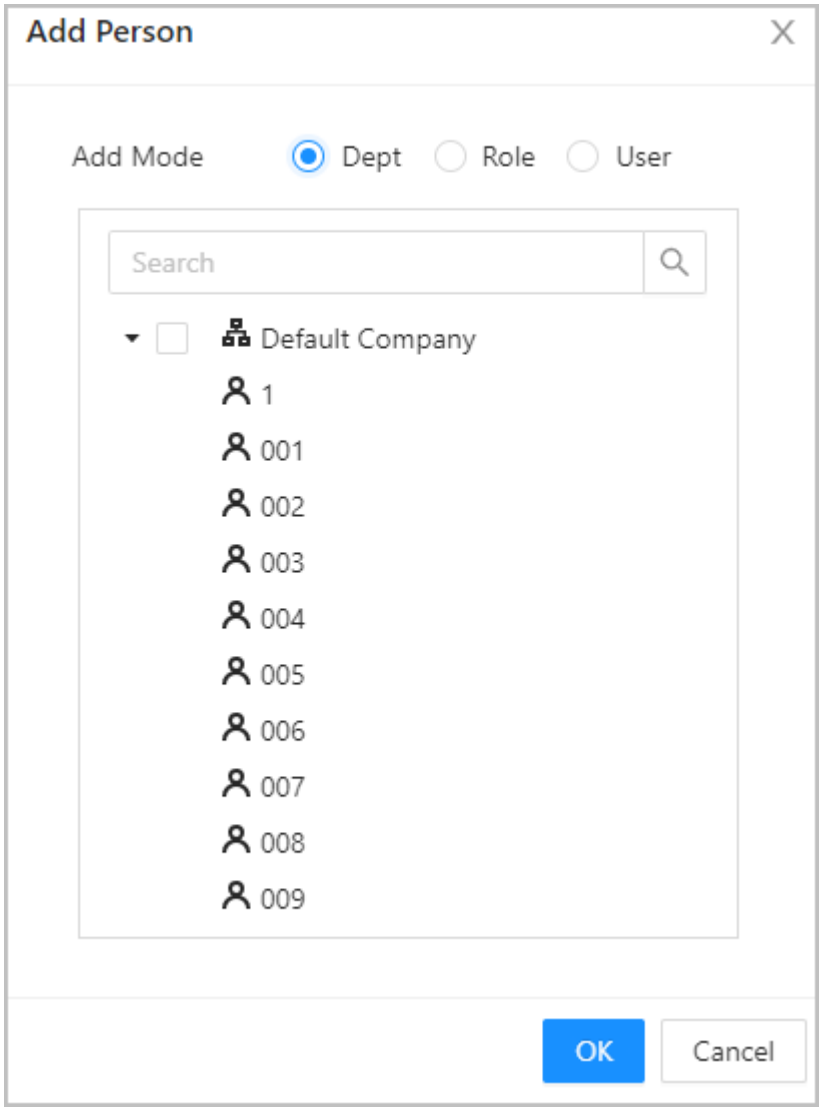
Step 4 In the **Person Info** area, click **Add** to select personnel, and then click **OK**.

You can select personnel on the department, role or individual users.

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

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

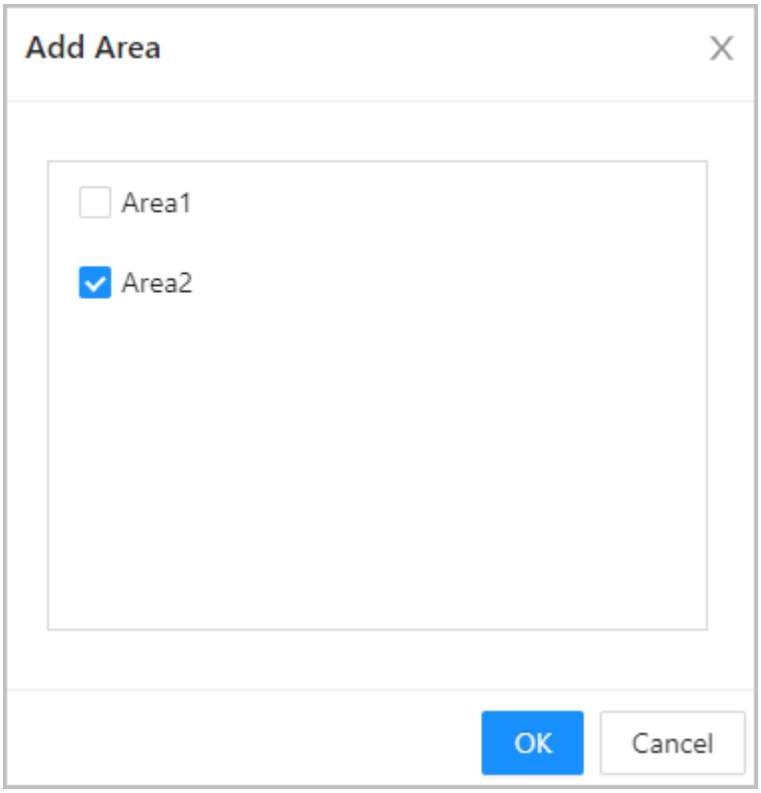
Figure 2-34 Add personnel



You can click + to create new permission groups. For details on creating permission groups, see "2.2.10 Adding Areas".

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

Figure 2-35 Add area



Step 6 In the **Time Templates** area, select the weekly plan and the holiday plan.

Step 7 Click **Apply**.

Related Operations

2.2.12 Viewing Authorization Progress

After you assign access permissions to users, you can view the authorization process.

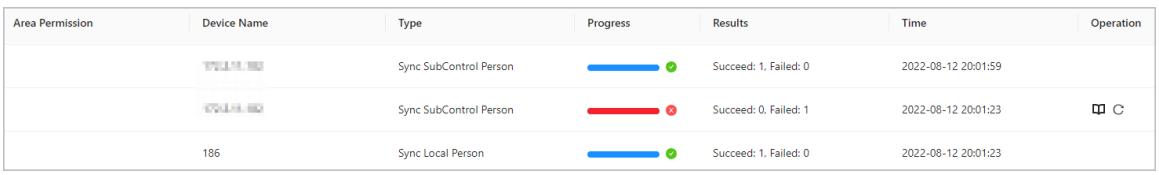
Procedure

Step 1 On the home page, select **Access Control Config** > **Authorization Progress**.

Step 2 View the authorization progress.

- Sync SubControl Person: Sync personnel on the main controller to the sub-controller.
- Sync Local Person: Sync personnel on the management platform of the main controller to its server.
- Sync Local Time: Sync the time templates in the area permissions to the sub-controller.

Figure 2-36 Authorization progress



Step 3 (Optional) If authorization failed, click to try again.

You can click to view details on the failed authorization task.

2.2.13 Configuring Access Control (Optional)

2.2.13.1 Configuring Basic Parameters

Procedure

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

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

Figure 2-37 Basic parameters

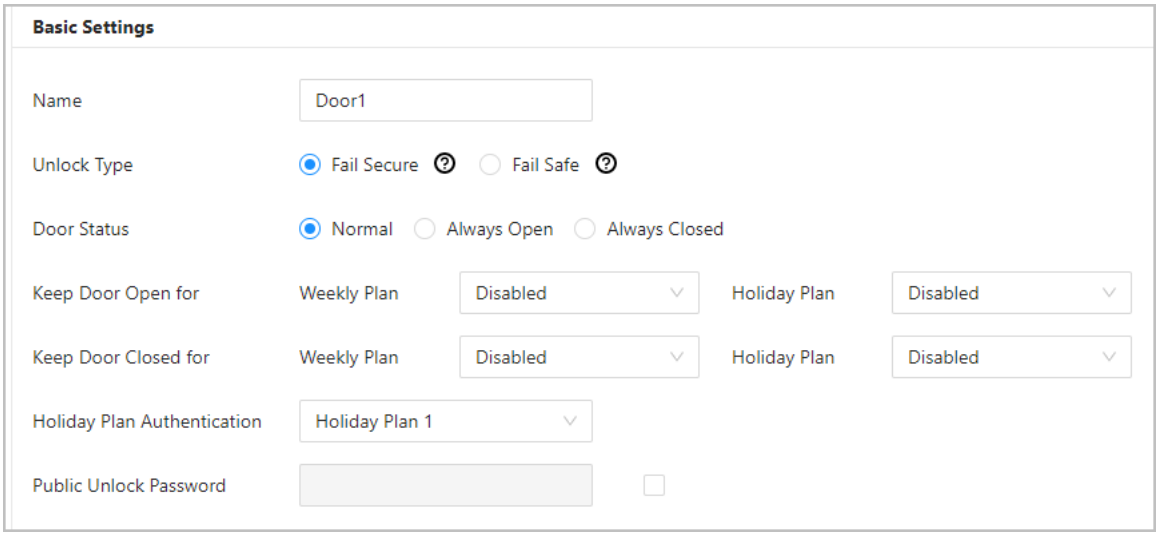


Table 2-8 Basic parameters description

Parameter	Description
Name	The name of the door.
Unlock Type	• If you selected **12 V** to supply power for the lock through the controller during the log-in wizard, you can set fail secure or fail safe. ◇ Fail secure: When the power is interrupted or fails, the door stays locked. ◇ Fail safe: When the power is interrupted or fails, the door automatically unlocks to allow people to leave. • If you selected **Relay** to supply power for the lock through the relay during the login wizard, you can set relay open or relay close. ◇ Relay open=locked: Set the lock to remain locked when the relay is open. ◇ Relay open=unlocked: Set the lock to unlock when the relay is open.
Door Status	Set the door status. • **Normal** : The door will be unlocked and locked according to your settings. • **Always Open** : The door remains unlocked all the time. • **Always Closed** : The door remains locked all the time.

Parameter	Description
Keep Door Open For	The door remains open during the defined week plan or holiday plan.
Keep Door Closed For	The door remains closed during the defined week plan or holiday plan.
Holiday Plan Authentication	Authorized access is allowed for always closed door in the defined holiday plan.
Normally Closed 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.
Public Unlock Password	Turn on this function, and then enter a password, and then you can unlock the door by only entering the public password.

2.2.13.2 Configuring Unlock Methods

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

Procedure

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

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

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

     Bluetooth card can not be selected when you set the combination method to **And**.
  3. Select unlock methods, and then configure other parameters.

Figure 2-38 Unlock settings

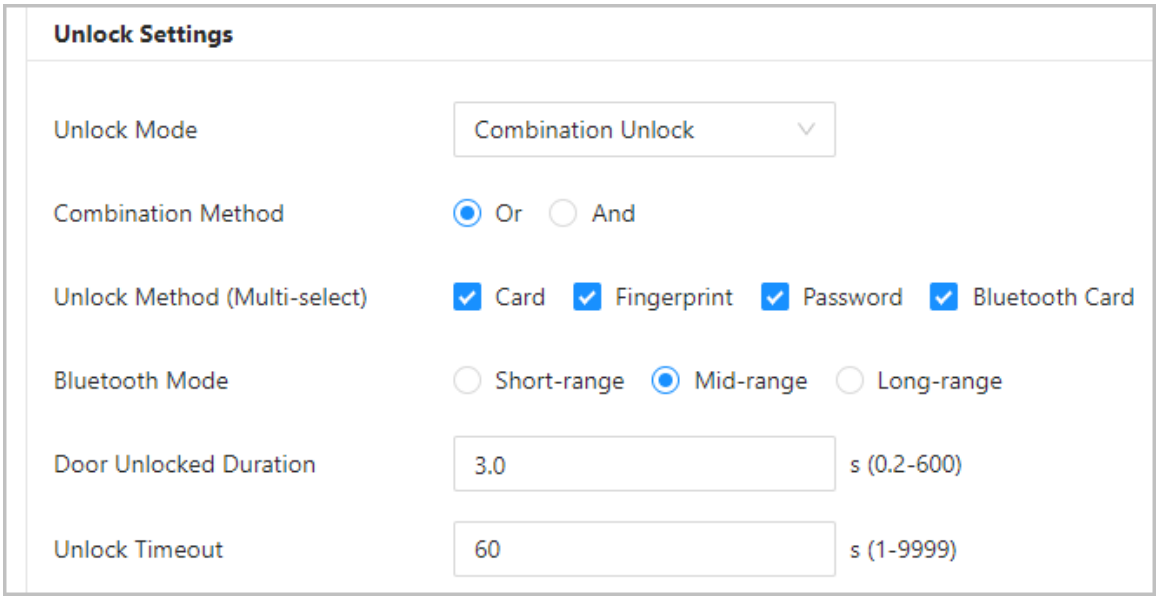


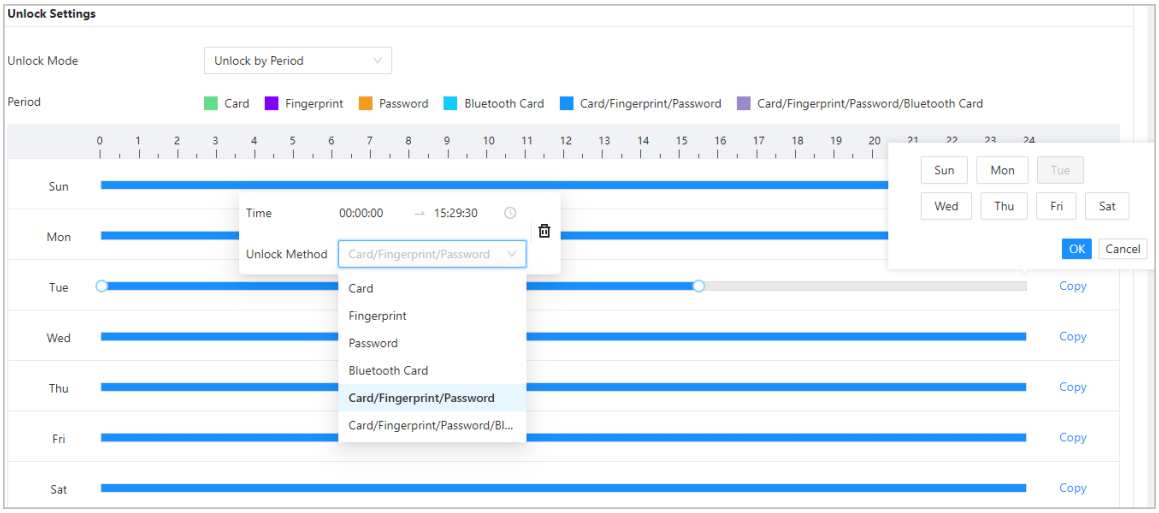
Table 2-9 Unlock settings description

Parameter	Description
Unlock Method (Multi-select)	Supports unlocking through card, fingerprint, password or Bluetooth card. The Bluetooth card function is turned off by default.
Bluetooth Mode	The Bluetooth card must be a certain distance away from the access control device to exchange data and unlock the door. Following are the ranges that are most suitable for it. • Short-range: The Bluetooth unlock range is less than 0.2 m. • Mid-range: The Bluetooth unlock range is less than 2 m. • Long-range: The Bluetooth unlock range is less than 10 m. ⚠ The Bluetooth unlock range might differ depending on models of your phone and the enviroment.
Door Unlock Duration	After a person is granted access, the door will remain unlocked for a defined time for them to pass through. It ranges from 0.2 s to 600 seconds.
Unlock Timeout	A timeout alarm is triggered when the door remains unlocked for longer than the defined value.

- Unlock by period
  1. In the **Unlock Mode** list, select **Unlock by Period**.
  2. Drag the slider to adjust time period for each day.
     
     You can also click **Copy** to apply the configured time period to other days.
  3. Select an unlock method for the time period, and then configure other parameters.

You can only configure up to 4 time sections for each day.

Figure 2-39 Unlock by period



Step 3 Click **Apply**.

2.2.13.3 Configuring Alarms

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

Procedure

Step 1 Select **Access Control Config** > **Door Parameters** > **Alarm Settings**.

Step 2 Configure alarm parameters.

Figure 2-40 Alarm

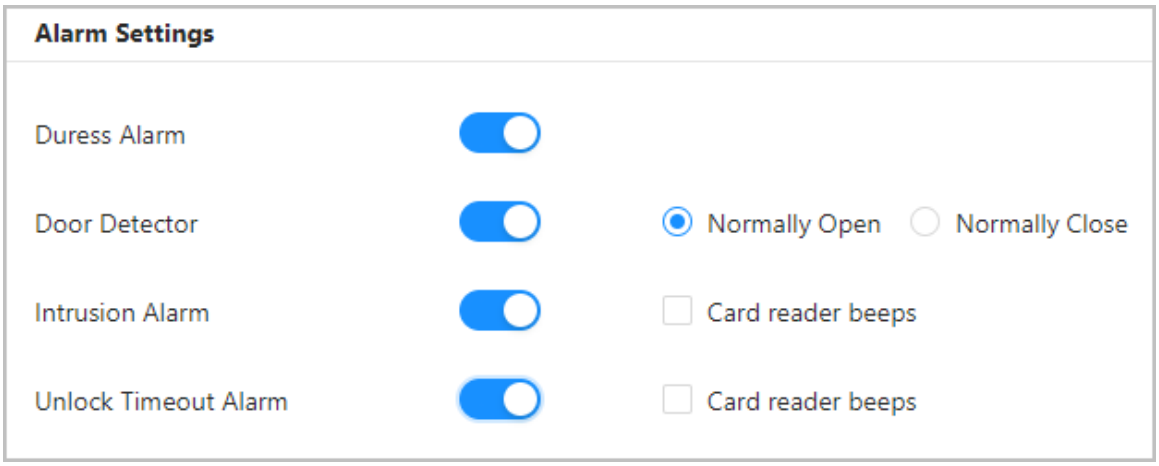


Table 2-10 Description of alarm parameters

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

Parameter	Description
Intrusion Alarm	• When door detector is enabled, an intrusion alarm will be triggered if the door is opened abnormally. • A timeout alarm will be triggered if the door remains unlocked longer than the defined unlock time. • When **Card reader beeps** is enabled, the card reader beeps when the intrusion alarm or timeout alarm is triggered.
Unlock Timeout Alarm	

Step 3 Click **Apply**.

2.2.14 Configuring the Password Unlock

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

Background Information

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

Procedure

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

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

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

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

2.2.15 Configuring Global Alarm linkages (Optional)

You can configure global alarm linkages across different Access Controllers.

Procedure

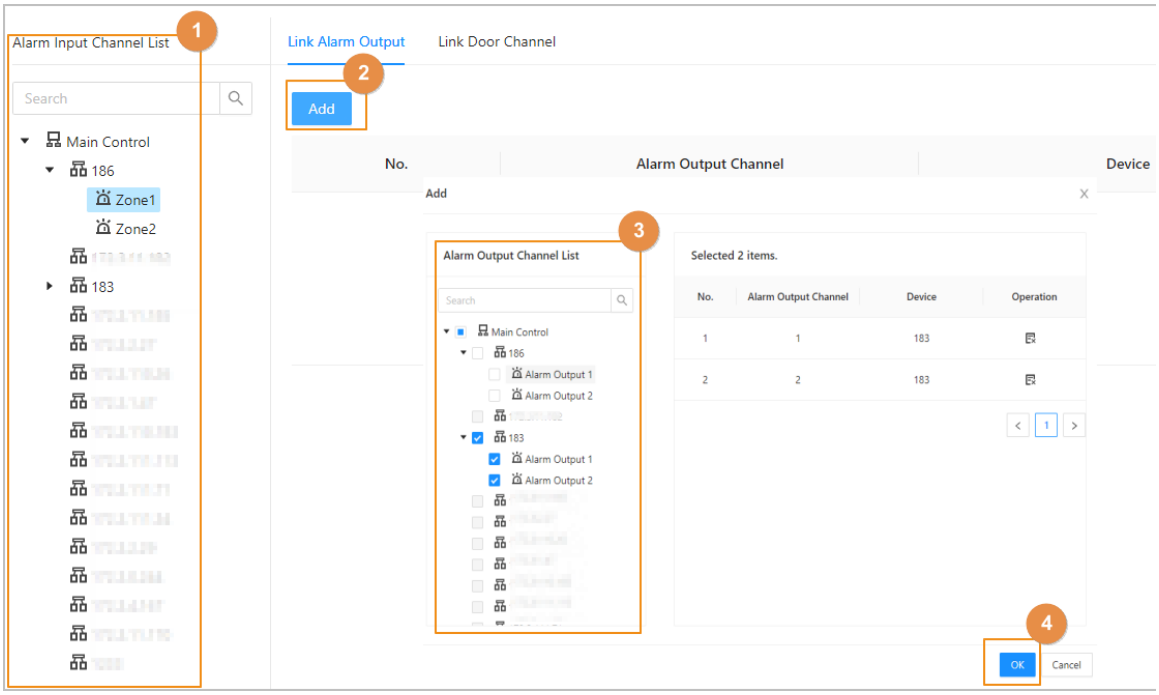
Step 1 Select **Access Control Config** > **Global Alarm Linkage**.

- When you have configured both global alarm linkages and local alarm linkages, and if the global alarm linkages conflict with the local alarm linkages, the last alarm linkages you have configured will take effective.
- When you have configured alarm linkages for sub controllers through the main controller, if the main controller has been restored to the factory defaults, we recommended you restore the sub controller to factory defaults at the same time.

Step 2 Configure the alarm output.

1. Select an alarm input from the alarm input channel list, and then click **Link Alarm Output**.
2. Click **Add** , select an alarm output channel, and then click **OK**.

Figure 2-41 Alarm output

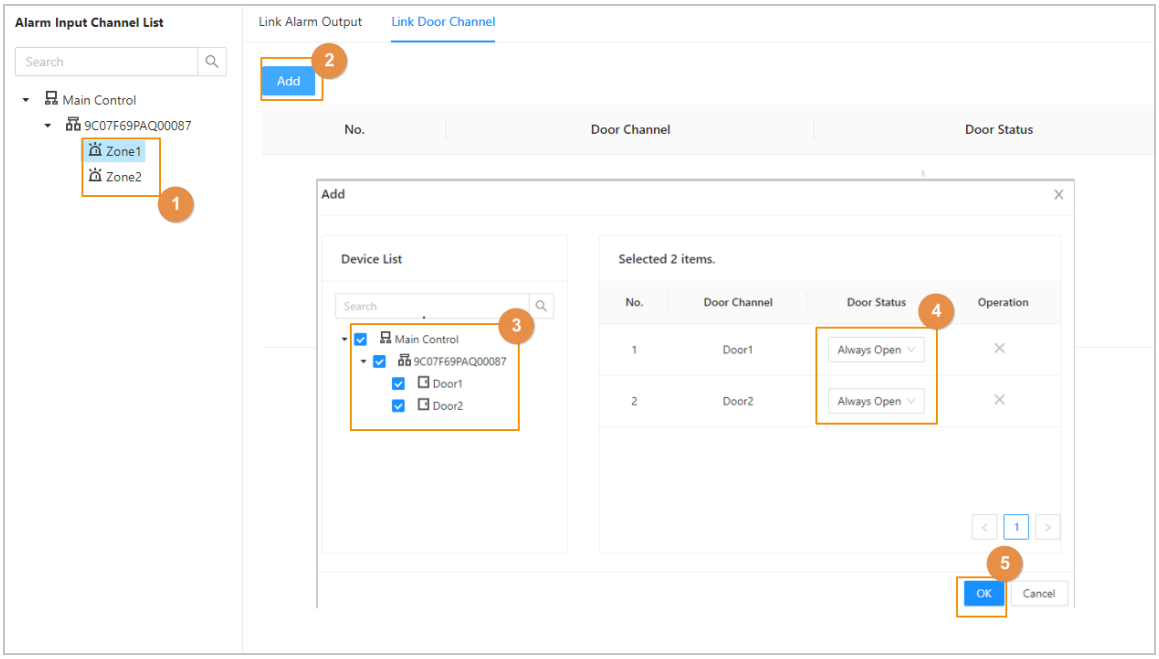


3. Turn on the alarm output function and then enter the alarm duration.
4. Click **Apply**.

Step 3 Configure the door linkage.

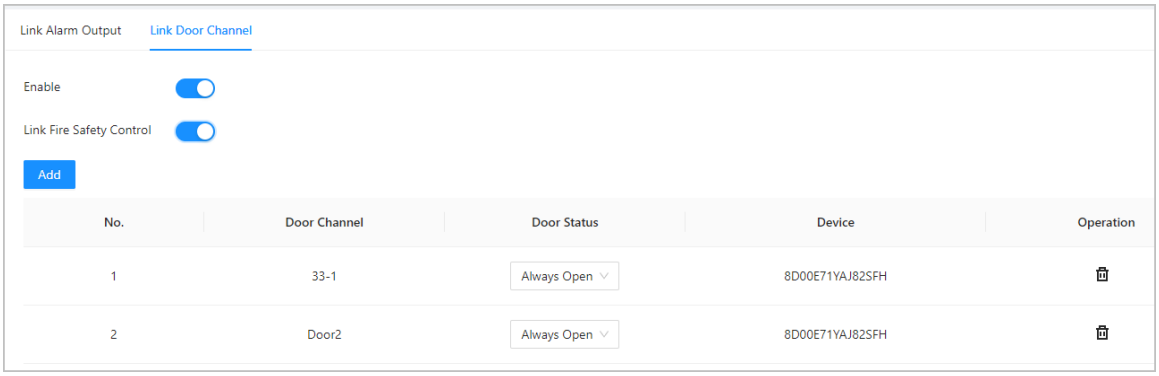
1. Select an alarm input from the channel list, and then click **Add**.
2. Select the linkage door, select the door status, and then click **OK**.
   - Always Closed: The door automatically locks when an alarm is triggered.
   - Always Open: The door automatically unlocks when an alarm is triggered.

Figure 2-42 Door linkage



3. Click **Enable** to turn on the door linkage function.

Figure 2-43 Door linkage



If you turn on link fire safety control, all door linkages will automatically change to the **Always Open** status, and all the doors will open when the fire alarm is triggered.

4. Click **Apply**.

   You can click **Copy to** to apply the pre-configured alarm linkages to other alarm input channels.

2.2.16 Configuring First Card Unlock

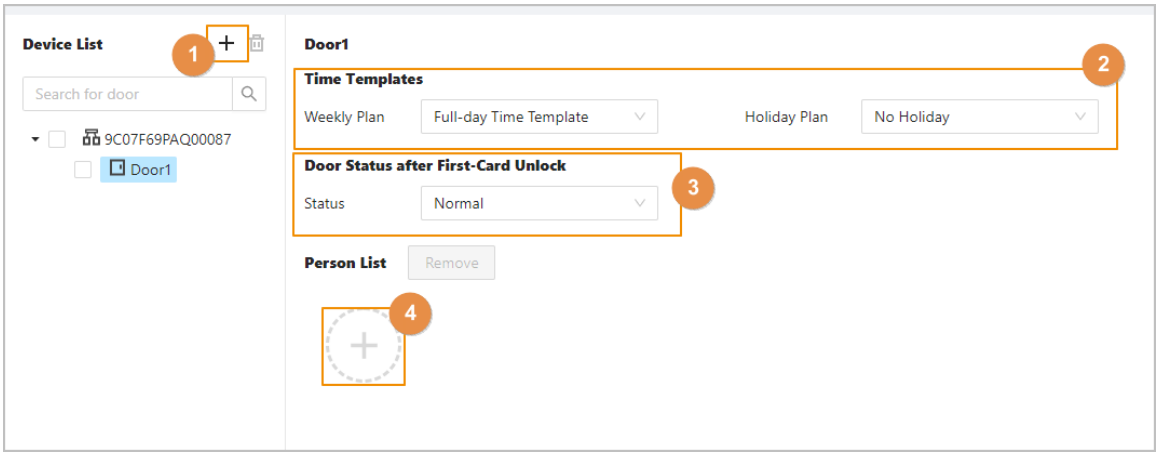
Define certain people as the first-card holders, other users can verify their identities to unlock the door only after the first-card holders verify their identities first.

Procedure

Step 1 Select **Access Control Config** > **First-card Unlock**.

Step 2 In the device list, click +, and then select the door.

Figure 2-44 Assign first-card permission to users



Step 3 Select the weekly plan and the holiday plan.

First-card is valid only during the defined time.

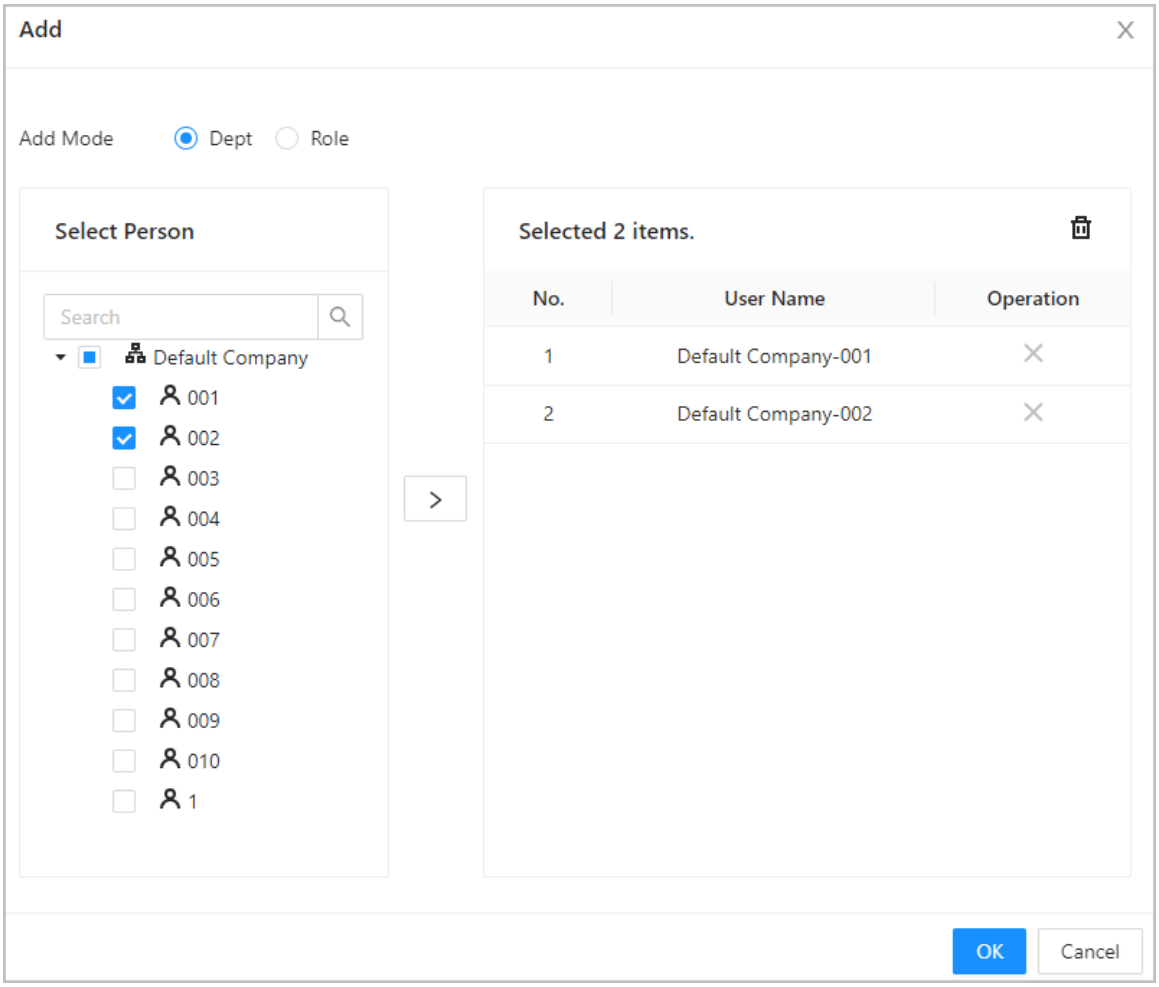
Step 4 Select the door status.

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

Step 5 Click ⊕ to add first-card users, and then click **OK**.

You can select users from department or roles.

Figure 2-45 Add first-card users



2.2.17 Configuring Multi-person Unlock

Users must verify their identities on the Access Controller in an established sequence before the door unlocks.

Background Information

We do not recommend you add first-card users into groups of multi-person unlock.

Procedure

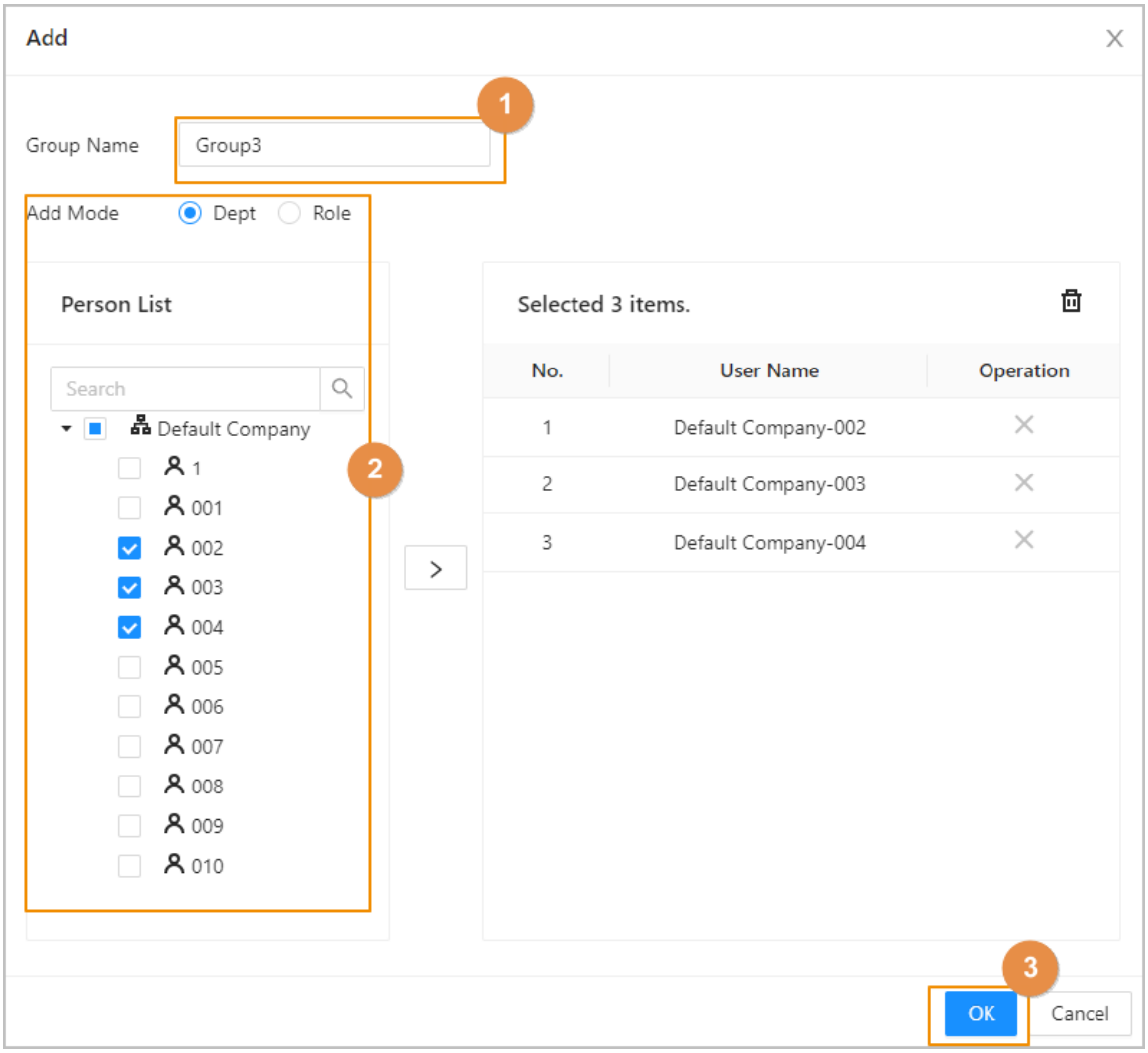
Step 1 Select **Access Control Config** > **Multi-person Unlock**.

Step 2 Click + to add doors to the device list.

Step 3 Click **Person Group Management** , and then click **Add** to add groups of multi-person unlock.

1. Create a name for the group.
2. Select users from departments or roles.
3. Click **OK**.

Figure 2-46 Add groups



Step 4 Select a door, and then click **Add Person Groups**.

Step 5 Select groups, and then click **OK**.

You can add up to 4 groups for each door. Each group can have up to 50 users.

Step 6 Configure the parameters of multi-person unlock.

1. Enter the valid No.

   The valid No. indicates the number of people in each group who need to verify their identities on the Access Controller before the door unlocks. For example, if the valid No. is set to 2 for a group, any 2 people from the group need to verify their identities to unlock the door.

   The valid number ranges from 1 to 5 in each group.

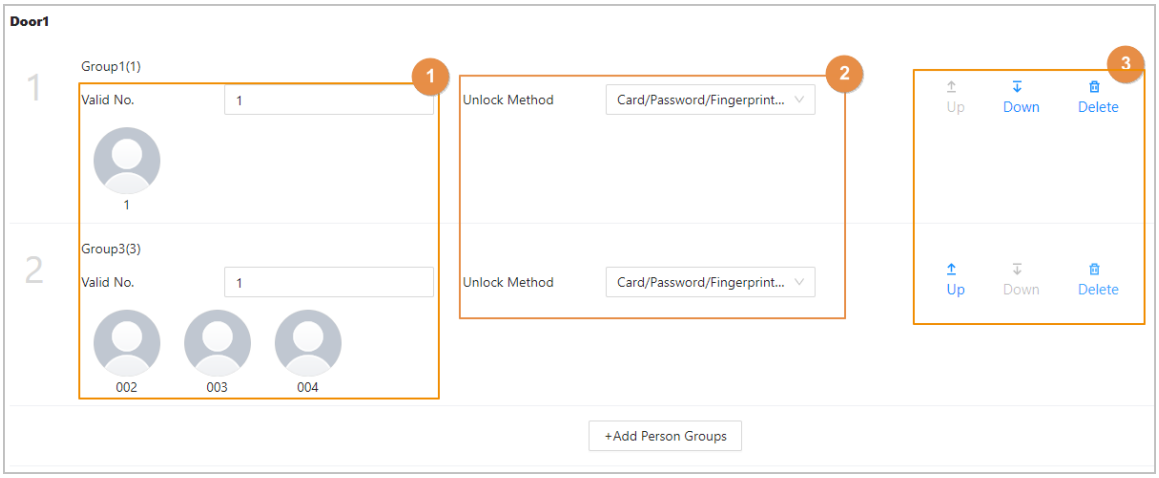
2. Select the unlock method.

   Users in the group must verify their identities through the defined unlock methods.

3. (Optional) Click **Up** or **Down** to change the sequence of groups.

   If more than one groups are added, users must verifying their identities according the defined sequence of groups.

Figure 2-47 Configure multi-person unlock



Step 7 Click **Apply**.

2.2.18 Configuring Anti-passback

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

Background Information

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

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

Procedure

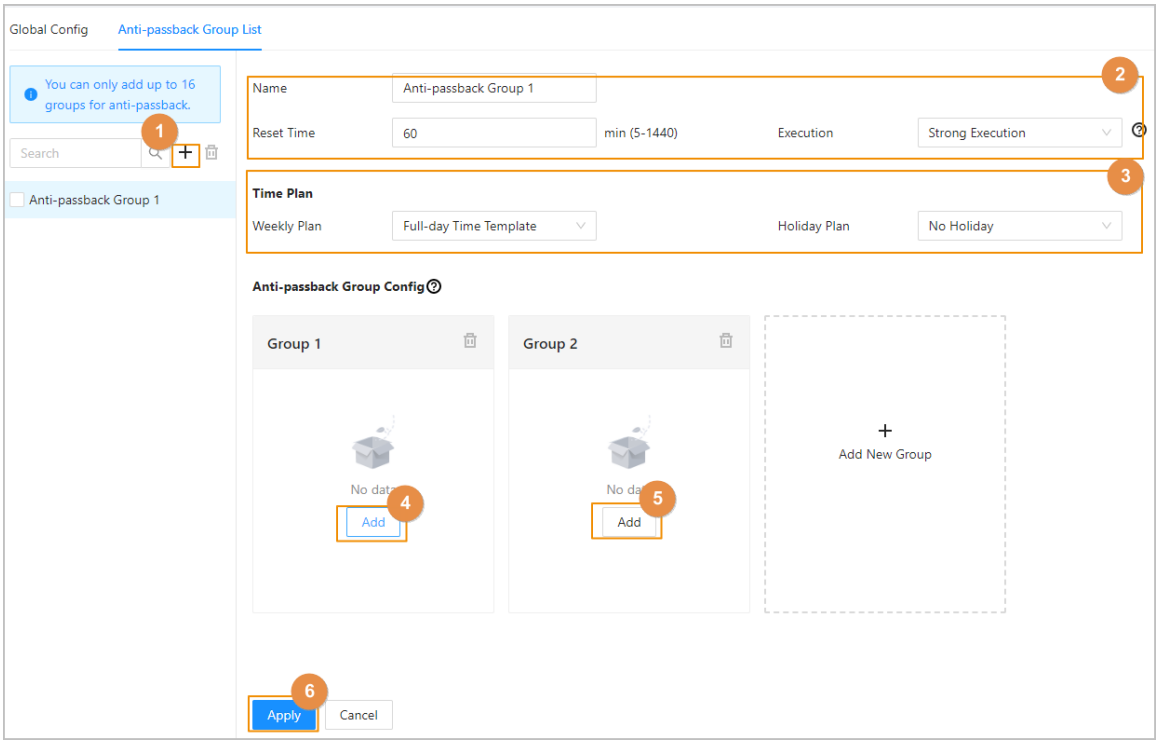
Step 1 Select **Access Control Config** > **Global Anti-passback**.

Step 2 Turn on the **Reset Anti-Passback** function, and then select a reset time.

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

Step 3 Click **Anti-passback Group List**, and then click + to add an anti-passback group.

Figure 2-48 Configure anti-passback



Step 4 Create a name for the anti-passback group, enter a reset time, and then select the execution mode.

Set a time period when the anti-passback alarm will be triggered. For example, if the reset time is set to 30 minutes, when a person enters after being authorized, and exits without being authorized, if they attempt to enter again in 30 minutes, an anti-passback alarm will be triggered.

- Strong execution: The sub controller and main controller perform the anti-passback function even when they go offline.
- Weak execution: The sub controller and main controller do not perform the anti-passback function when they go offline.

Step 5 Select the weekly plan and the holiday plan.

Anti-passback is effective during the defined time.

Step 6 In group 1, click **Add**, and then select card readers.

Step 7 In group 2, click **Add**, and then select card readers.

At least 2 groups must be added.

Step 8 (Optional) You can click **Add New Group** to add more groups.

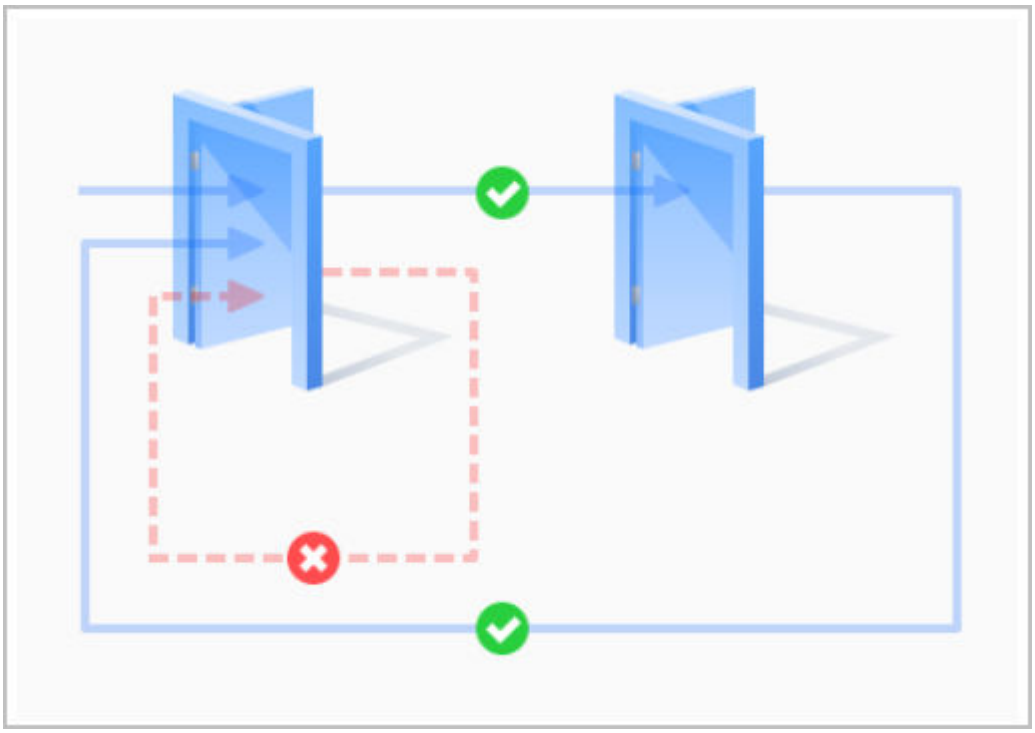
You can add more than one readers in a group, and users can swipe at any one of the readers to gain access.

Step 9 Click **Apply**.

Results

The group number indicates the sequence of swiping cards. Card must be used following the specific sequence of groups. For example, you must swipe card at a reader in group 1, and then at a reader for group 2, and then at a reader in group 3, ect. As long as you swipe card following the established sequence, the system works fine.

Figure 2-49 Anti-passback function



2.2.19 Configuring Multi-door Interlock

Multi-door interlock controls the locking of two or more doors. If one door is unlocked, access will be prohibited for the remaining doors.

Background Information

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

2.2.19.1 Configuring Interlock within a Group

If any doors in a group is opened, the other doors in the group cannot be unlocked.

Procedure

Step 1 Select **Access Control Config** > **Global Multi-door Interlock**, and then click **Interlock within Group**.

Step 2 Click +, and then add a interlock group.

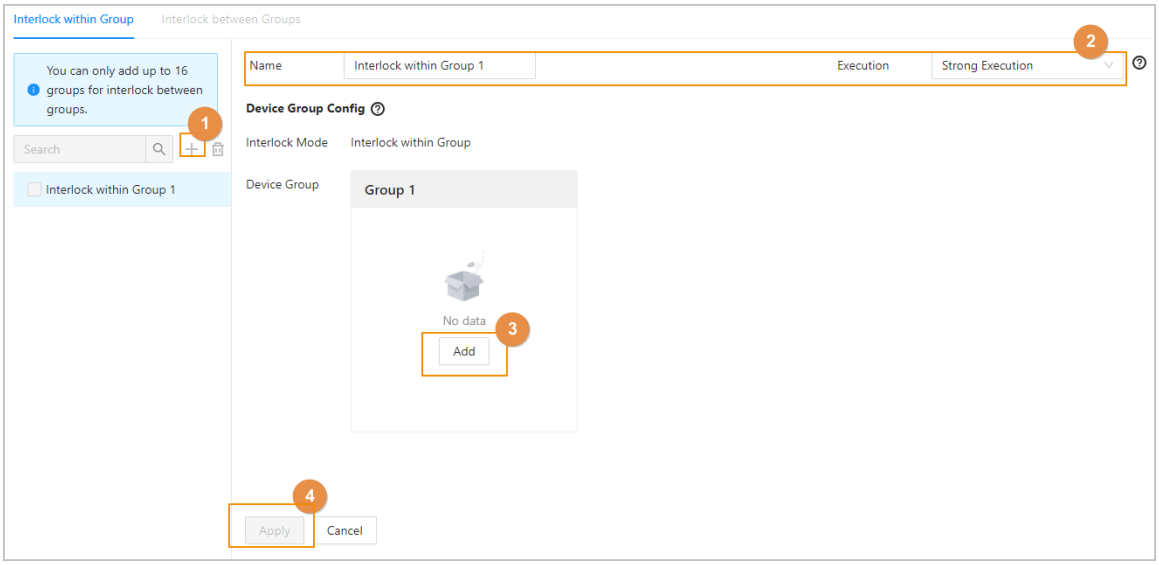
Step 3 Create a name for the interlock group, and then select the execution mode.

- Strong execution: The sub controller and main controller perform the interlock function even when they go offline.
- Weak execution: The sub controller and main controller do not perform the interlock function when they go offline.

Step 4 Click **Add** to add doors in a device group.

At least 2 doors must be added to a group.

Figure 2-50 Interlock within a group



Step 5 Click **Apply**.

Results

After a person's identity has been verified and they opened the door, they have to close the door behind them first before they can open the next door.

2.2.19.2 Configuring Interlock between Groups

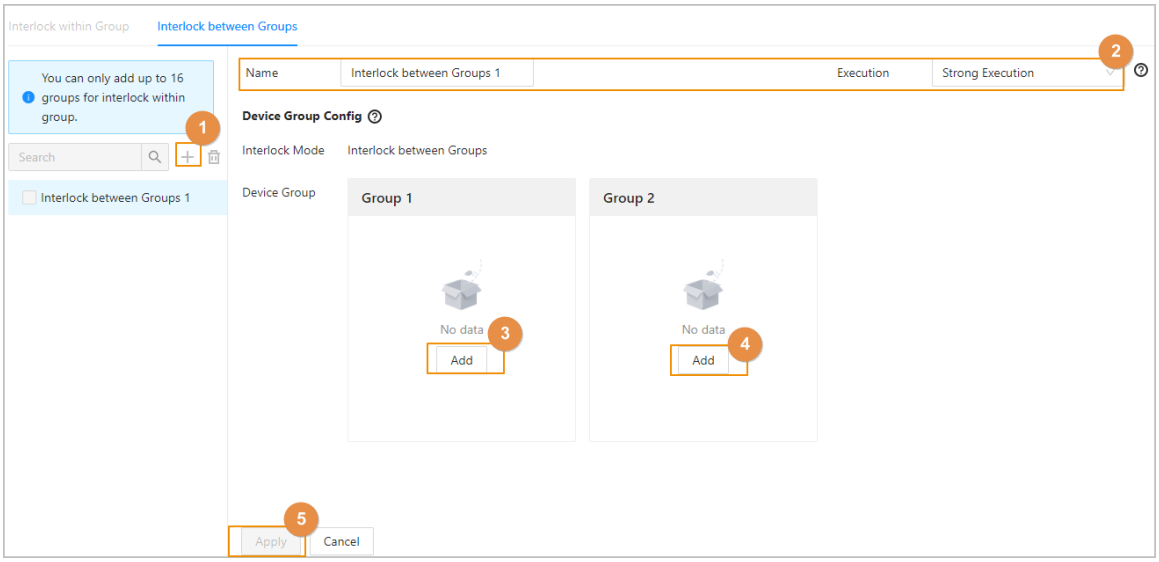
If any doors in a group is unlocked, the doors in the other groups cannot open.

Procedure

Step 1 Select **Access Control Config** > **Global Multi-door Interlock**, and then click **Interlock between Groups**.

Step 2 Click ＋, and then add a interlock group.

Figure 2-51 Interlock between groups



Step 3 Create a name for the interlock group, and then select the execution mode.

- Strong execution: The sub controller and main controller perform interlock function even when they go offline.
- Weak execution: The sub controller and main controller do not perform interlock function when they go offline.

Step 4 In group 1, click **Add** to add doors to the group.

Step 5 In group 2, click **Add** to add doors to the group.

Step 6 Click **Apply**.

Results

If any doors in one group is unlocked, the doors in the other group cannot open.

2.2.20 Access Monitoring (Optional)

2.2.20.1 Remotely Opening and Closing Doors

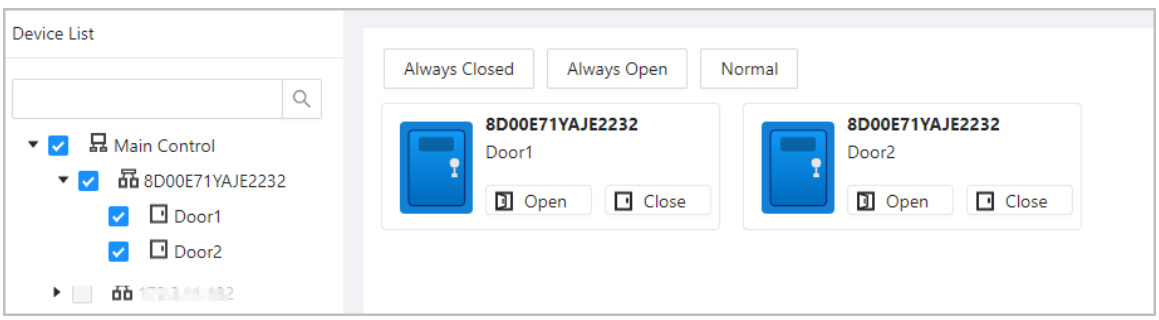
You can remotely monitor and control the door through platform. For example, you can remotely open or close the door.

Procedure

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

Step 2 Select the door, and then click **Open** or **Close** to remotely control the door.

Figure 2-52 Remotely control the door



Related Operations

- Event filtering: Select the event type in **Event Info**, and the event list displays the selected event types, such as alarm events and abnormal events.
- Event deleting: Click to clear all events from the event list.

2.2.20.2 Setting Always Open and Always Closed

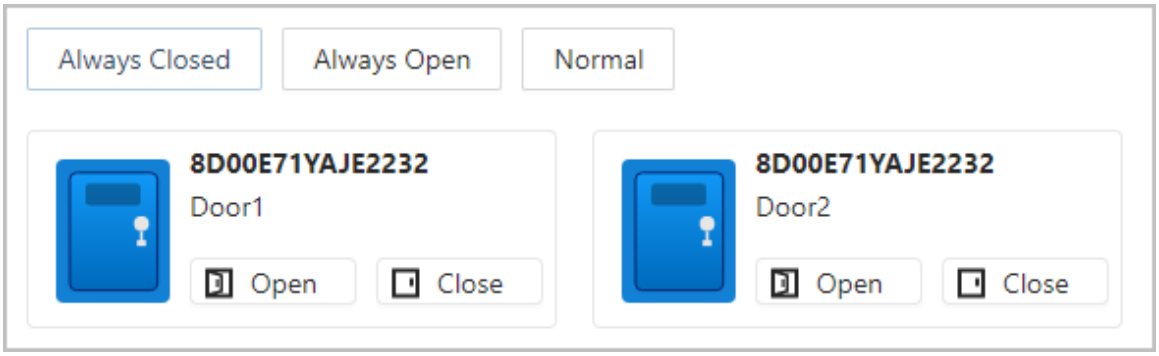
After setting always open or always close, the door remains open or closed all the time.

Procedure

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

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

Figure 2-53 Always open or close



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

2.2.21 Local Device Configurations (Optional)

Local device configurations can only be applied to the local Access Controllers.

2.2.21.1 Configure Local Alarm Linkages

You can only configure local alarm linkages on the same access controller. Each controller has 2 alarm inputs and 2 alarm outputs.

Procedure

Step 1 On the home page, select **Local Device Config** > **Local Alarm Linkage**.

Step 2 Click to configure local alarm linkage.

Figure 2-54 Local alarm linkage

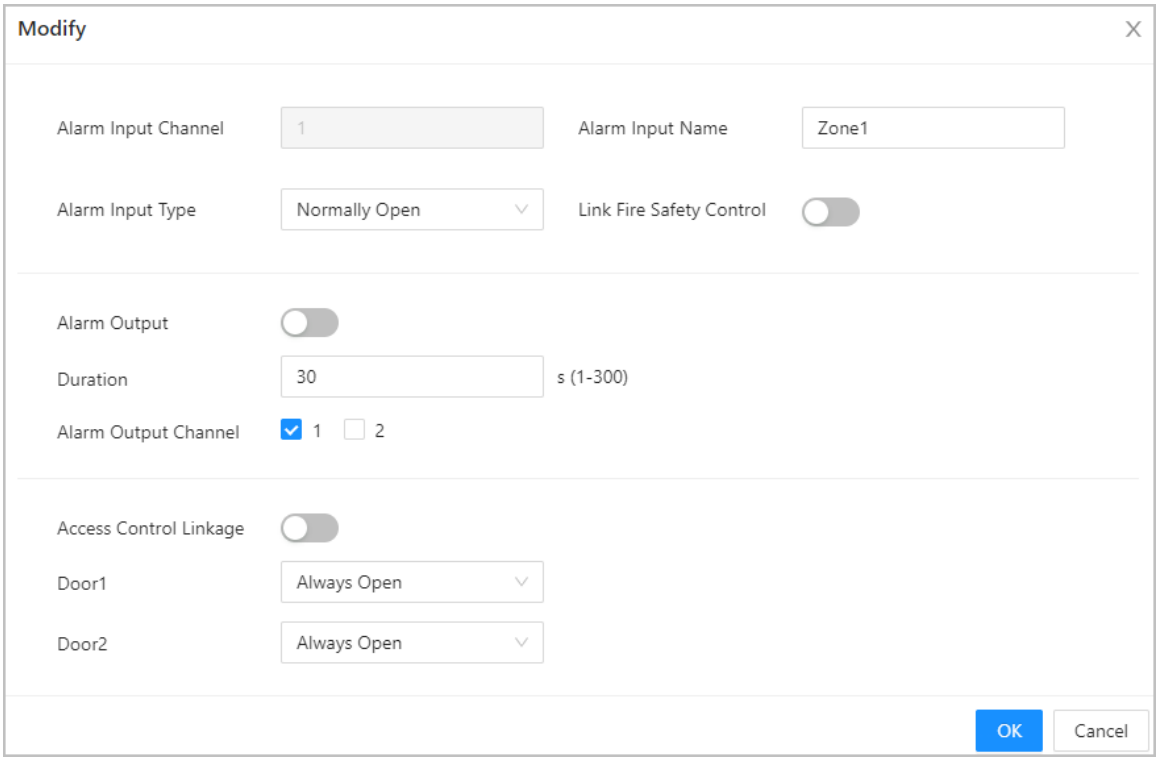


Table 2-11 Local alarm linkage

Parameter	Description
Alarm input channel	The number of the alarm input channel. Each controller has 2 alarm inputs and 2 alarm outputs.
Alarm Input Name	The name of the alarm input.
Alarm Input Type	The type of the alarm input. • Normally Open • Normally Closed
Link Fire Safety Control	If you turn on the link fire safety control, all the doors will open when the fire alarm is triggered.
Alarm Output	You can turn on the alarm output function.
Duration	When an alarm is triggered, the alarm remains on for a defined time.
Alarm Output Channel	Select the alarm output channel. Each controller has 2 alarm inputs and 2 alarm outputs.
Access Control Linkage	Turn on this function to configure the door linkage.
Door1/Door2	Set the door to always open or always closed status. When an alarm is triggered, the door will automatically open or close.

Step 3 Click **OK**.

2.2.21.2 Configuring Card Rules

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

Procedure

Step 1 On the home page, select **Local Device Config** > **Access Card Rule Config**.

Step 2 Click **Add**, and then configure new Wiegand formats.

You can also Click **Add Protocol** to import a Wiegand file to the platform.

Figure 2-55 Add new Wiegand formats

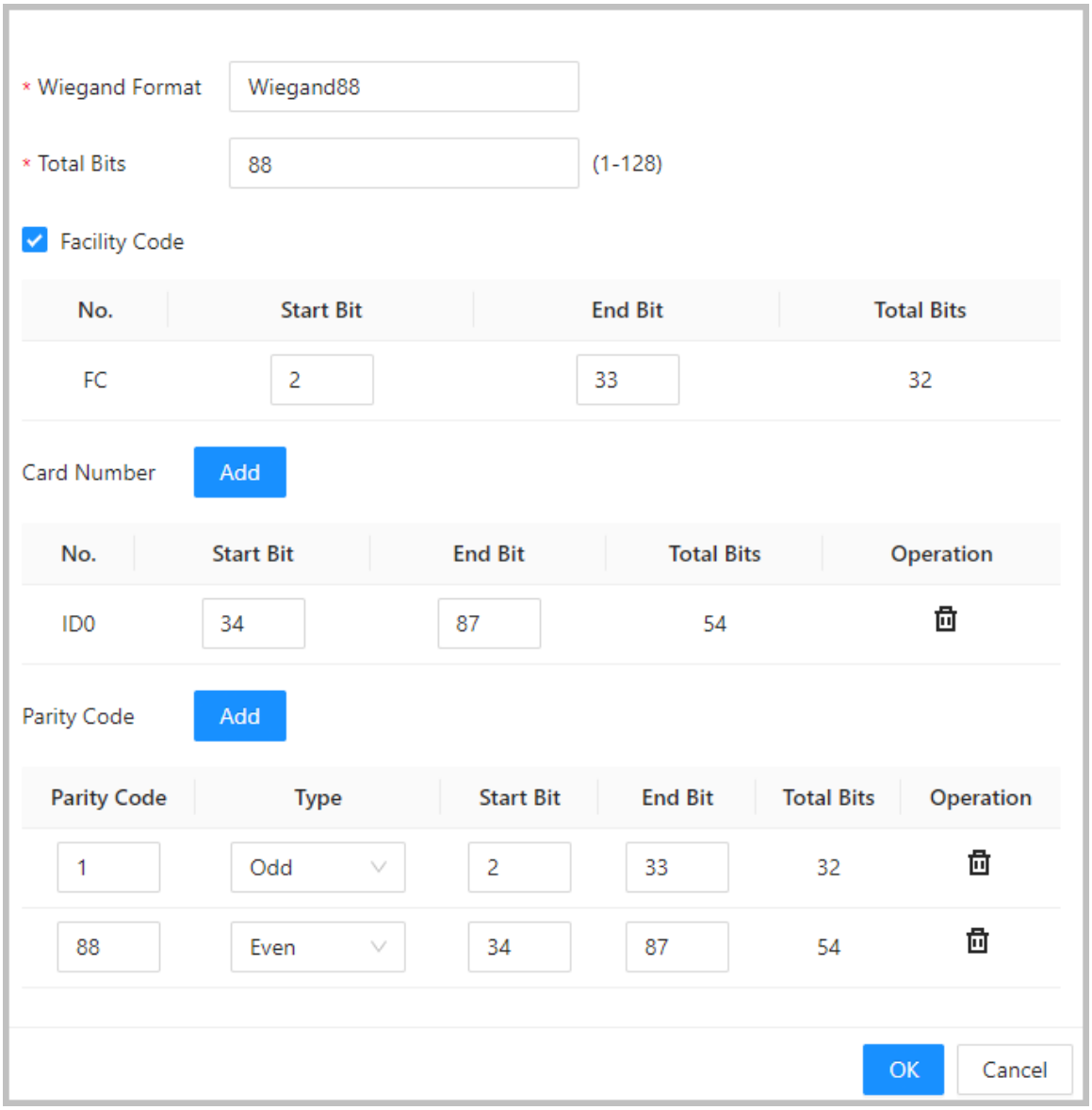


Table 2-12 Configure the Wiegand format

Parameter	Description
Wiegand format	The name of the Wiegand format.

Parameter	Description
Total bits	Enter the total number of bits.
Facility Code	Enter the start bit and the end bit for the facility code.
Card number	Enter the start bit and the end bit for the card number.
Parity Code	1. Enter the even parity start bit and even parity end bit. 2. Enter the odd parity start bit and odd parity end bit.

Step 3 Click **OK**.

Related Operations

- Facility Code: If this function is enabled and you 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 this 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 has 3 characters at most. When you manually entering card, the system will automatically add leading zero to fixed number length. For example, if the card number you enter is less than 5 characters, like 56, leading zero is added to fix the number length to 5 characters, like 00056, and another 0 is added to function as a facility code. Therefore, the final card No. will be 000056.

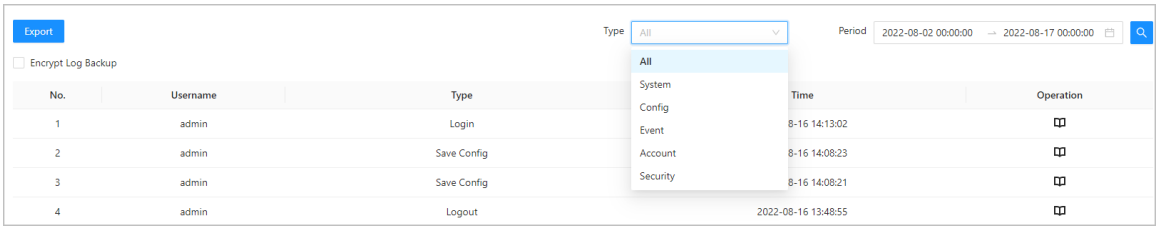
2.2.21.3 Backing up System Logs

Procedure

Step 1 On the home page, select **Local Device Config** > **System Logs**.

Step 2 Select the type of log, and then select the time range.

Figure 2-56 Back up logs



Step 3 Click **Encrypt Log Backup**, and then enter the password to back up encrypted logs.

Step 4 (Optional) You can also click **Export** to export logs.

2.2.21.4 Configuring Network

2.2.21.4.1 Configuring TCP/IP

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

Procedure

Step 1 Select **Local Device Config** > **Network Setting** > **TCP/IP**.

Step 2 Configure the parameters.

Figure 2-57 TCP/IP

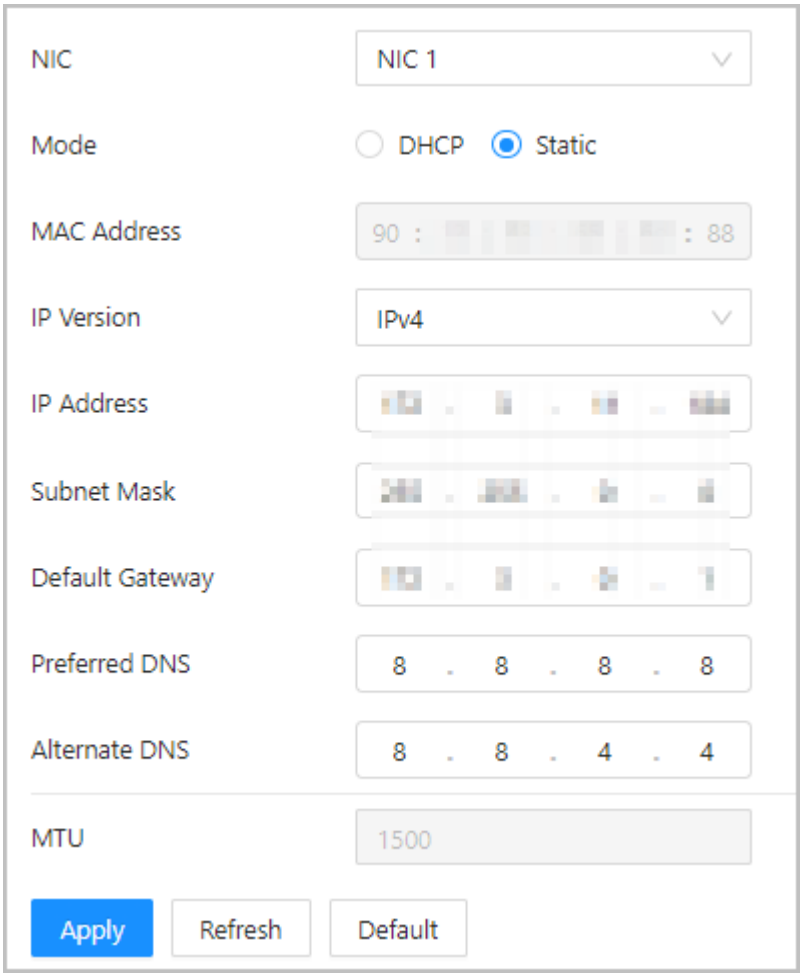


Table 2-13 Description of TCP/IP

Parameter	Description
IP Version	IPv4.
MAC Address	MAC address of the Access Controller.
Mode	• **Static** : Manually enter IP address, subnet mask, and gateway. • **DHCP** : Dynamic Host Configuration Protocol. When DHCP is turned on, the Access Controller will automatically be assigned IP address, subnet mask, and gateway.
IP Address	If you select static mode, configure the IP address, subnet mask and gateway. IP address and gateway must be on the same network segment.
Subnet Mask	
Default Gateway	
Preferred DNS	Set the IP address of the preferred DNS server.
Alternate DNS	Set the IP address of the alternate DNS server.

Step 3 Click **OK**.

2.2.21.4.2 Configuring Ports

You can limit access to the Access Controller at the same time through web, desktop client and phone.

Procedure

Step 1 Select **Local Device Config** > **Network Setting** > **Port**.

Step 2 Configure port numbers.

You need to restart the controller to make the configurations effective for all the parameters except **Max Connection** and **RTSP Port**.

Figure 2-58 Configure ports

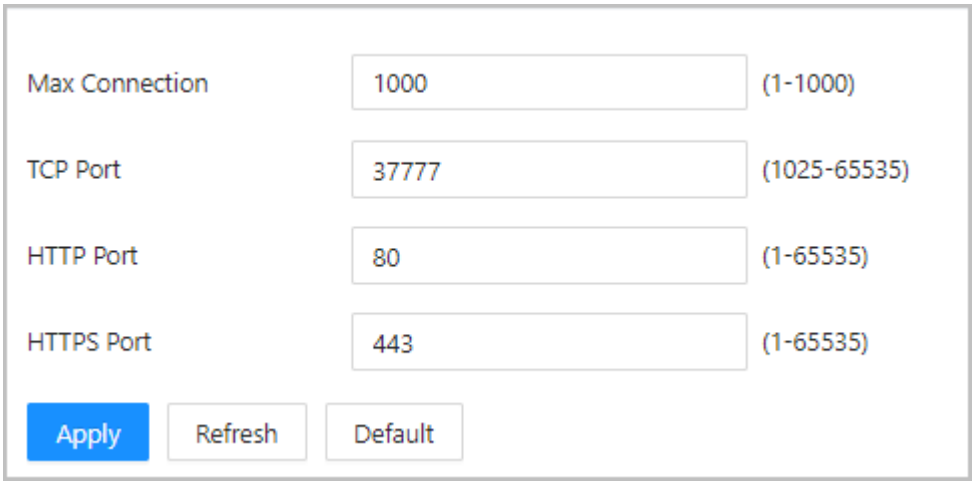


Table 2-14 Description of ports

Parameter	Description
Max Connection	You can set the maximum number of clients that can access the Access Controller at the same time, such as the web client, desktop client and phone.
TCP Port	It is 37777 by default.
HTTP Port	It is 80 by default. If you want to change the port number, add the new port number after the IP address when you log in to the webpage.
HTTPS Port	It is 443 by default.

Step 3 Click **OK**.

2.2.21.4.3 Configuring Cloud Service

Add the Main Controller to DMSS before you request Bluetooth cards for users. For details on using DMSS, see the user's manual of DMSS.

Background Information

If you have changed the password of the Main Controller, or restored it to factory defaults, you need to delete the controller on DMSS and add it to DMSS again.

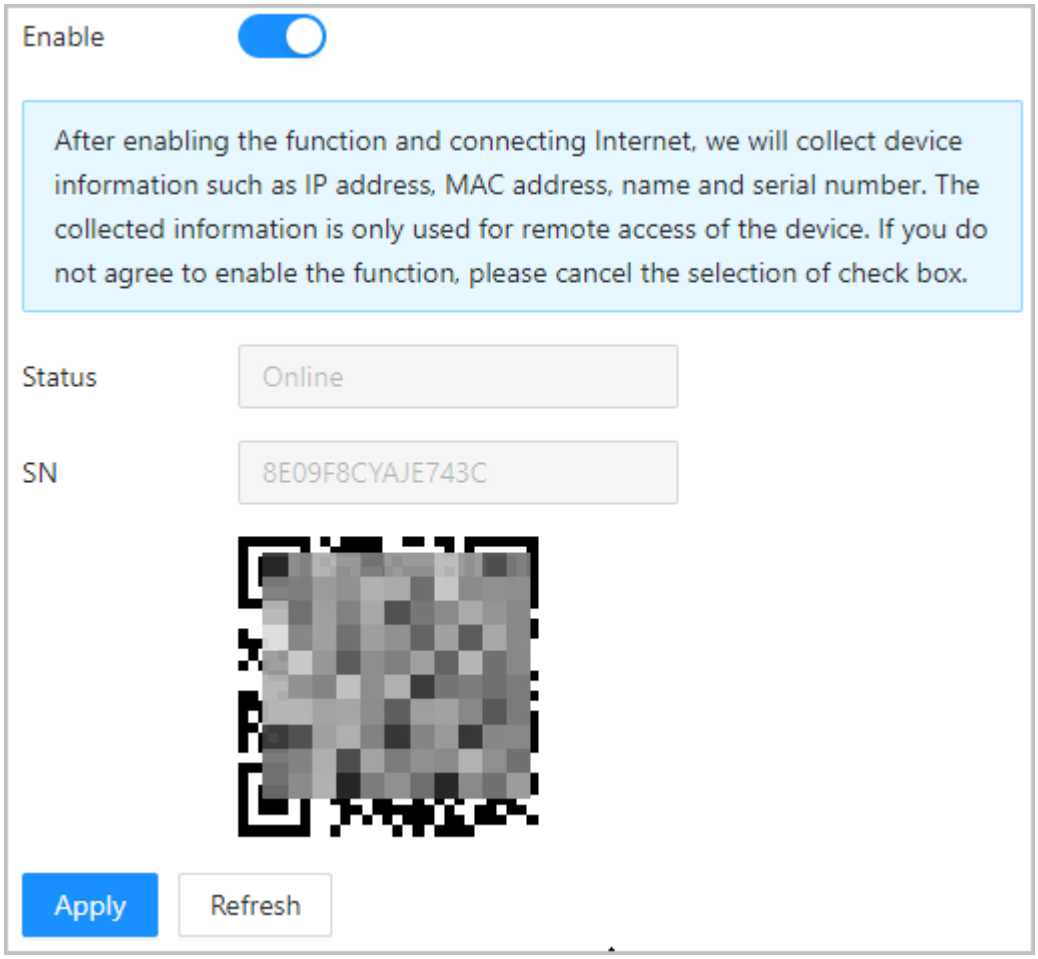
Procedure

Step 1 On the home page, select **Local Device Config** > **Network Setting** > **Cloud Service**.

Step 2 Turn on the cloud service function.

The cloud service function is turned on by default.

Figure 2-59 Cloud service



Step 3 Click **Apply**.

Step 4 Download DMSS and sign up with Email, scan the QR code with DMSS to add the Access Controller to it.

2.2.21.4.4 Configuring Automatic Registration

The Access Controller reports its address to the designated server so that you can get access to the Access Controller through the management platform.

Procedure

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

Step 2 Enable the automatic registration function, and then configure the parameters.

Figure 2-60 Register

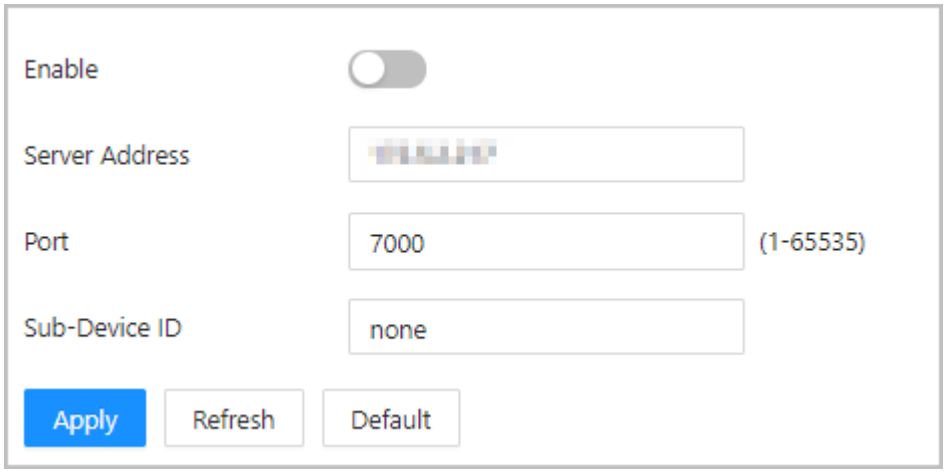


Table 2-15 Automatic registration description

Parameter	Description
Server Address	The IP address of the server.
Port	The port of the server used for automatic registration.
Sub-Device ID	Enter the sub-device ID (user defined). When you add the Access Controller to the management platform, the sub-device ID on the management platform must conform to the defined sub-device ID on the Access Controller.

Step 3 Click **Apply**.

2.2.21.4.5 Configuring Basic Service

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

Procedure

Step 1 Select **Network Settings** > **Basic Service**.

Step 2 Configure the basic service.

Figure 2-61 Basic service

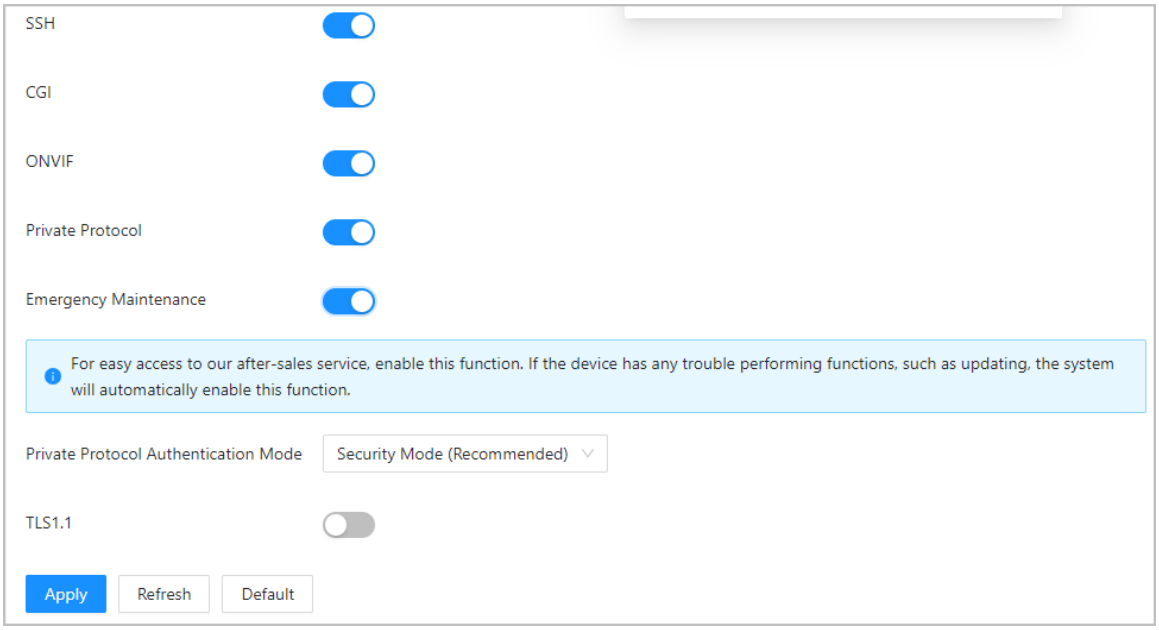


Table 2-16 Basic service parameter description

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.
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.
Private Protocol	The platform adds devices through TLSv1.1 protocol. Security risks might present when TLSv1.1 is enabled. Please be advised.
Emergency Maintenance	It is turned off by default.
Private Protocol Authentication Mode	Set the authentication mode, including safe mode and compatibility mode. It is recommended to choose **Security Mode**. • Security Mode (recommended): Does not support accessing the device through Digest, DES, and plaintext authentication methods, improving device security. • Compatible Mode: Supports accessing the device through Digest, DES, and plaintext authentication methods, with reduced security.

Step 3 Click **Apply**.

2.2.21.5 Configuring Time

Procedure

Step 1 On the home page, select **Local Device Config** > **Time**.

Step 2 Configure the time of the Platform.

Figure 2-62 Date settings

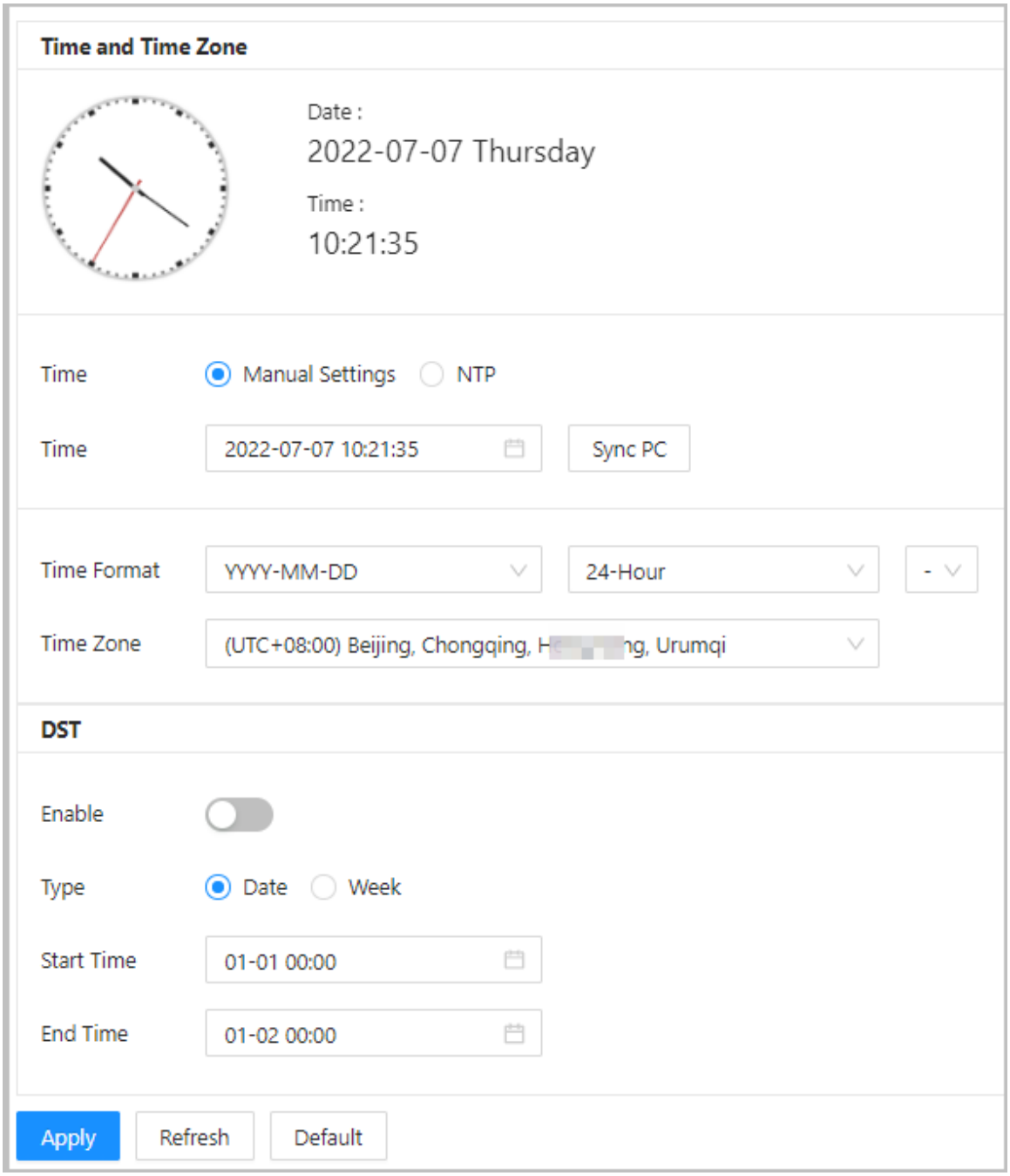


Table 2-17 Time settings description

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

Step 3 Click **Apply**.

2.2.21.6 Account Management

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

2.2.21.6.1 Adding Administrator Accounts

Add administrators on the Access Controller.

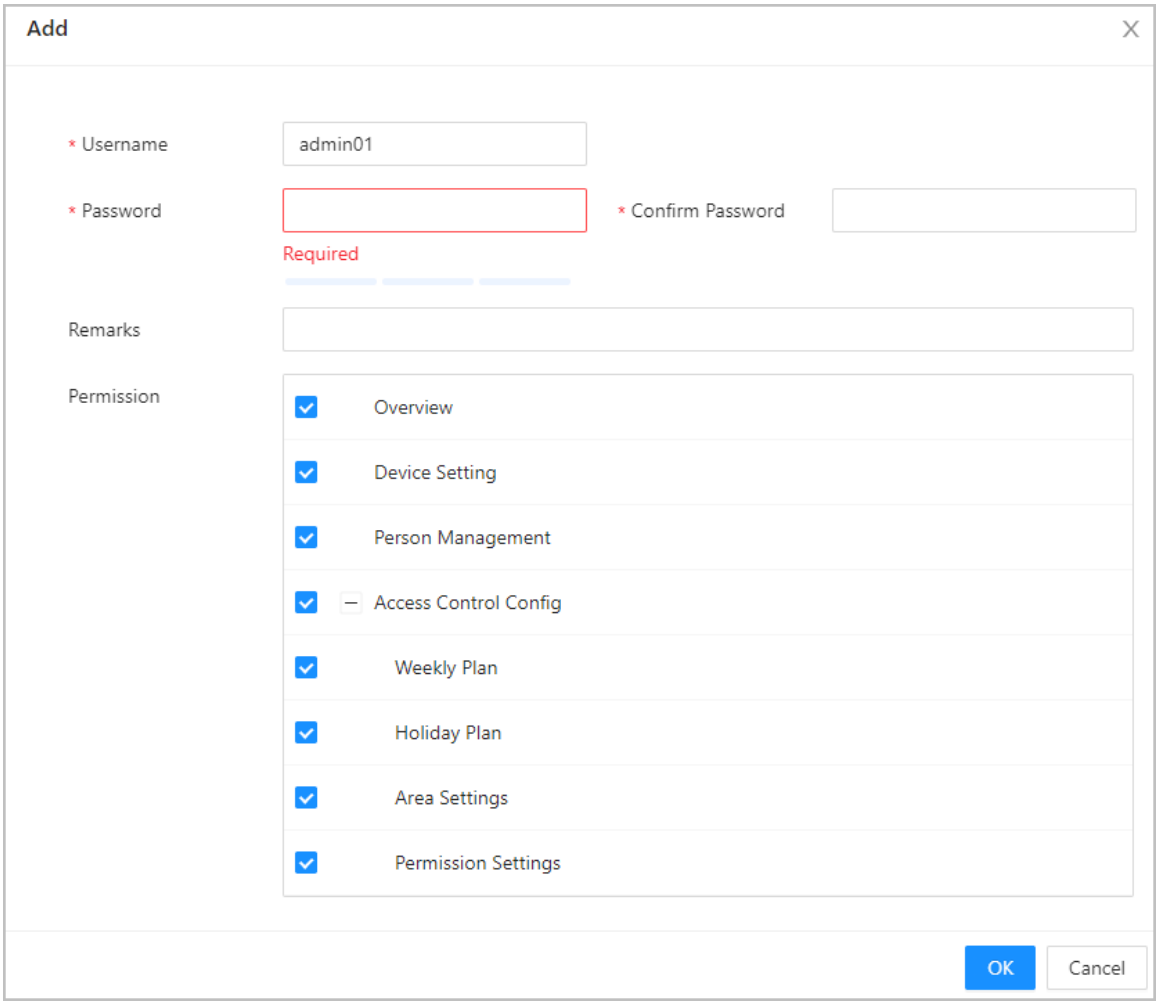
Procedure

Step 1 On the home page, select **Local Device Config** > **Account Management** > **Account**.

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

- The username cannot be the same as the existing account. The username can contain up to 31 characters, and supports numbers, letters, underlines, dots, and @.
- The password must contain 8 to 32 non-blank characters and contain at least 2 types of the following characters: upper case and lower case letters, numbers, and special characters (excluding ' " ; : &). Set a high-security password by following the password strength prompt.

Figure 2-63 Add administrator accounts



Step 3 Click **OK**.

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

2.2.21.6.2 Resetting the Password

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

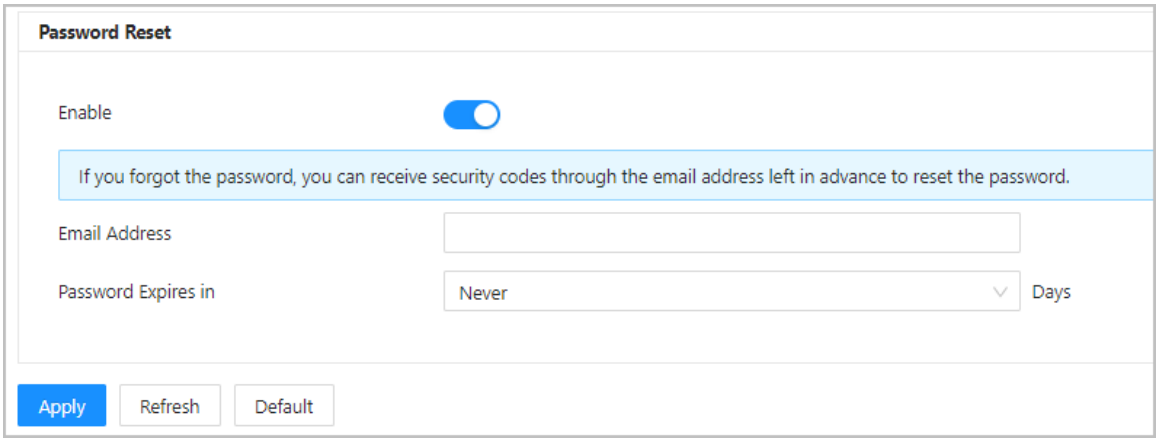
Procedure

Step 1 Select **Local Device Config** > **Account Management** > **Account**.

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

Step 3 Turn on the password reset function.

Figure 2-64 Reset password



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

Step 4 Click **Apply**.

2.2.21.6.3 Adding ONVIF Users

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

Procedure

Step 1 On the home page, select **Local Device Config** > **Account Management** > **ONVIF Account**.

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

Figure 2-65 Add the ONVIF user

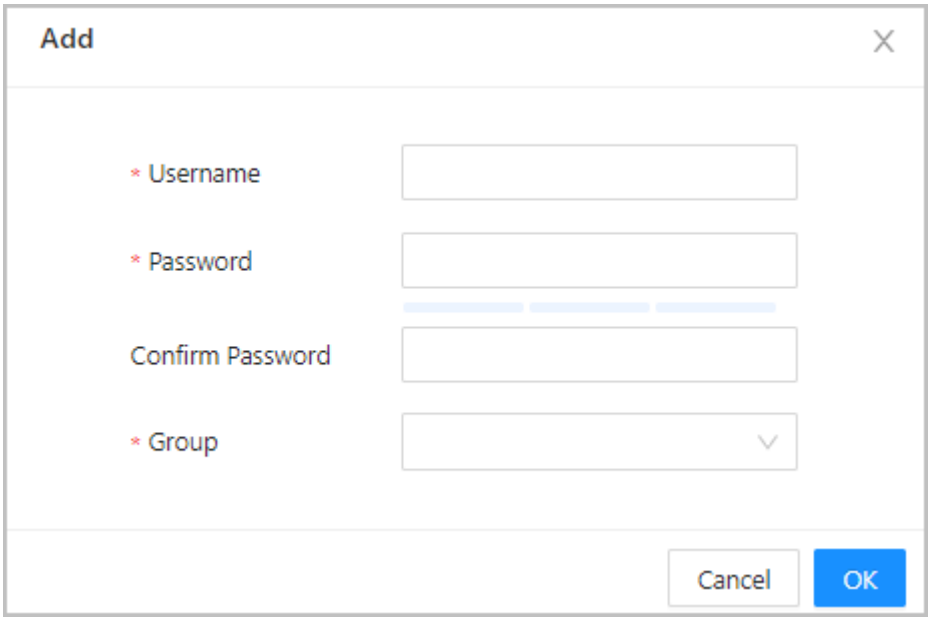


Table 2-18 ONVIF user description

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

Step 3 Click **OK**.

2.2.21.7 Maintenance

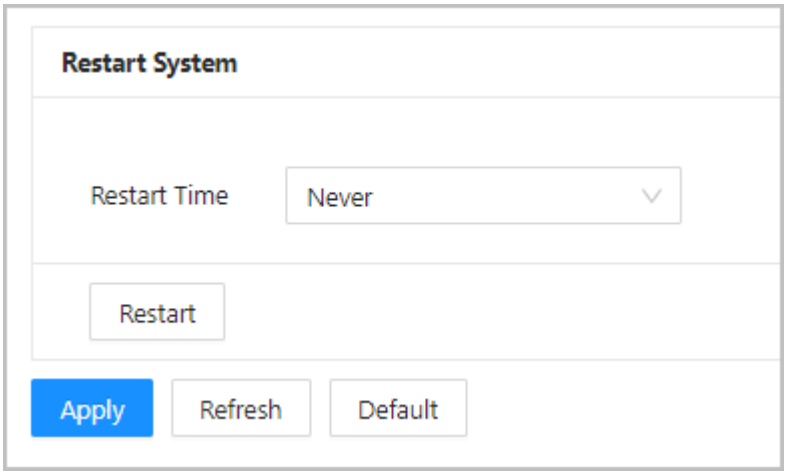
You can regularly restart the Access Controller during its idle time to improve its performance. It is **Never** by default, we recommend you change it to one day a week.

Procedure

Step 1 Log in to the webpage.

Step 2 Select **Local Device Config** > **Maintenance**.

Figure 2-66 Maintenance



Step 3 Set the restart time, and then click **OK**.

Step 4 (Optional) Click **Restart**, and the Access Controller will restart immediately.

2.2.21.8 Advanced Management

When more than one Access Controller requires the same configurations, you can configure them quickly by importing or exporting configuration files.

2.2.21.8.1 Exporting and Importing Configuration Files

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

Background Information

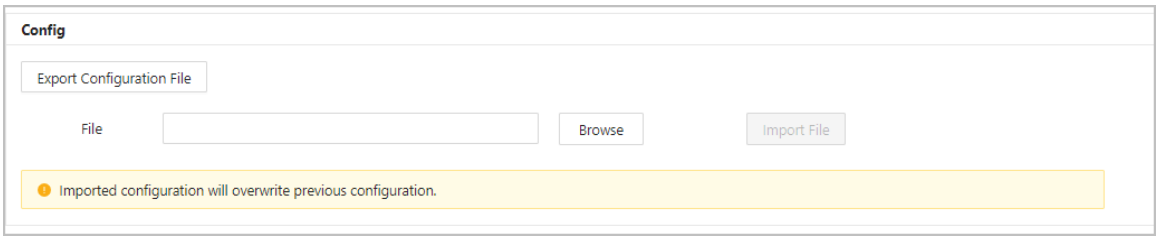
Configurations on device management, advanced access control, time schedules, hardware cannot be exported.

Procedure

Step 1 Log in to the webpage.

Step 2 Select **Local Device Config** > **Advanced Settings**.

Figure 2-67 Configuration management



Step 3 Export or import configuration files.

- Export the configuration file.

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

  The IP will not be exported.

- Import the configuration file.

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

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

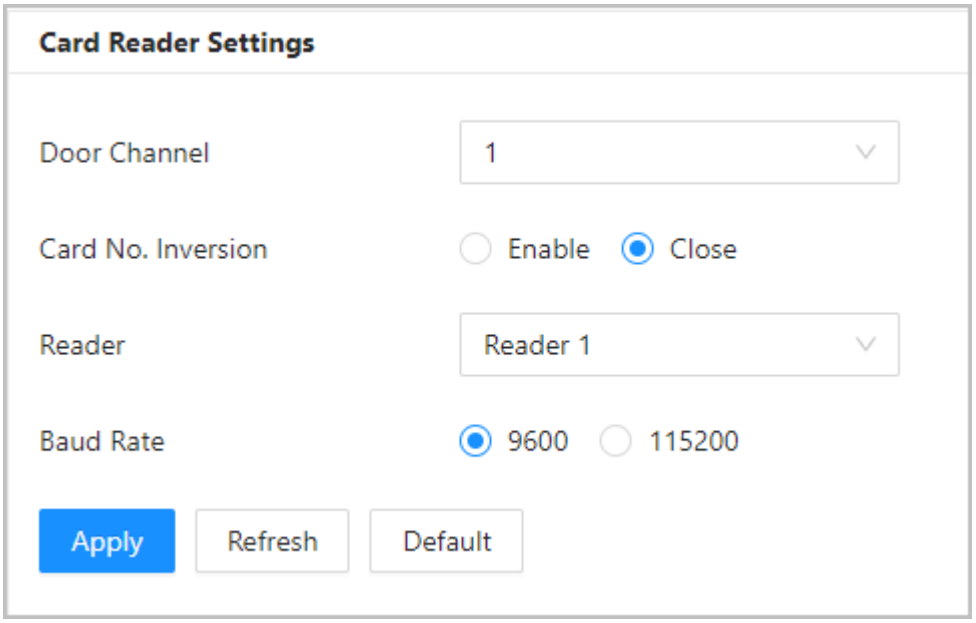
2.2.21.8.2 Configuring the Card reader

Procedure

Step 1 On the home page, select **Local Device Config** > **Advanced Settings**.

Step 2 Configure the card reader.

Figure 2-68 Configure the card reader



2.2.21.8.3 Configuring the Fingerprint Level

On the home page, select **Local Device Config** > **Advanced Settings**, and then enter the fingerprint threshold. The value ranges from 1 to 10, and higher value means higher recognition accuracy.

Figure 2-69 Fingerprint level



2.2.21.8.4 Configuring RS-485 Expansion

If the Access Controller is mounted to the access controller metal case, select **Local Device Config** > **RS-485 Expansion**, and then select **Access Control Metal Case**.

2.2.21.8.5 Restoring the Factory Default Settings

Procedure

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

⚠

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

Step 2 Restore to the factory default settings if necessary.

- **Factory Defaults** : Resets all the configurations of the Controller and delete all the data.
- **Restore to Default (Except for User Info)** : Resets the configurations of the Access Controller and deletes all the data except for user information, and information that was configured during the login wizard).

Only the main controller supports **Restore to Default (Except for User Info)**.

2.2.21.9 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 Access Controller during the update.

2.2.21.9.1 File Update

Procedure

Step 1 On the home page, select **Local Device Config** > **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 Access Controller will restart after the update finishes.

2.2.21.9.2 Online Update

Procedure

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

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

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

Step 3 Click **Manual Check** to update the Access Controller when the latest version update is available.

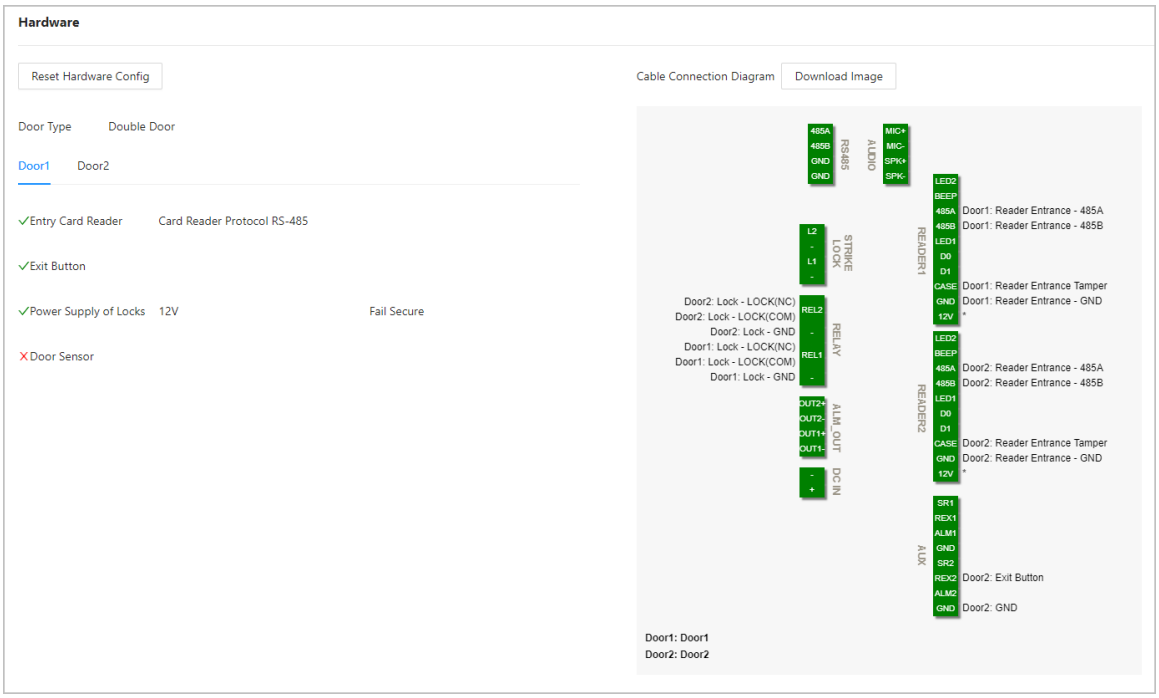
2.2.21.10 Configuring Hardware

On the home page, select **Local Device Config** > **Hardware**. You can view the hardware you have configured when you log in to the platform for the first time. You can also click **Reset Hardware Config** to re-configure the hardware. For details, see Table 2-1 .

When you switch between single door and double door, we recommend you restore the main controller factory defaults.

The wring diagram is generated for your reference. You can download it to your computer.

Figure 2-70 Hardware



2.2.21.11 Viewing Version Information

On the home page, select **Local Device Config** > **Version Info**, and you can view information on the version, such as device model, serial number, hardware version, legal information and more.

2.2.21.12 Viewing Legal Information

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

2.2.22 Viewing Records

You can view alarm logs and unlock logs.

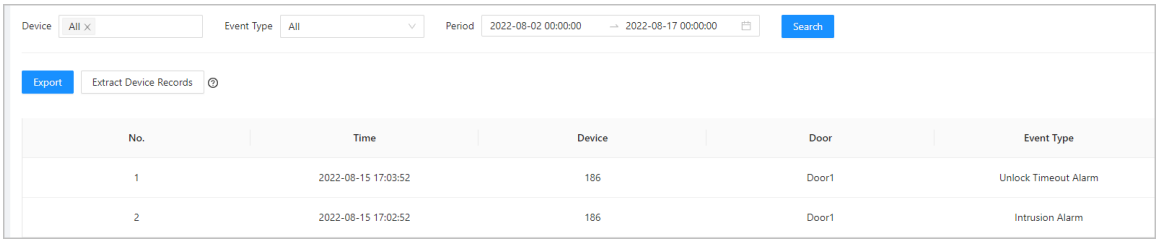
2.2.22.1 Viewing Alarm Records

Procedure

Step 1 On the home page, select **Reporting** > **Alarm Records**.

Step 2 Select the device, department and the time range, and then click **Search**.

Figure 2-71 Alarm records



- **Export** : Exports unlock logs on the main controller to a local computer.
- **Extract Device Records** : When logs for sub controller are generated when they go online, you can extract logs from the sub controller to the main controller.

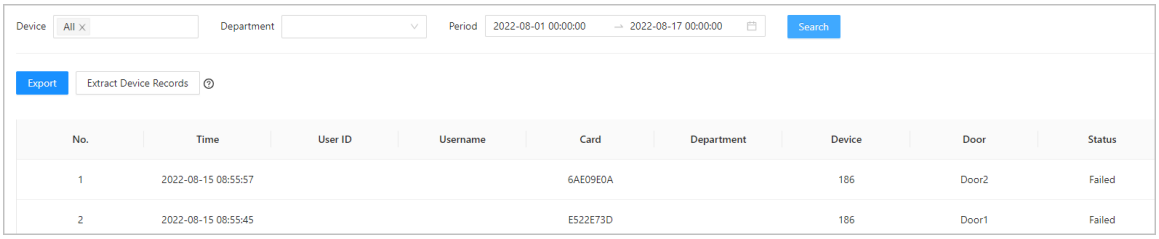
2.2.22.2 Viewing Unlock Records

Procedure

Step 1 On the home page, select **Reporting** > **Unlock Records**

Step 2 Select the device, department and the time range, and then click **Search**.

Figure 2-72 Unlock logs



- Export: Exports unlock logs.
- Extract Device Records: When logs on sub controller are generated when they go online, you extract logs on the sub controller to the main controller.

2.2.23 Security Settings(Optional)

2.2.23.1 Security Status

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

Background Information

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

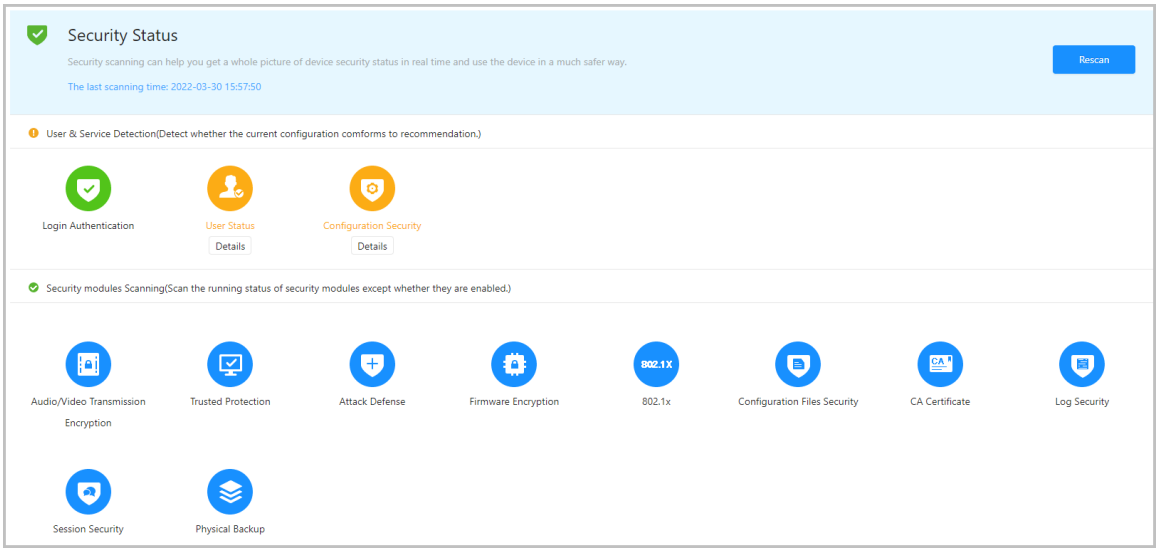
Procedure

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

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

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

Figure 2-73 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 **Rejoin Detection**, and the abnormality that was ignored will be scanned again.
- Click **Optimize** to troubleshoot the abnormality.

2.2.23.2 Configuring HTTPS

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

Procedure

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

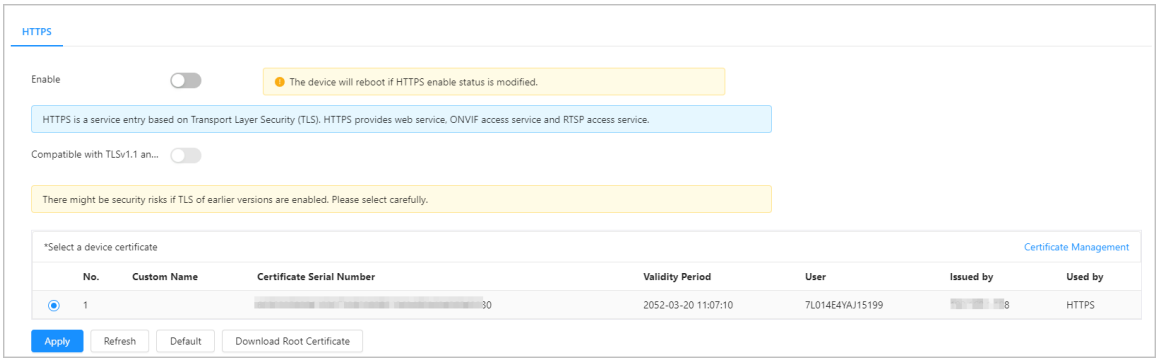
Step 2 Turn on the HTTPS service.

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

Step 3 Select the certificate.

If there are no certificates in the list, click **Certificate Management** to upload a certificate. For details, see "2.2.23.4 Installing Device Certificate".

Figure 2-74 HTTPS



Step 4 Click **Apply**.

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

2.2.23.3 Attack Defense

2.2.23.3.1 Configuring Firewall

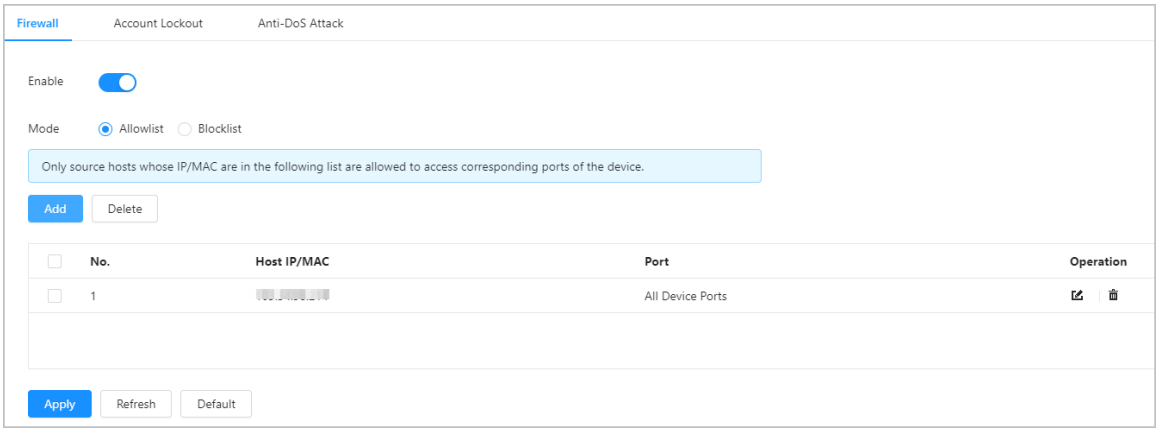
Configure firewall to limit access to the Access Controller.

Procedure

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

Step 2 Click to enable the firewall function.

Figure 2-75 Firewall

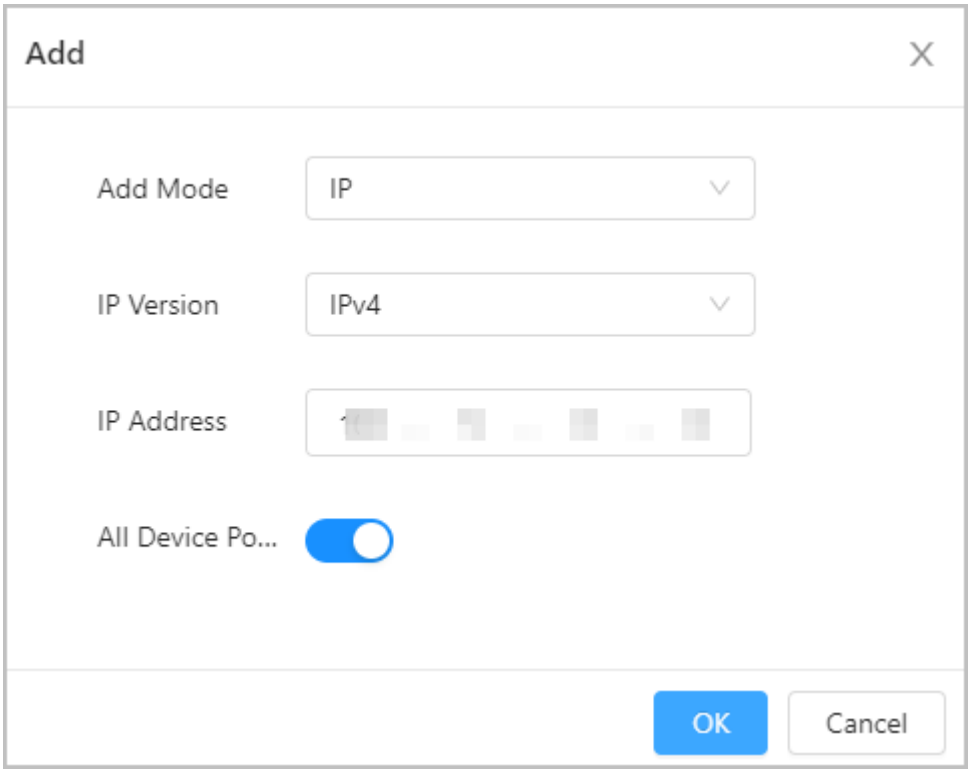


Step 3 Select the mode: **Allowlist** and **Blocklist**.

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

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

Figure 2-76 Add IP information



Step 5 Click **OK**.

Related Operations

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

2.2.23.3.2 Configuring Account Lockout

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

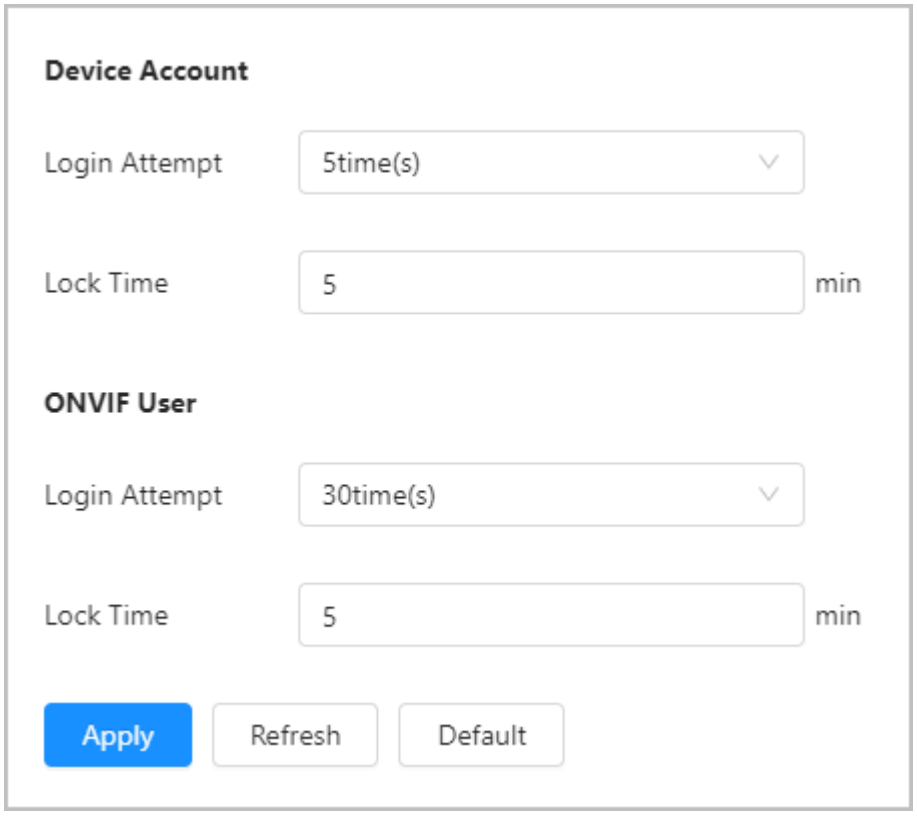
Procedure

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

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

- 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.

Figure 2-77 Account lockout



Step 3 Click **Apply**.

2.2.23.3.3 Configuring Anti-DoS Attack

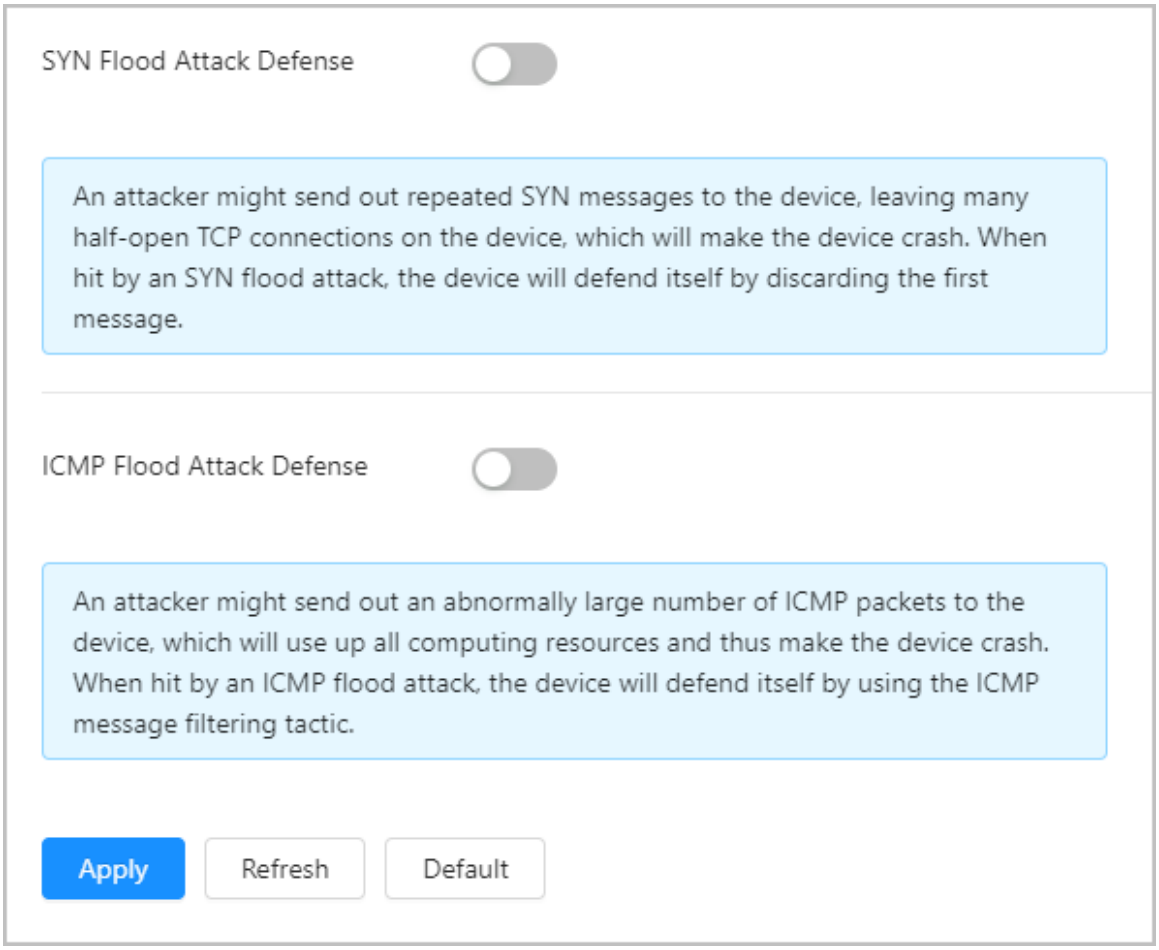
You can enable **SYN Flood Attack Defense** and **ICMP Flood Attack Defense** to defend the Access Controller against Dos attacks.

Procedure

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

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

Figure 2-78 Anti-DoS attack



Step 3 Click **Apply**.

2.2.23.4 Installing Device Certificate

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

2.2.23.4.1 Creating Certificate

Create a certificate for the Access Controller.

Procedure

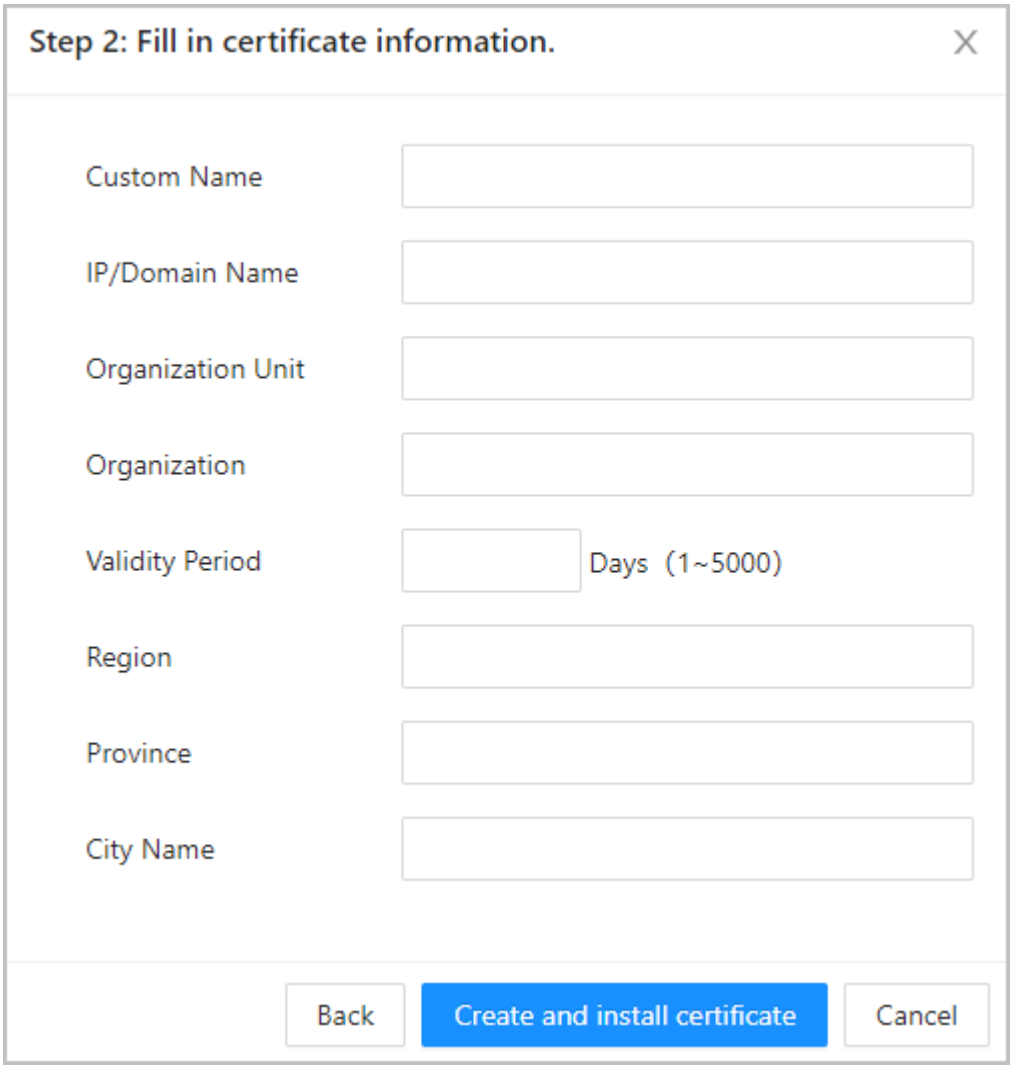
Step 1 Select **Security** > **CA Certificate** > **Device Certificate**.

Step 2 Select **Install Device Certificate**.

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

Step 4 Enter the certificate information.

Figure 2-79 Certificate information



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

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

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

Related Operations

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

2.2.23.4.2 Applying for and Importing CA Certificate

Import the third-party CA certificate to the Access Controller.

Procedure

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

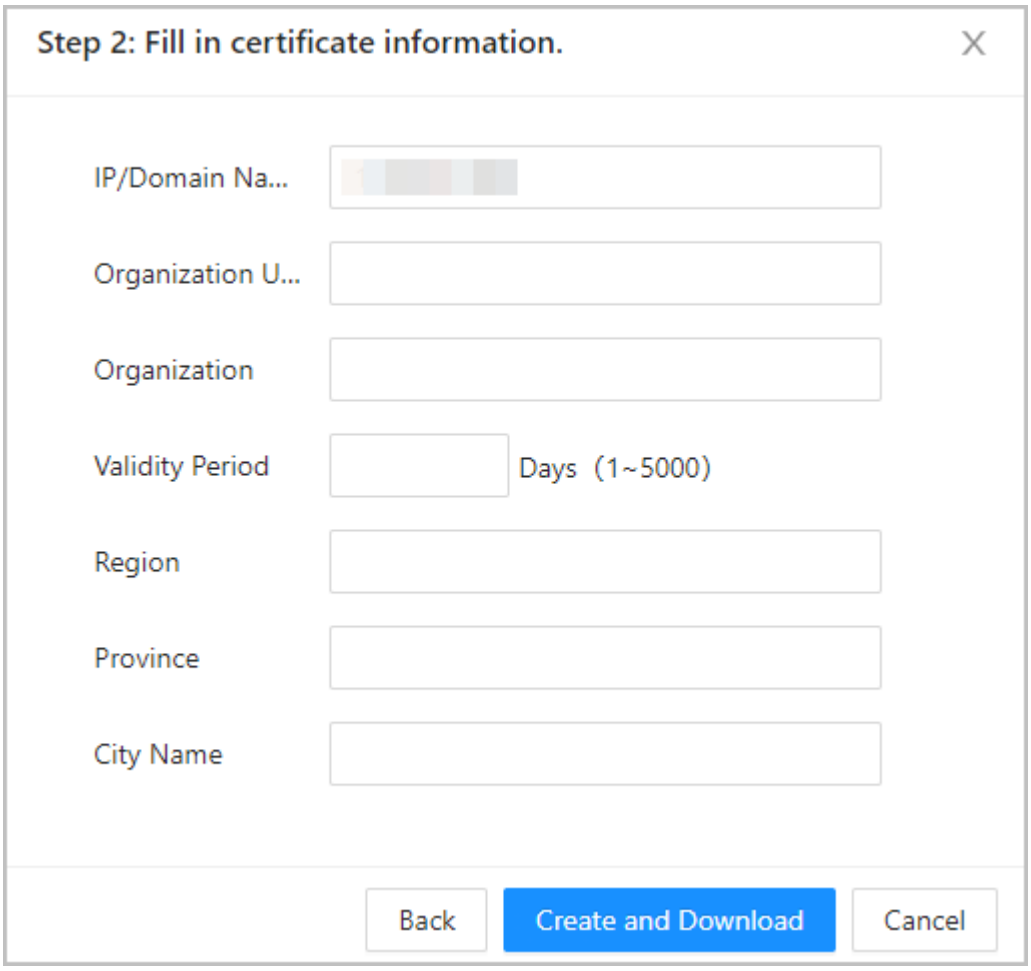
Step 2 Click **Install Device Certificate**.

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

Step 4 Enter the certificate information.

- IP/Domain name: the IP address or domain name of the Access Controller.
- Region: The name of region must not exceed 3 characters. We recommend you enter the abbreviation of region name.

Figure 2-80 Certificate information (2)



Step 5 Click **Create and Download**.

Save the request file to your computer.

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

Step 7 Import the signed CA certificate.

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

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

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

Related Operations

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

- Click to download the certificate.
- Click to delete the certificate.

2.2.23.4.3 Installing Existing Certificate

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

Procedure

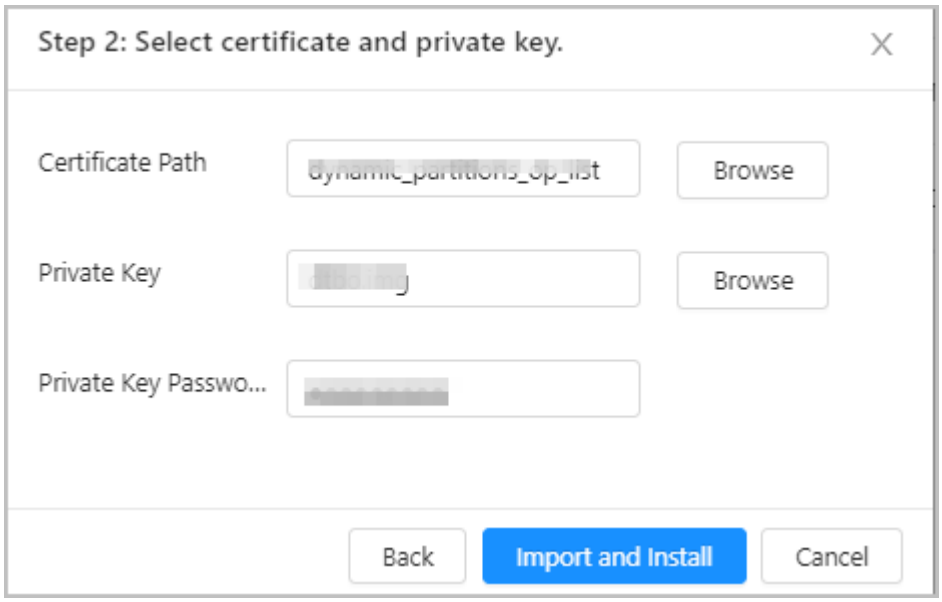
Step 1 Select **Security** > **CA Certificate** > **Device Certificate**.

Step 2 Click **Install Device Certificate**.

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

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

Figure 2-81 Certificate and private key



Step 5 Click **Import and Install**.

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

Related Operations

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

2.2.23.5 Installing the Trusted CA Certificate

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

Background Information

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

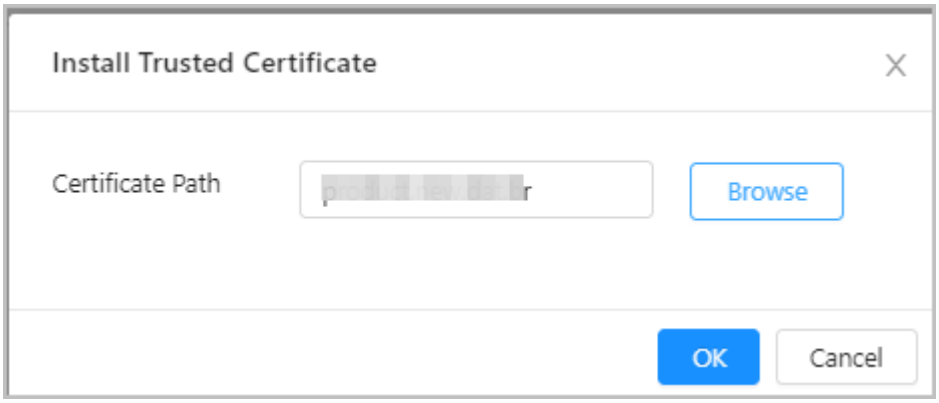
Procedure

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

Step 2 Select **Install Trusted Certificate**.

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

Figure 2-82 Install the trusted certificate



Step 4 Click **OK**.

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

Related Operations

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

2.2.23.6 Security Warning

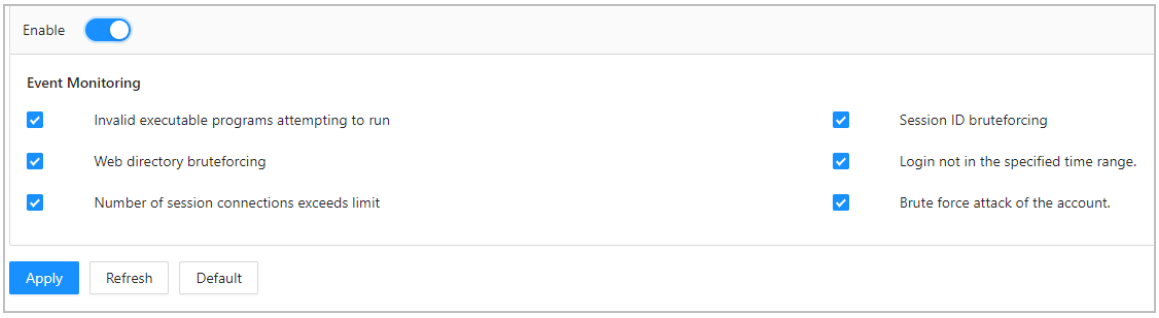
Procedure

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

Step 2 Enable the security warning function.

Step 3 Select the monitoring items.

Figure 2-83 Security warning



Step 4 Click **Apply**.

2.3 Configurations of Sub Controller

You can log in to the webpage of the sub controller to configure it locally.

2.3.1 Initialization

Initialize the sub controller when you log in to the webpage for the first time or after the sub controller is restored to its factory default settings. For details on how to initialize the sub controller, see "2.2.2 Initialization".

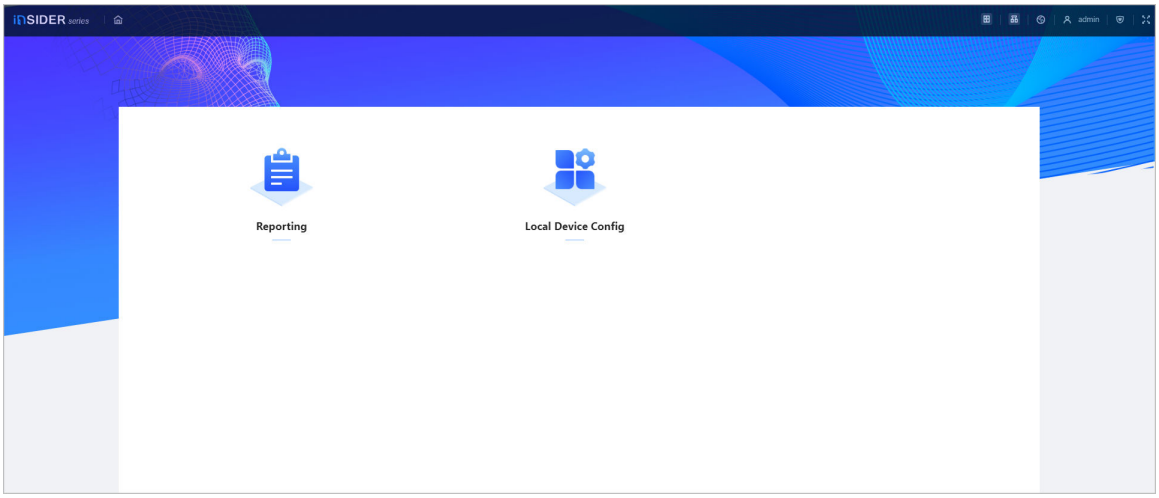
2.3.2 Logging In

Set the Access Control to sub controller while going through the login wizard. For details, see "2.2.3 Logging In".

2.3.3 Home Page

The webpage of the sub controller only includes **Local Device Config** and **Reporting** menu. For details, see "2.2.21 Local Device Configurations (Optional)" and "2.2.22 Viewing Records".

Figure 2-84 Home page

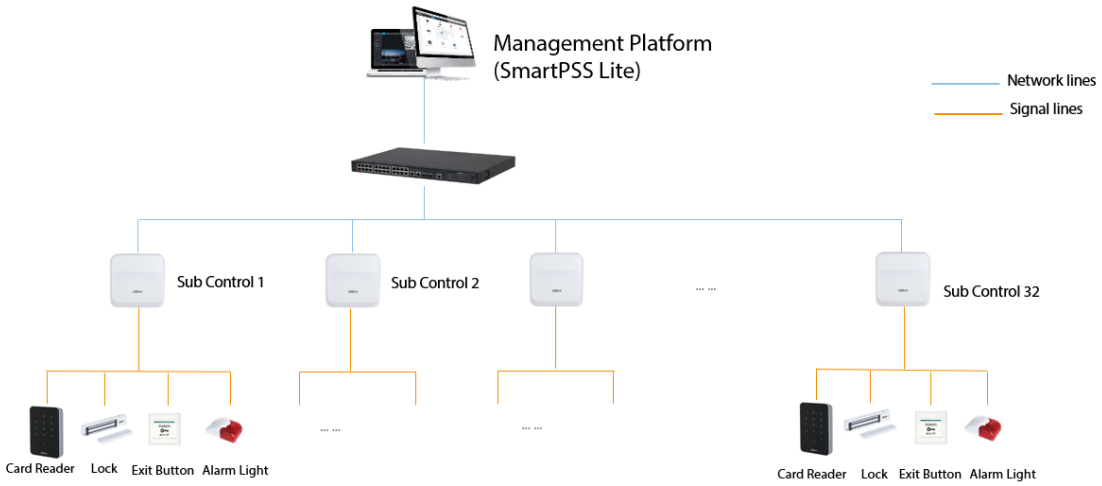


3 Smart PSS Lite-Sub Controllers

3.1 Networking Diagram

The sub controllers are added to a standalone management platform, such as SmartPSS Lite. You can manage all sub controllers through SmartPSS Lite.

Figure 3-1 Networking Diagram



3.2 Configurations on SmartPSS Lite

Add sub controllers to SmartPSS Lite and configure them on the platform. For details, see the user's manual of SmartPSS Lite.

3.3 Configurations on Sub Controller

For details, see "2.3 Configurations of Sub Controller".

Appendix 1 Cybersecurity Recommendations

Cybersecurity is more than just a buzzword: it's something that pertains to every device that is connected to the internet. IP video surveillance is not immune to cyber risks, but taking basic steps toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations from Dahua on how to create a more secured security system.

Mandatory actions to be taken for basic device network security:

1. **Use Strong 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; character types include 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 overlapped characters, such as 111, aaa, etc.

2. **Update Firmware and Client Software in Time**

   - According to the standard procedure in Tech-industry, we recommend to keep your device (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the device is connected to the public network, it is recommended to enable the "auto-check for updates" function to obtain timely information of firmware updates released by the manufacturer.
   - We suggest that you download and use the latest version of client software.

"Nice to have" recommendations to improve your device network security:

1. **Physical Protection**

   We suggest that you perform physical protection to device, especially storage devices. For example, place the device in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable device (such as USB flash disk, serial port), etc.

2. **Change Passwords Regularly**

   We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

3. **Set and Update Passwords Reset Information Timely**

   The device supports password reset function. Please set up related information for password reset in time, including the end user's mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

4. **Enable Account Lock**

   The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

5. **Change Default HTTP and Other Service Ports**

   We suggest you to change default HTTP and other service ports into any set of numbers between 1024–65535, reducing the risk of outsiders being able to guess which ports you are using.

6. **Enable HTTPS**

   We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

7. **MAC Address Binding**

   We recommend you to bind the IP and MAC address of the gateway to the device, thus reducing the risk of ARP spoofing.

8. **Assign Accounts and Privileges Reasonably**

   According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

9. **Disable Unnecessary Services and Choose Secure Modes**

   If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.

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

   - SNMP: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
   - SMTP: Choose TLS to access mailbox server.
   - FTP: Choose SFTP, and set up strong passwords.
   - AP hotspot: Choose WPA2-PSK encryption mode, and set up strong passwords.

10. **Audio and Video Encrypted Transmission**

    If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

    Reminder: encrypted transmission will cause some loss in transmission efficiency.

11. **Secure Auditing**

    - Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
    - Check device log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

12. **Network Log**

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

13. **Construct a Safe Network Environment**

    In order to better ensure the safety of device and reduce potential cyber risks, we recommend:

    - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
    - The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
    - Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
    - Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.

More information

Please visit Dahua official website security emergency response center for security announcements and the latest security recommendations.

ENABLING A SAFER SOCIETY AND SMARTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.
Address: No. 1399, Binxing Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053
Email: dhoverseas@dhvisiontech.com | Tel: +86-571-87688888 28933188