SmartPSS Lite Access Control Solution

User's Manual

V1.1.2

Foreword

General

This manual introduces the functions and operations of the access control solution of the SmartPSS Lite platform (hereinafter referred to as "the Platform"). Read carefully before using the platform, 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
V1.1.2	Updated the person management and access control configurations.	January 2024
V1.1.1	Updated the home page layout.	September 2023
V1.1.0	● Updated person management function. ● Updated access controller configuration function.	December 2022
V1.0.1	Updated staff display image.	August 2022
V1.0.0	First release.	April 2022

Privacy Protection Notice

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

About the Manual

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

Table of Contents

1 Overview

The access control solution is used with the access control devices through SmartPSS Lite platform, which is helpful in small and medium scenarios such as controlling doors remotely and configuring alarms.

2 Access Guide

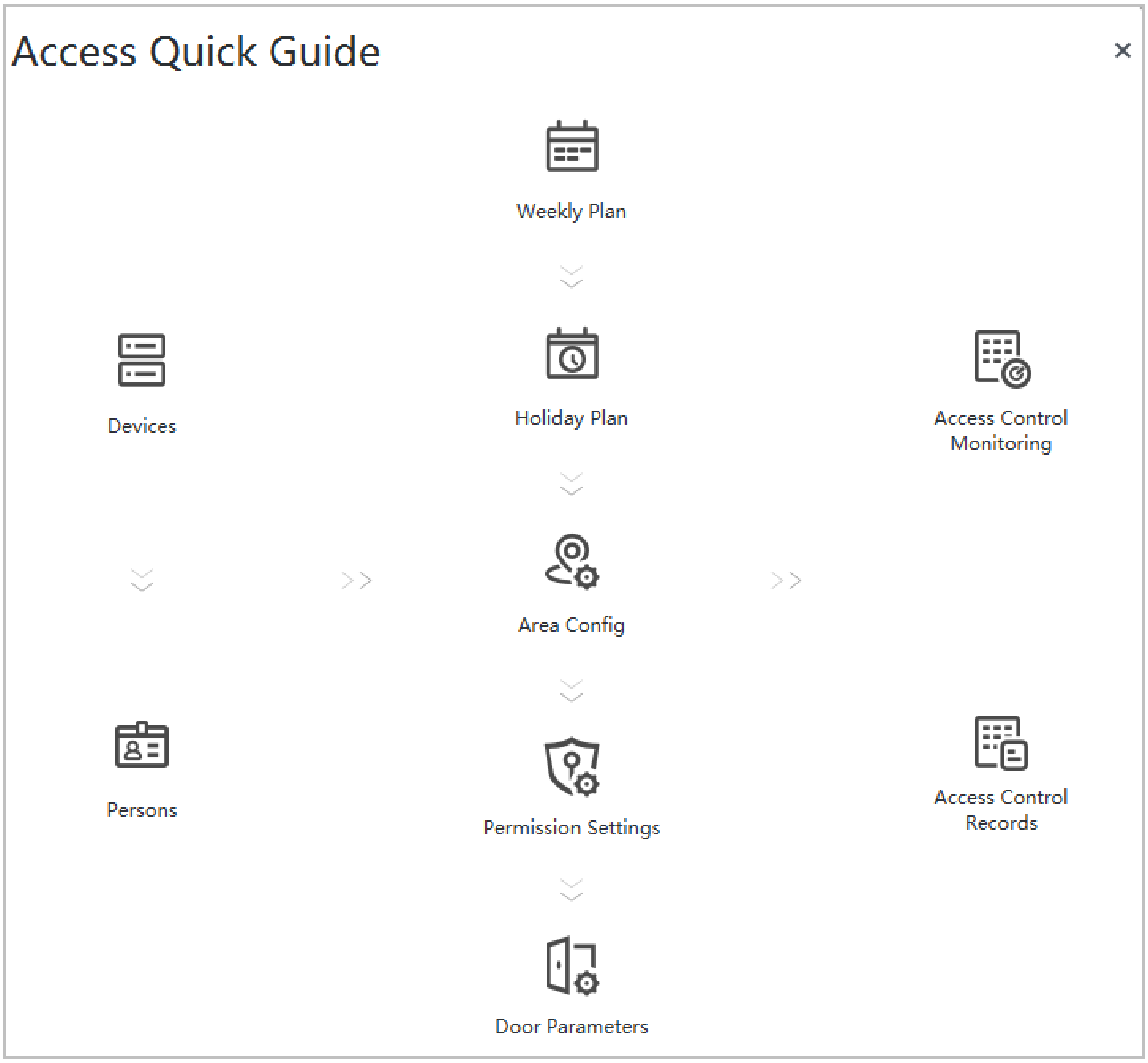
You can configure the access control by following the guide below.

Procedure

Step 1 Select **Access Control** in the left bar.

Step 2 Click **Guide** on the home page.

Figure 2-1 Access guide



3 Person Management

3.1 Adding Company

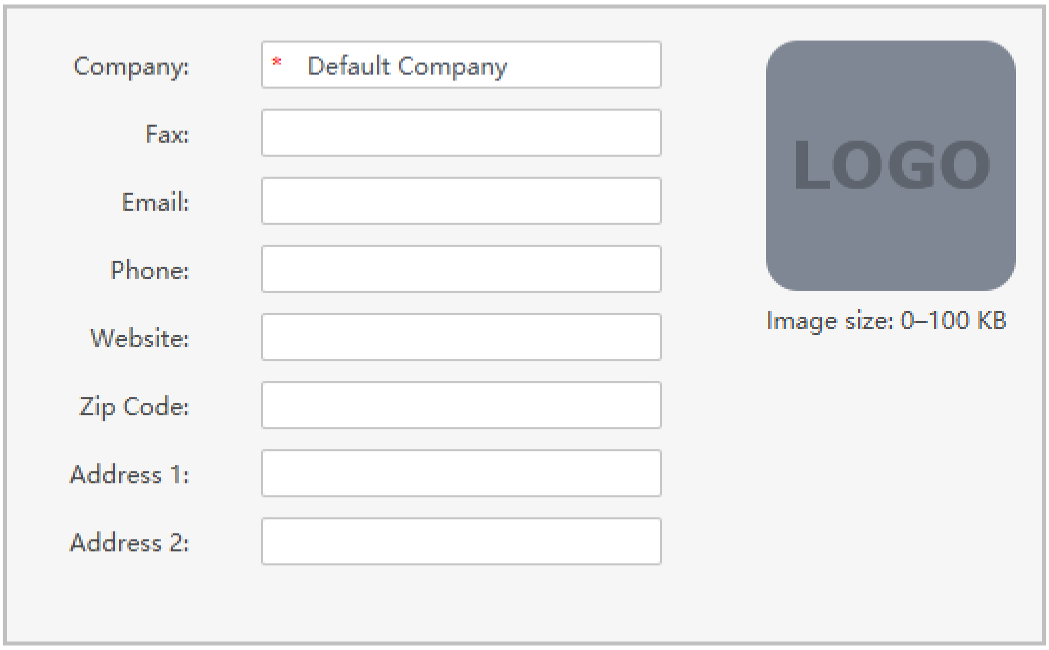
Procedure

Step 1 Select **Person** > **Company**.

Step 2 Configure the company information.

Step 3 Upload the company logo, and then click **OK**.

Figure 3-1 Add company



Company: * Default Company

Fax:

Email:

Phone:

Website:

Zip Code:

Address 1:

Address 2:

Image size: 0–100 KB

3.2 Adding Person

Background Information

Select one of the methods to add staff.

- Add staff one by one manually.
- Add staff in batches.
- Extract staff information from other devices.
- Import staff information from the local.

3.2.1 Adding Departments

Procedure

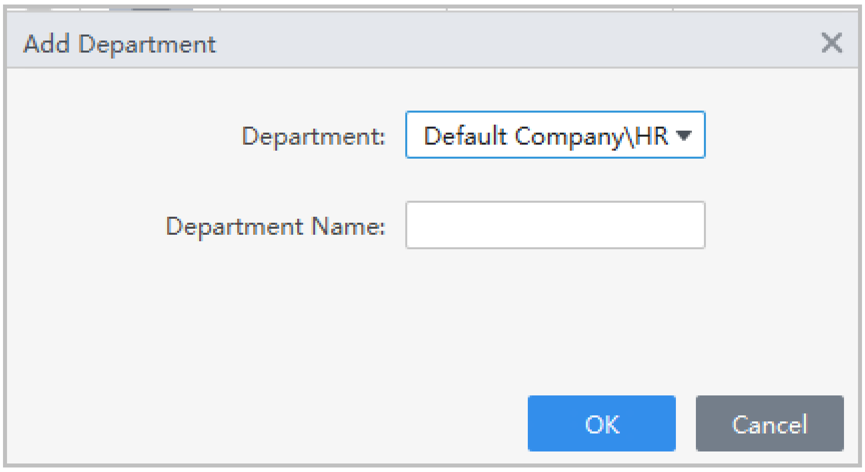
Step 1 Select **Person** > **Person Management**.

Step 2 In the department organization tree, click +.

Step 3 Select an existing department, and then enter the name of the new department.

Step 4 Click **OK**.

Figure 3-2 Add departments



Department: Default Company\HR

Department Name:

Related Operations

- Click 🗑 to delete the department.
- Click ✎ to rename the department.

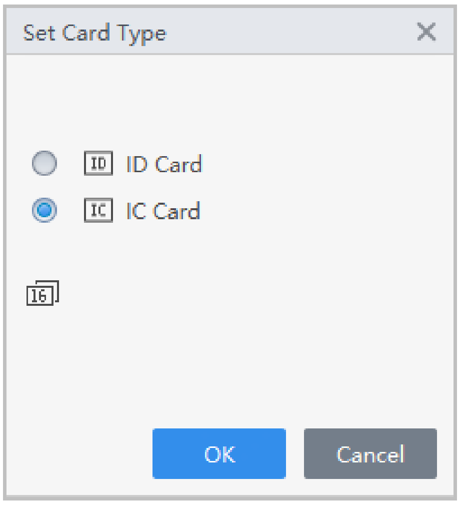
3.2.2 Setting Card Type

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

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

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

Figure 3-3 Set card type



○ ID Card

● IC Card

3.2.3 Adding Personnel One by One

Procedure

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

Step 2 Enter basic information of person.

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

- Set password

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

- Configure card

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

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

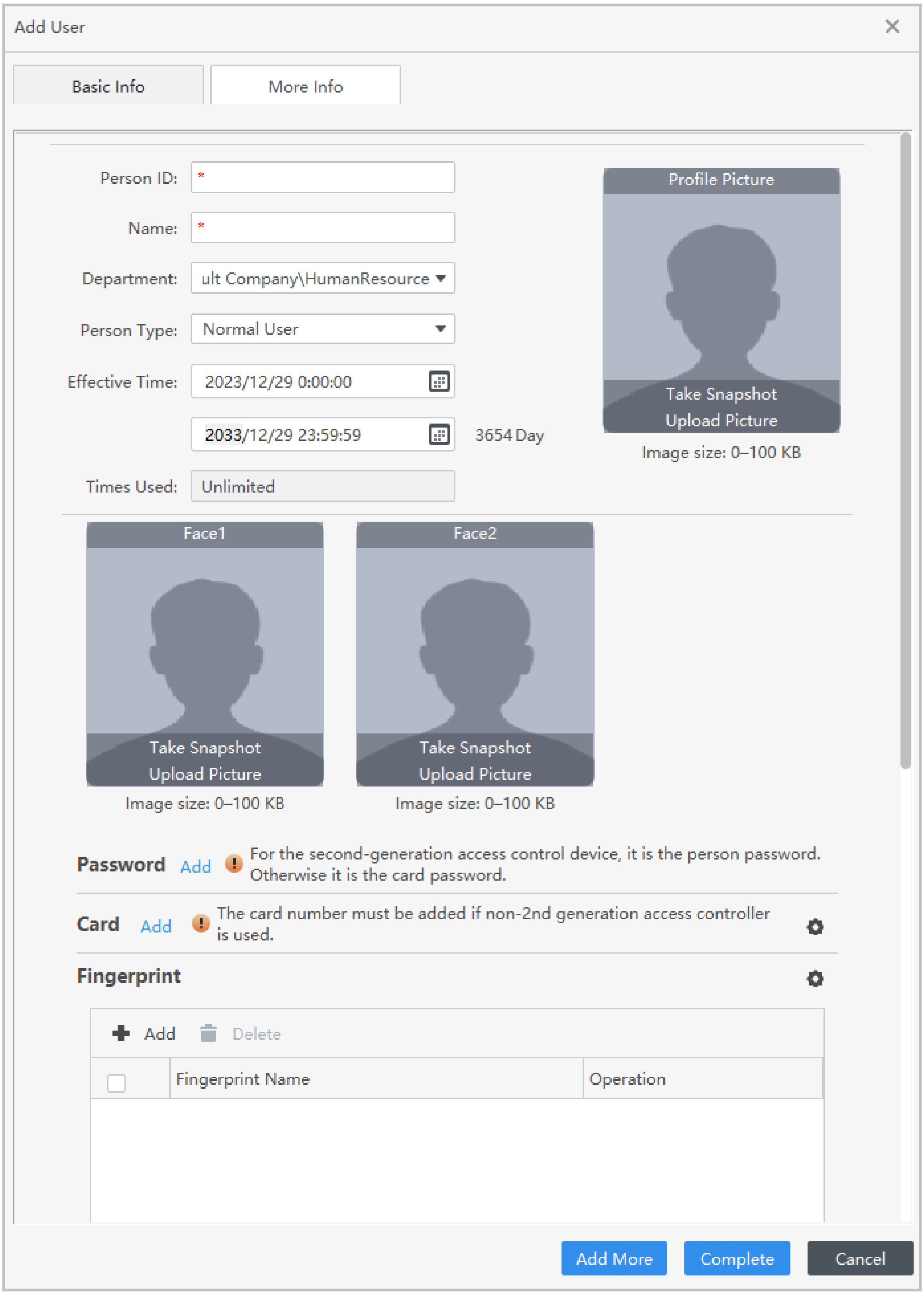
- Configure fingerprint

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

- Configure feature codes

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

Figure 3-4 Add basic information



Person ID: *

Name: *

Department: ult Company\HumanResource

Person Type: Normal User

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

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

Times Used: Unlimited

Image size: 0–100 KB

Image size: 0–100 KB

Image size: 0–100 KB

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

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

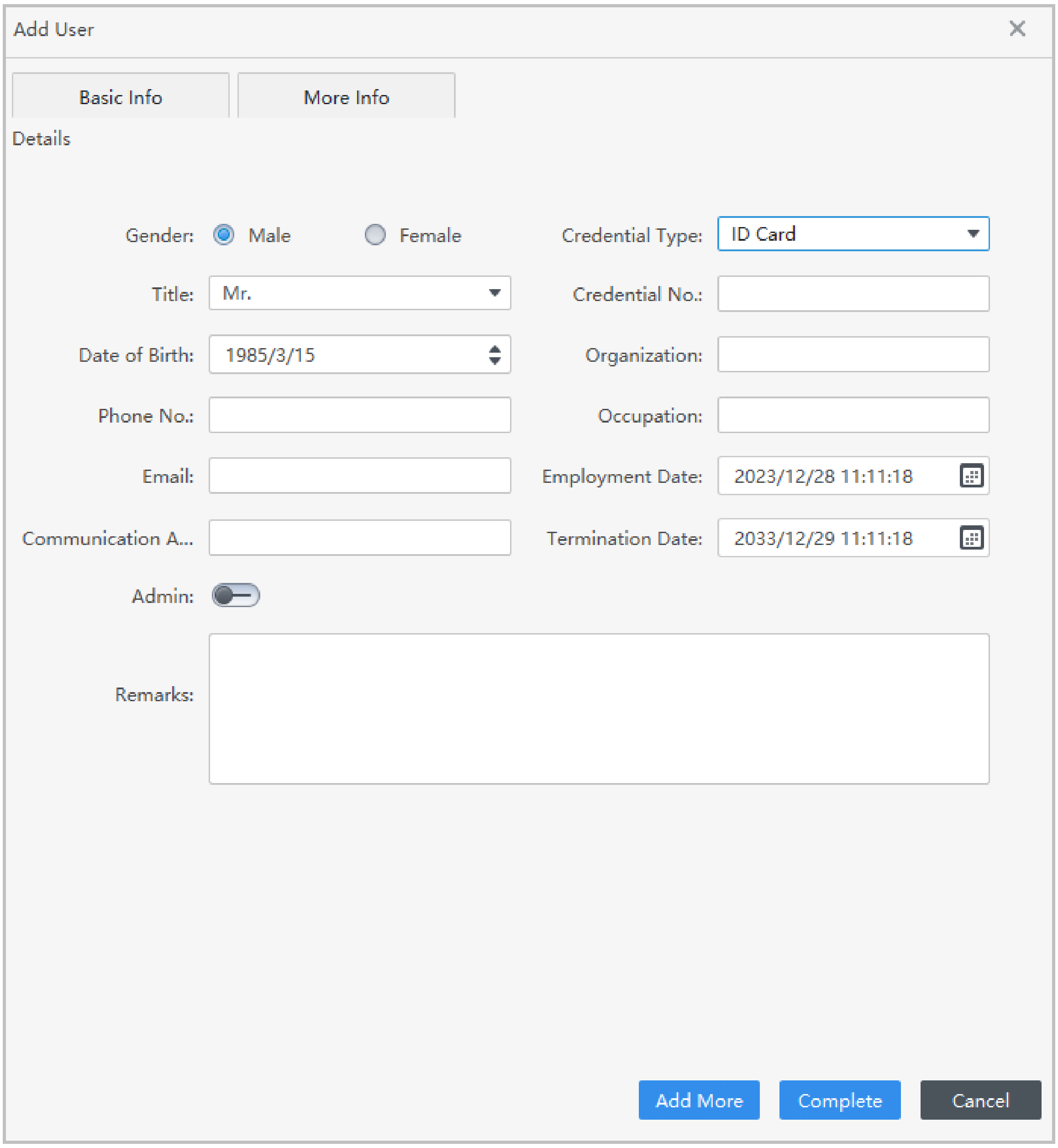
Fingerprint

➕ Add 🗑 Delete

□	Fingerprint Name	Operation

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

Figure 3-5 Add more information



Add User

Basic Info | More Info

Details

Gender: ● Male ○ Female

Title: Mr.

Date of Birth: 1985/3/15

Phone No.:

Email:

Communication A...:

Admin:

Remarks:

Credential Type: ID Card

Credential No.:

Organization:

Occupation:

Employment Date: 2023/12/28 11:11:18

Termination Date: 2033/12/29 11:11:18

Step 4 Click **Complete**.

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

Related Operations

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

3.2.4 Adding Personnel in Batches

Procedure

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

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

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

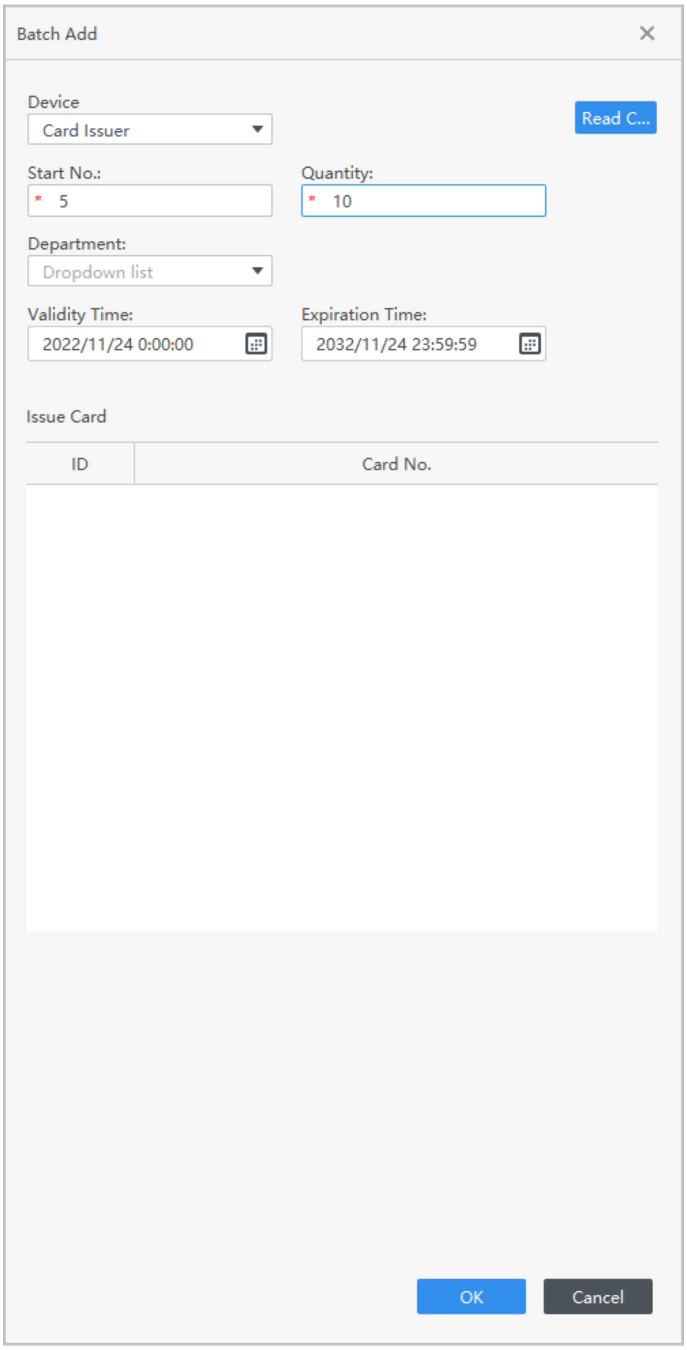
Step 4 Click **Read Card No.**.

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

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

Step 6 Click **OK**.

Figure 3-6 Add personnel in batches



Batch Add

Device: Card Issuer

Start No.: * 5

Quantity: * 10

Department: Dropdown list

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

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

Issue Card

ID	Card No.

3.2.5 Other Operations

3.2.5.1 Issuing Cards in Batches

You can issue cards to staffs who have been added but have no card.

Procedure

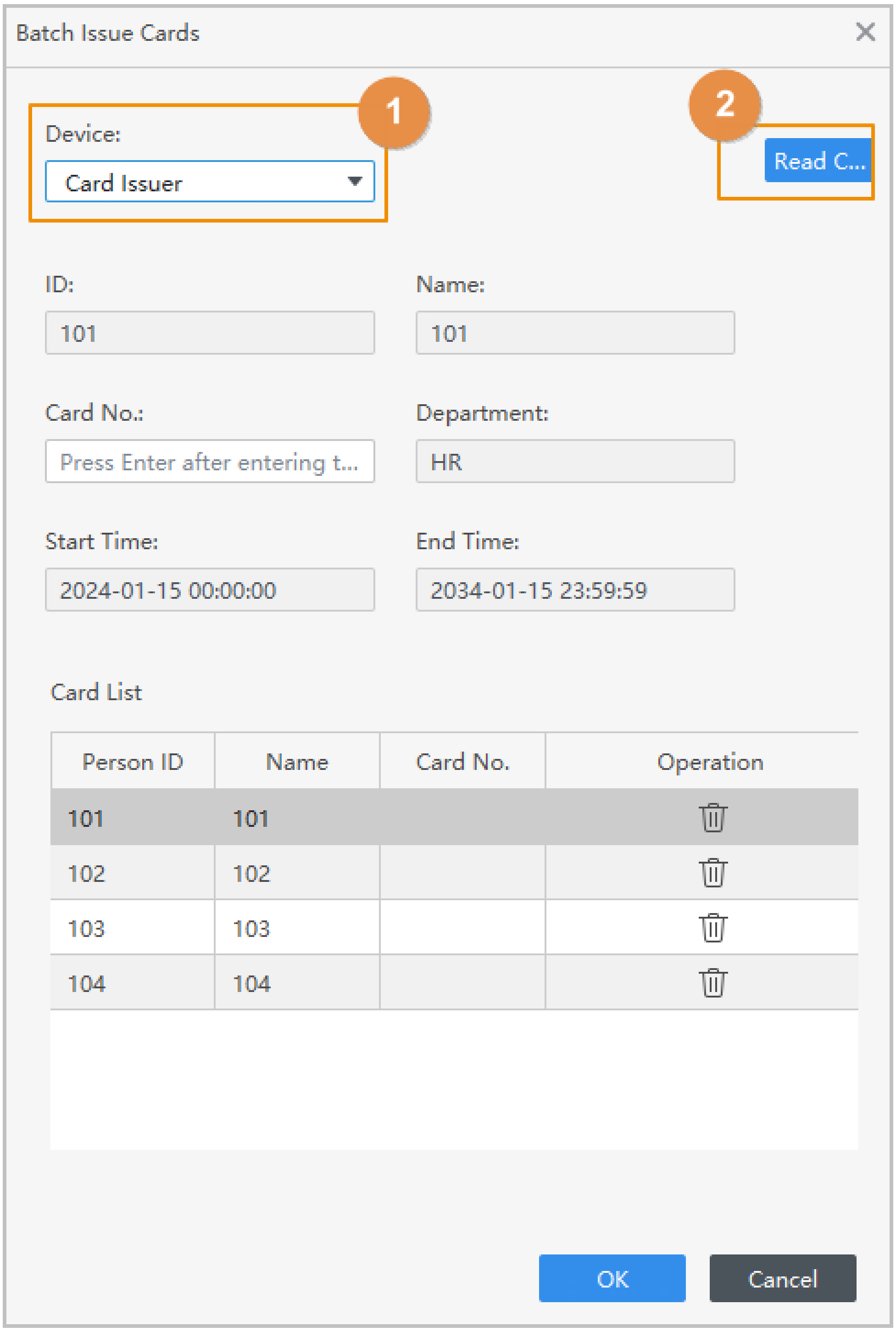
Step 1 Select **Person** > **Person Management**.

Step 2 Select personnel, and then select **Batch Update** > **Batch Issue Card**.

Step 3 Issue card in batches. Card number can be read automatically by card reader or entered manually.

- Use card issuer or card reading device to automatically read card number.
  1. Select the card issuer or a card reading device, and then click **Read Card No.**.
  2. According to the order list, put the cards of the corresponding personnel on the card swiping area in sequence, and then the system will automatically read and fill in the card number.

Figure 3-7 Read automatically



Device: Card Issuer

ID: 101

Name: 101

Card No.: Press Enter after entering t...

Department: HR

Start Time: 2024-01-15 00:00:00

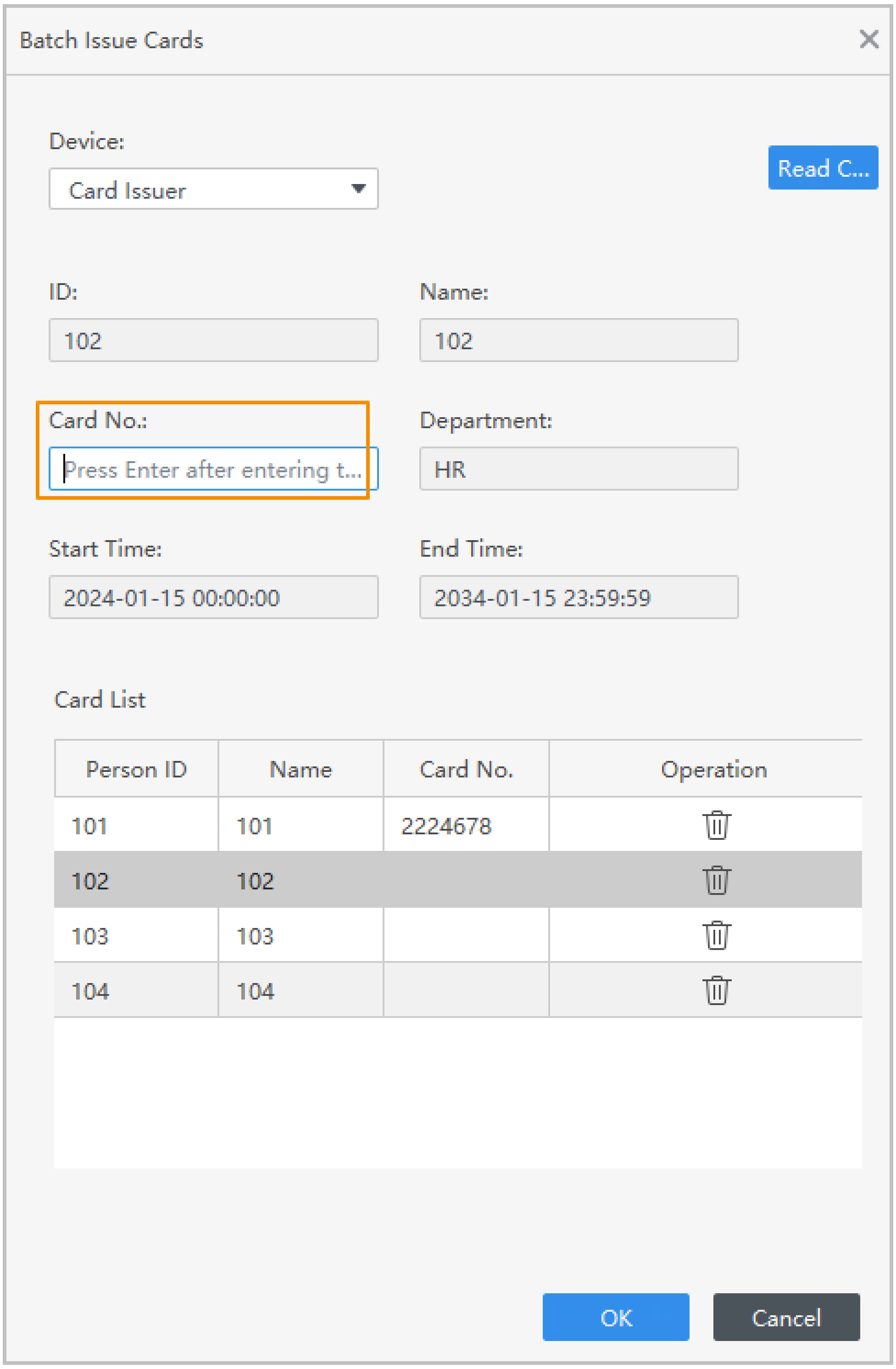
End Time: 2034-01-15 23:59:59

Card List

Person ID	Name	Card No.	Operation
101	101		🗑
102	102		🗑
103	103		🗑
104	104		🗑

- Enter manually
  1. Select the personnel in card list, and then enter the corresponding card number.
  2. Press the **Enter** key.

Figure 3-8 Enter card number manually



Batch Issue Cards

Device: Card Issuer

ID: 102

Name: 102

Card No.: Press Enter after entering t...

Department: HR

Start Time: 2024-01-15 00:00:00

End Time: 2034-01-15 23:59:59

Card List

Person ID	Name	Card No.	Operation
101	101	2224678	🗑
102	102		🗑
103	103		🗑
104	104		🗑

Step 4 Click **OK**.

3.2.5.2 Extracting Personnel Information

Extract users from devices to the platform.

Procedure

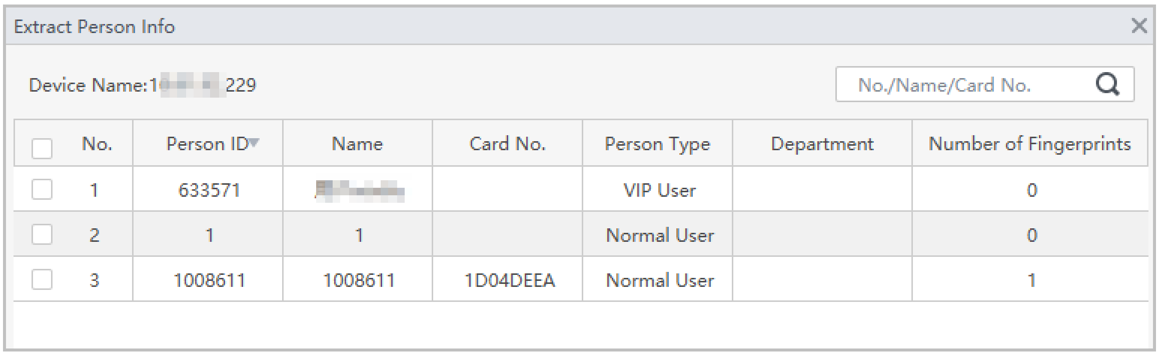
Step 1 Select **Person** > **Person Management**, and then click **Extract**

Step 2 Select a device, and then click **OK**.

You can select to extract the user of **All** , **Success** or **Failure** from the drop-down list next to **Extract**.

Step 3 Select personnel, and then click **Extract** to extract the users on the device to the platform.

Figure 3-9 Extract users



Device Name:1[redacted]229

□	No.	Person ID	Name	Card No.	Person Type	Department	Number of Fingerprints
□	1	633571	[redacted]		VIP User		0
□	2	1	1		Normal User		0
□	3	1008611	1008611	1D04DEEA	Normal User		1

Results

The users that are successfully extracted from devices will be displayed on the **Person Management** page.

3.2.5.3 Importing Personnel Information

Import personnel information to the platform.

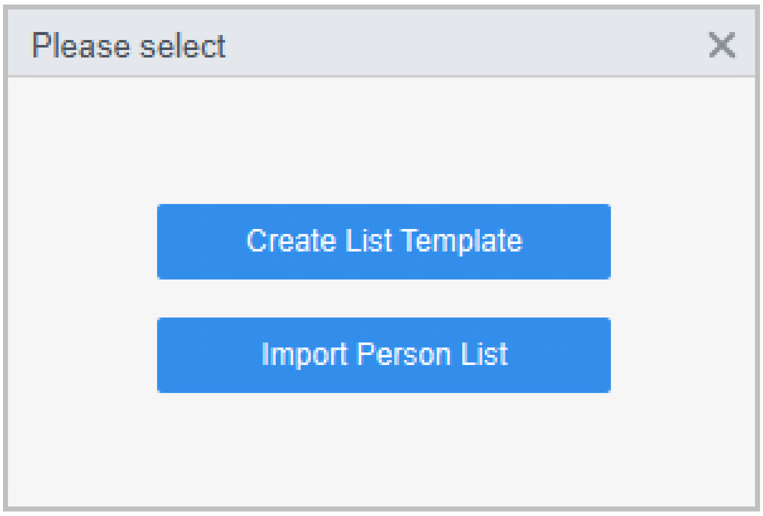
Procedure

Step 1 Click **Person** > **Person Management**, and then click **Import**.

Step 2 Click **Create List Template** to download a template.

Step 3 Fill in the template, and then click **Import Person List**.

Figure 3-10 Import staff information



3.2.5.4 Exporting Personnel Information

Select **Person** > **Person Management**, select personnel, and then click **Export** to export personnel information to your computer.

3.2.5.5 Searching for Personnel

Select **Person** > **Person Management**, search for personnel by ID, name or card.

Figure 3-11 Search for staff

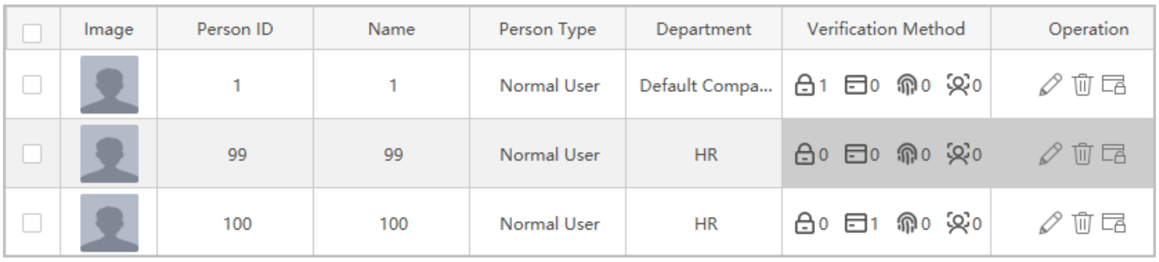
ID / Name / Card 🔍

3.2.5.6 Personnel Display

You can select display modes: card display and list display.

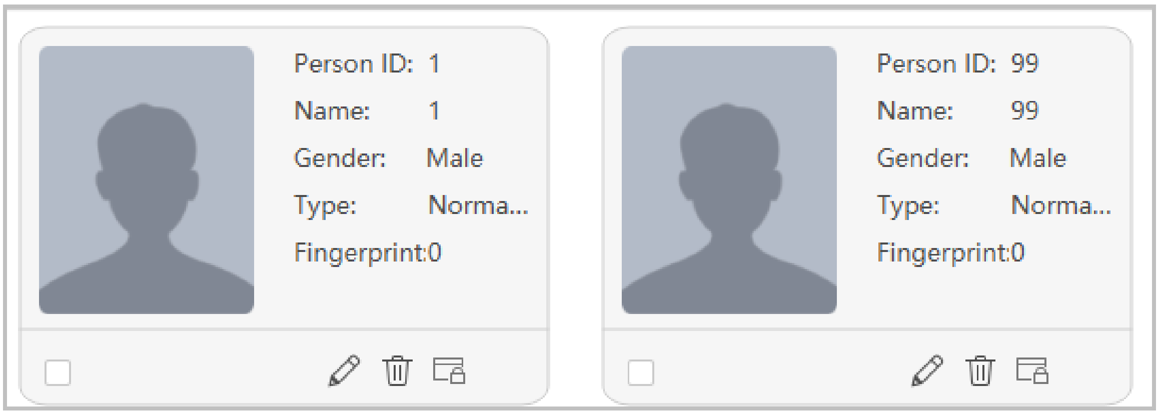
Click ▦ to display in cards; click ☰ to display in list.

Figure 3-12 Display in list



□	Image	Person ID	Name	Person Type	Department	Verification Method	Operation
□		1	1	Normal User	Default Compa...	🔒1 ▭0 ⦿0 ☺0	✎ 🗑 ▭
□		99	99	Normal User	HR	🔒0 ▭0 ⦿0 ☺0	✎ 🗑 ▭
□		100	100	Normal User	HR	🔒0 ▭1 ⦿0 ☺0	✎ 🗑 ▭

Figure 3-13 Display in card



Person ID: 1
Name: 1
Gender: Male
Type: Norma...
Fingerprint:0
□ ✎ 🗑 ▭

Person ID: 99
Name: 99
Gender: Male
Type: Norma...
Fingerprint:0
□ ✎ 🗑 ▭

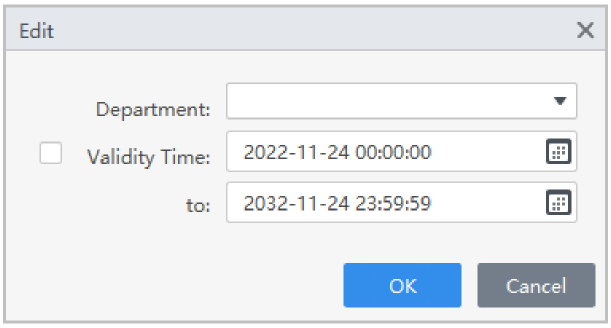
3.2.5.7 Editing Personnel in Batches

Procedure

Step 1 Select **Person** > **Person Management**.

Step 2 Select personnel, and then select **Batch Update** > **Batch Edit** to edit department and validity period in batches.

Figure 3-14 Edit department



Edit

Department:

□ Validity Time: 2022-11-24 00:00:00

to: 2032-11-24 23:59:59

3.3 Person Collection

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

Prerequisites

The push person information function is enabled on the access control device.

This function is only available on select models of access control device.

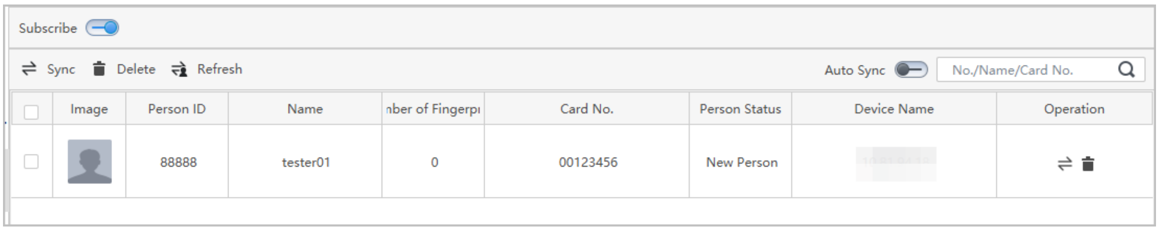
Procedure

Step 1 Select **Person** > **Person Collection**.

Step 2 Turn on **Subscribe**.

Step 3 If you have added new user or modified user information on the access control device, the user will be automatically pushed to the management platform.

Figure 3-15 Subscribe users

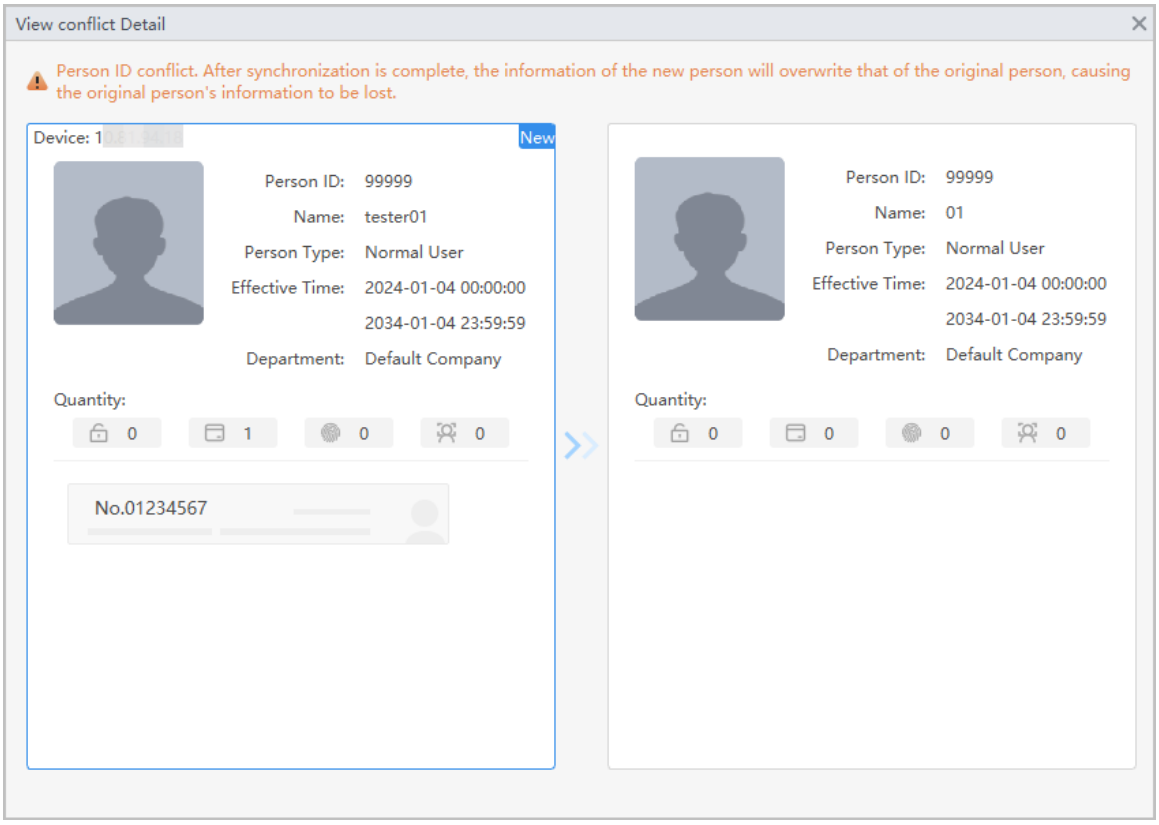


□	Image	Person ID	Name	nber of Fingerpı	Card No.	Person Status	Device Name	Operation
□		88888	tester01	0	00123456	New Person	[redacted]	⇌

Step 4 You can click ⇌ to synchronize the user to person management page.

If the user that are pushed to the platform have the same person ID or same card with any existing user in the **Person Management** page, the system will prompt conflict information. You can click to see details.

Figure 3-16 Person ID conflict



View conflict Detail

Person ID conflict. After synchronization is complete, the information of the new person will overwrite that of the original person, causing the original person's information to be lost.

Device: 1[redacted]

New

Person ID: 99999

Name: tester01

Person Type: Normal User

Effective Time: 2024-01-04 00:00:00

2034-01-04 23:59:59

Department: Default Company

Quantity:

0 1 0 0

No.01234567

Person ID: 99999

Name: 01

Person Type: Normal User

Effective Time: 2024-01-04 00:00:00

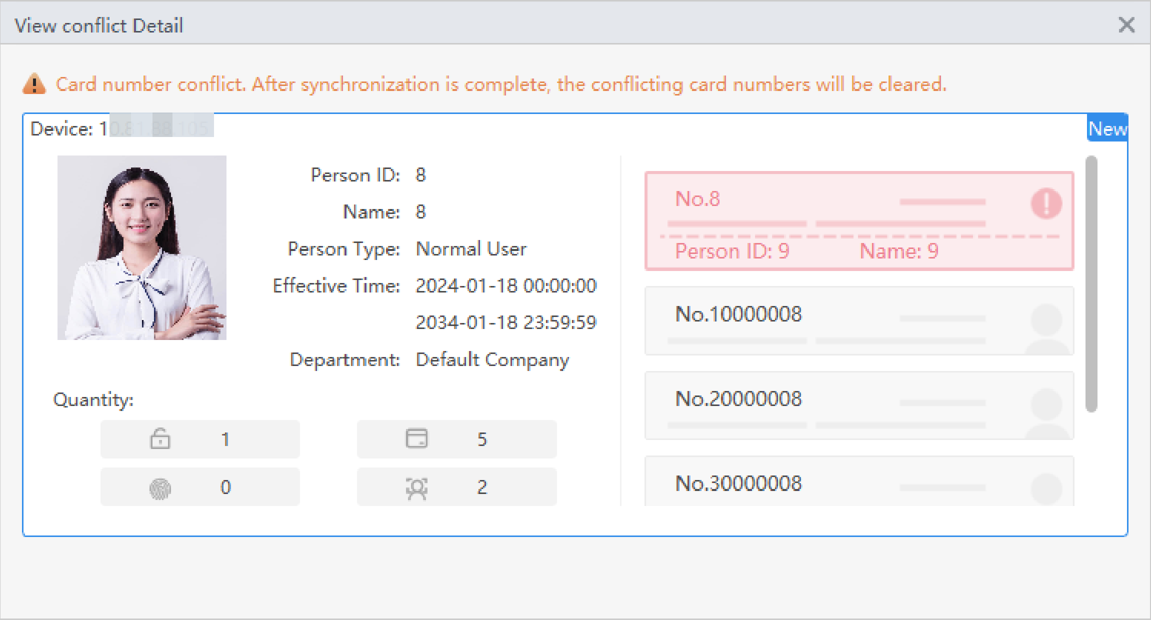
2034-01-04 23:59:59

Department: Default Company

Quantity:

0 0 0 0

Figure 3-17 Card number conflict



View conflict Detail

Card number conflict. After synchronization is complete, the conflicting card numbers will be cleared.

Device: 1[redacted]

New

Person ID: 8

Name: 8

Person Type: Normal User

Effective Time: 2024-01-18 00:00:00

2034-01-18 23:59:59

Department: Default Company

Quantity:

1 5

0 2

No.8

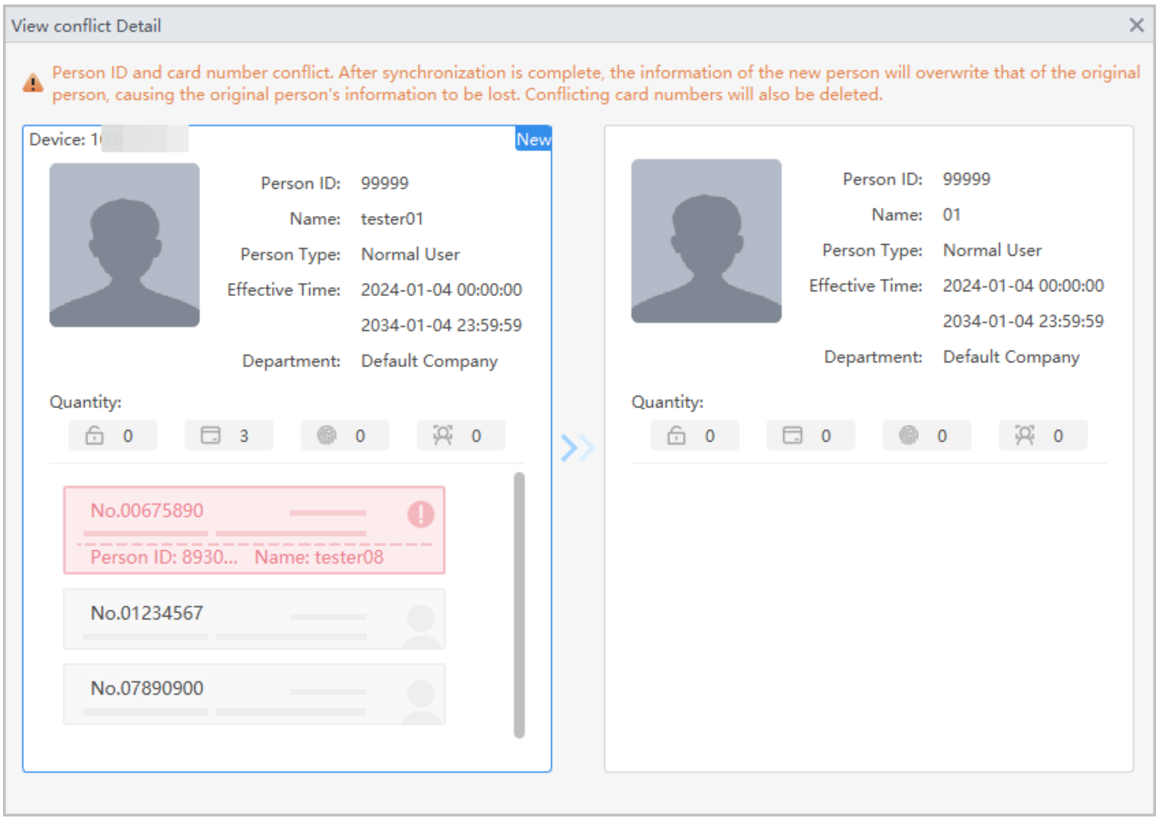
Person ID: 9 Name: 9

No.10000008

No.20000008

No.30000008

Figure 3-18 Person ID and card number conflict



View conflict Detail

Person ID and card number conflict. After synchronization is complete, the information of the new person will overwrite that of the original person, causing the original person's information to be lost. Conflicting card numbers will also be deleted.

Device: 1[redacted]

New

Person ID:	99999
Name:	tester01
Person Type:	Normal User
Effective Time:	2024-01-04 00:00:00
	2034-01-04 23:59:59
Department:	Default Company

Quantity: 0 3 0 0

No.00675890
Person ID: 8930... Name: tester08

No.01234567

No.07890900

Person ID:	99999
Name:	01
Person Type:	Normal User
Effective Time:	2024-01-04 00:00:00
	2034-01-04 23:59:59
Department:	Default Company

Quantity: 0 0 0 0

Related Operations

- Synchronize users in batches: Select users, and then click **Sync** , the selected users will be automatically synchronized to **Person Management** page.
- Automatically synchronize users: Enable **Auto Sync** , If the users that are pushed to the platform does not have the same person ID or same card with any existing user in the **Person Management** page, and the users will be automatically synchronized to **Person Management** page.
- Refresh: Refresh users with conflict information.

4 Permission Configuration

4.1 Adding Permission 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 Select **Access Control Config** > **Area Setting**.

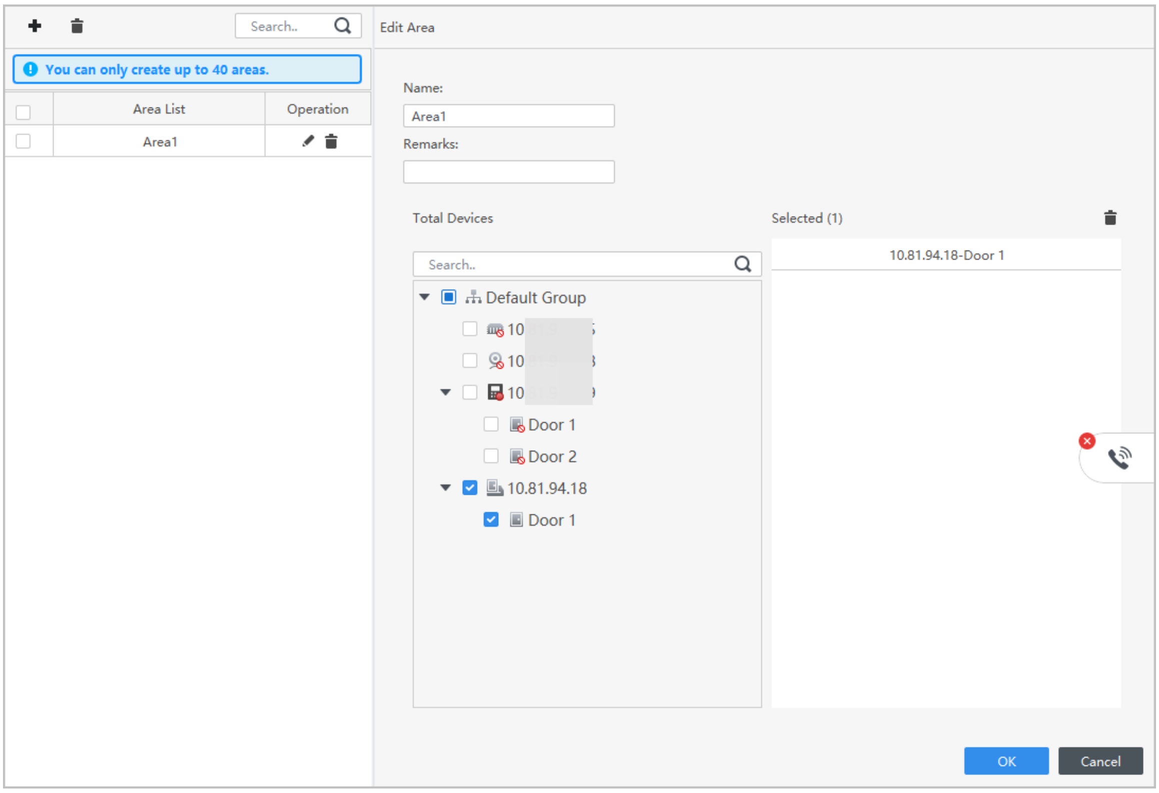
Step 2 Click ✚ to add a permission area.

You can add up to 40 areas.

Step 3 Configure the permission area.

1. Enter area name and remark.
2. Select door channels, such as door 1.
3. Click **OK**.

Figure 4-1 Add permission area



Search..

You can only create up to 40 areas.

	Area List	Operation
□	Area1	✎ 🗑

Edit Area

Name: Area1

Remarks:

Total Devices

Search..

- ■ Default Group
  - □ 10[redacted]
  - □ 10[redacted]
  - □ 10[redacted]
    - □ Door 1
    - □ Door 2
  - ☑ 10.81.94.18
    - ☑ Door 1

Selected (1)

10.81.94.18-Door 1

Related Operations

- 🗑: Delete the permission area.
- ✎: Modify the area information.

4.2 Assigning Permissions

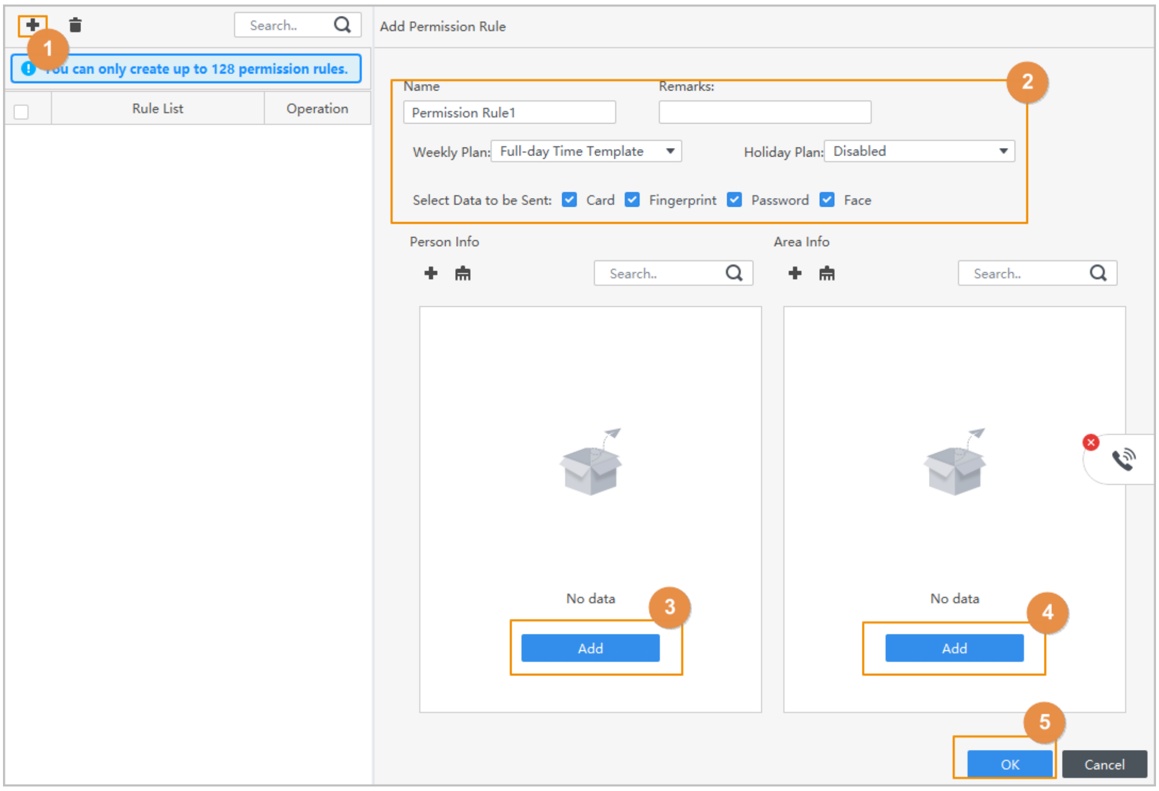
The method to configure permission for department and for personnel is similar, and here uses department as an example.

Procedure

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

Step 2 Click + to add a permission rule.

Figure 4-2 Assign permissions rules


You can only create up to 128 permission rules.

Add Permission Rule

Name: Permission Rule1

Remarks:

Weekly Plan: Full-day Time Template

Holiday Plan: Disabled

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

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

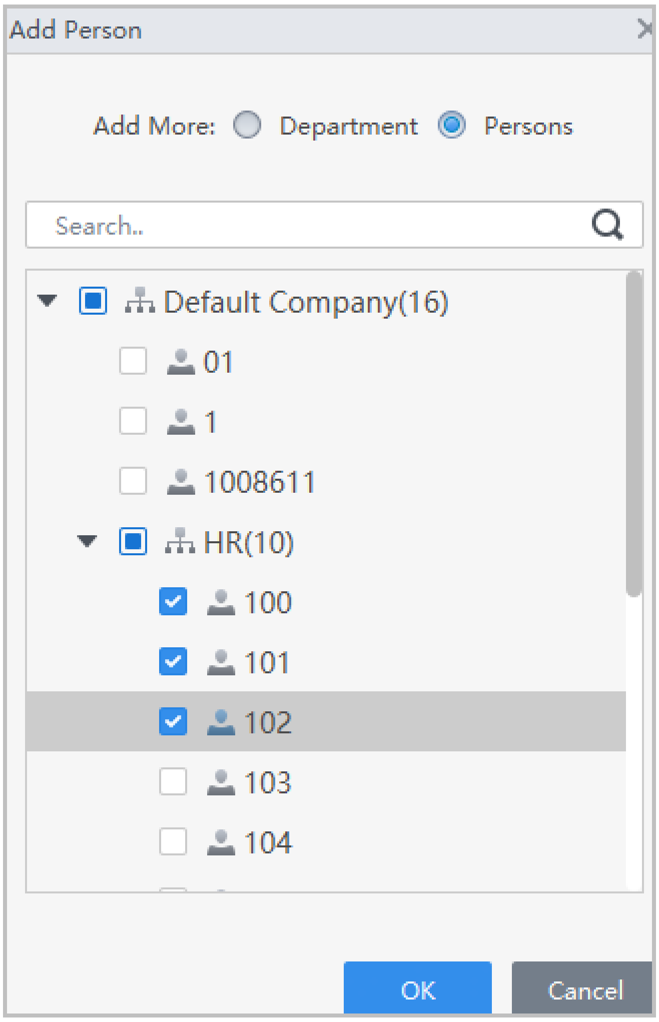
Step 4 In the **Person Info** area, click **Add** to select personnel, and then click **OK**.

You can select personnel on the department or individual users.

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

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

Figure 4-3 Add users



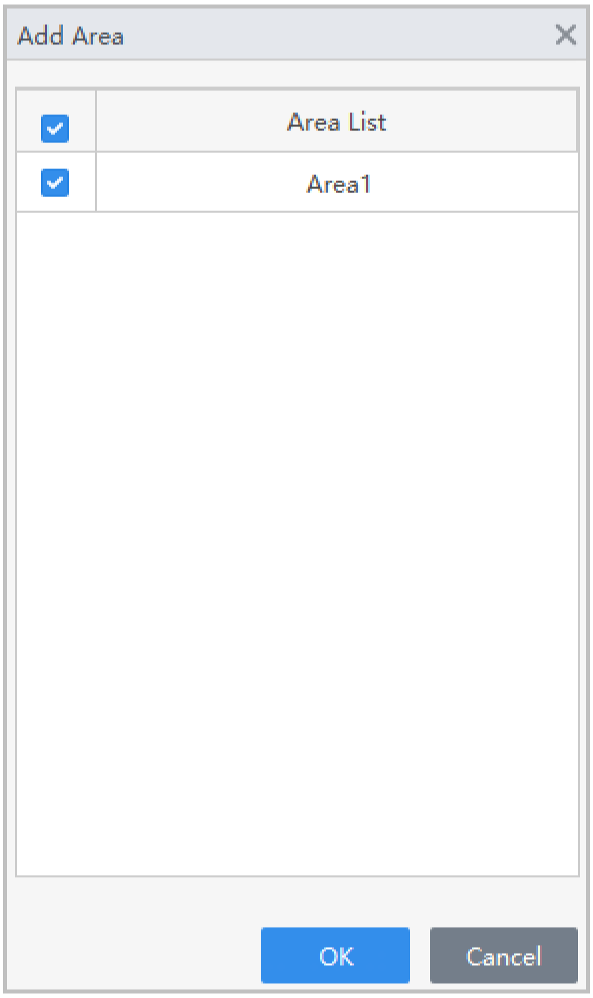
Add More: ○ Department ● Persons

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

You can click + to create new permission areas. For details on creating permission areas, see "4.1 Adding Permission Areas".

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

Figure 4-4 Add area



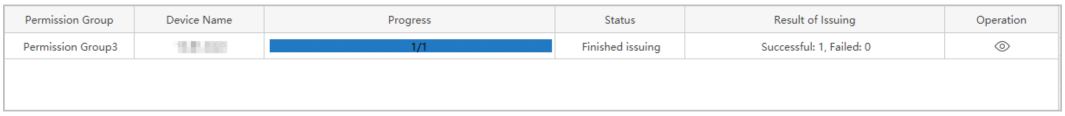
Add Area

☑	Area List
☑	Area1

Step 6 Click **OK**.

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

Figure 4-5 Authorization progress



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

4.3 Viewing Authorization Progress

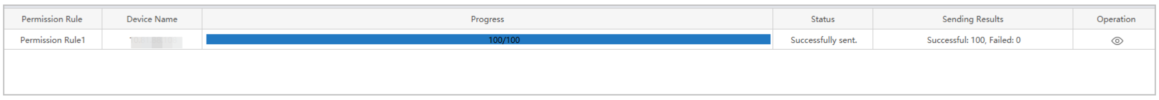
After you assign access permissions to users, you can view the authorization process.

Procedure

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

Step 2 View the authorization progress.

Figure 4-6 Authorization progress



Permission Rule	Device Name	Progress	Status	Sending Results	Operation
Permission Rule1	[redacted]	100/100	Successfully sent.	Successful: 100, Failed: 0	👁

Step 3 (Optional) If authorization failed, You can click 👁 to view details on the failed authorization tasks and resend.

5 Time Template Setting

5.1 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.

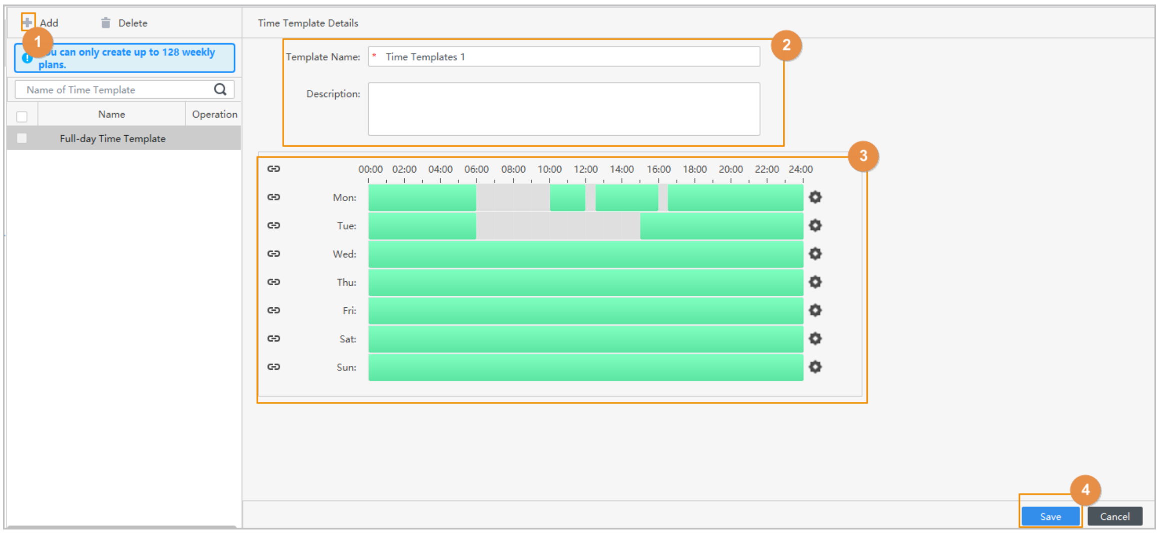
Procedure

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 5-1 Create the weekly plan



u can only create up to 128 weekly plans.

Template Name: * Time Templates 1

Description:

Step 3 Adjust the time period for each day.

- When the mouse pointer becomes a pen, you can hold and drag it to select a time range.
- When the mouse pointer becomes a eraser, you can hold and drag to cancel select a time range.

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

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

Step 4 Click **Save**.

5.2 Adding Holiday Plans (Optional)

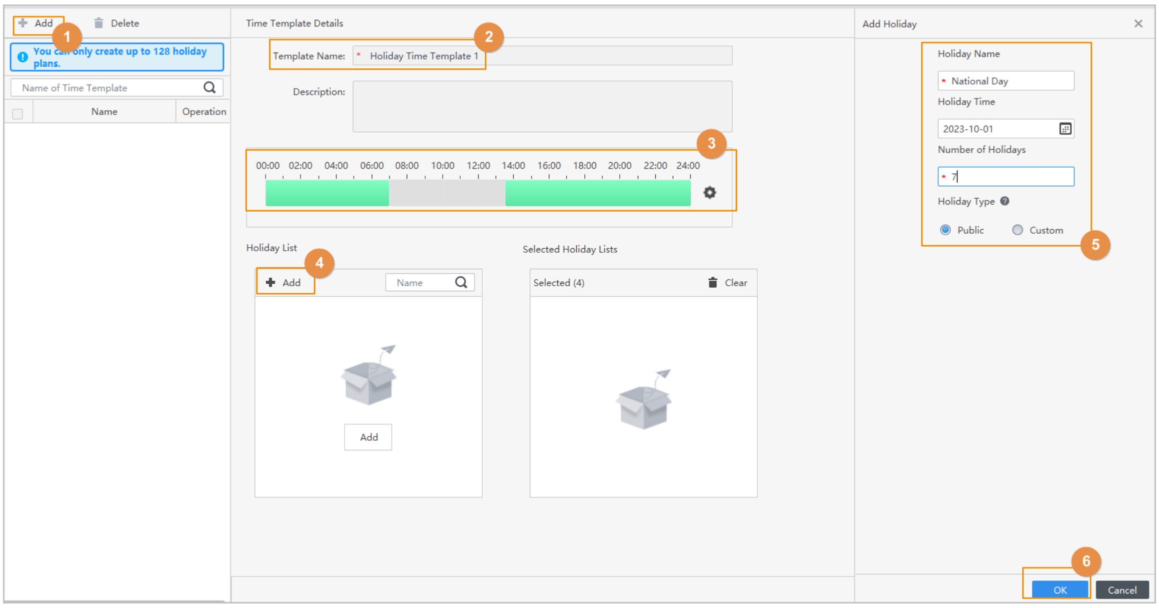
The holiday plan is used to set the unlock schedules for holidays.

Procedure

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

You can create up to 128 holiday plans.

Figure 5-2 Create holiday plan


You can only create up to 128 holiday plans.

Template Name: * Holiday Time Template 1

Holiday Name: * National Day

Holiday Time: 2023-10-01

Number of Holidays: * 7

Holiday Type: ● Public ○ Custom

Step 2 Enter the name of the holiday plan.

Step 3 Adjust the time period for each day.

- When the mouse pointer becomes a pen, you can hold and drag it to select a time range.
- When the mouse pointer becomes a eraser, you can hold and drag to cancel select a time range.

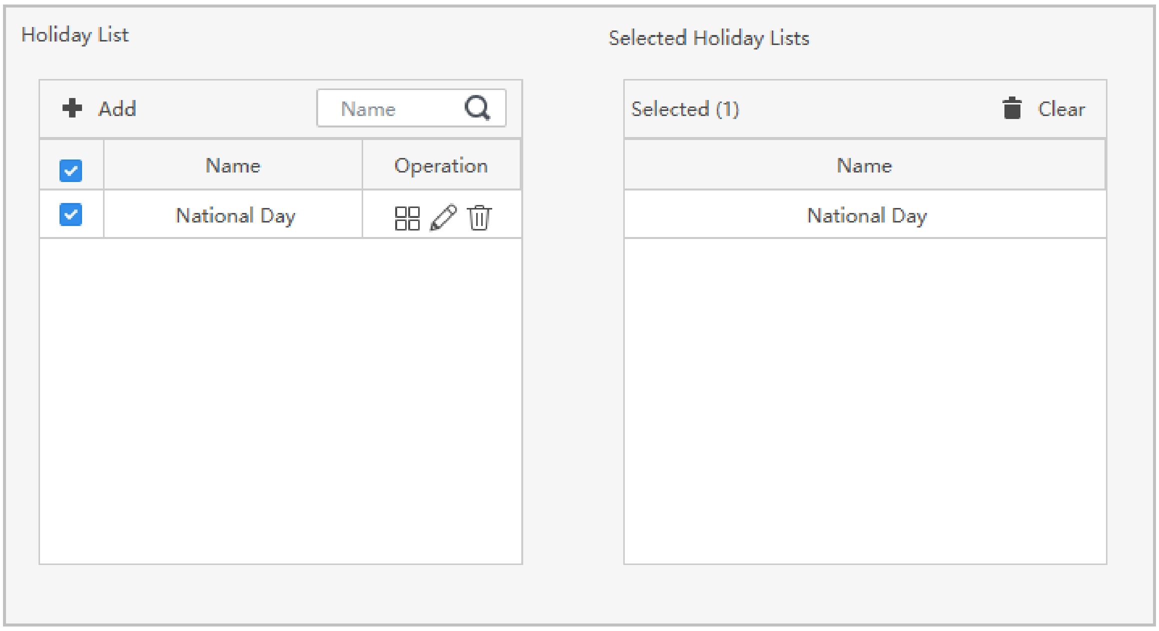
You can only configure up to 4 time sections for each day.

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.

Step 5 Select holidays, and then click **Apply**.

Figure 5-3 Select holidays



☑	Name	Operation
☑	National Day	

Name
National Day

6 Advanced Functions Configuration

6.1 Configuring First Card Unlock

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

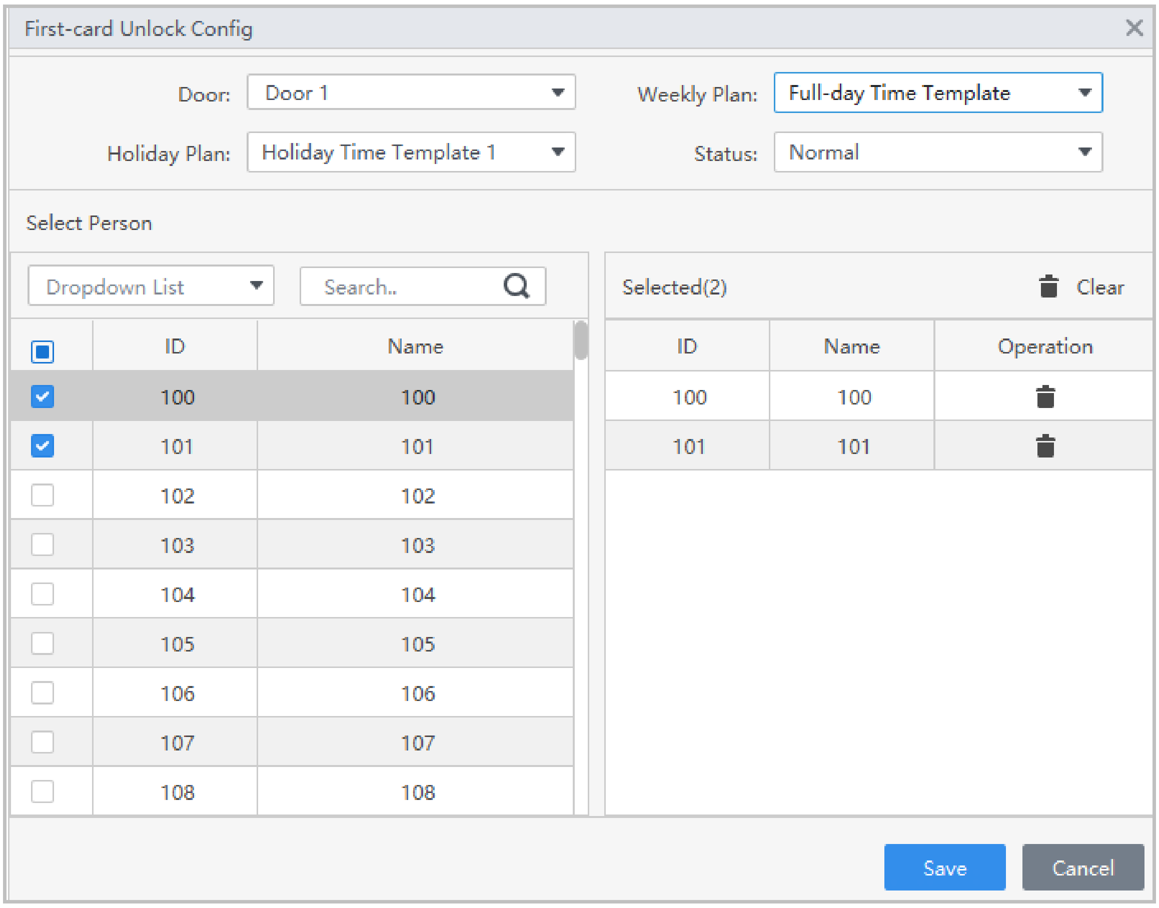
Procedure

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

Step 2 Click **Add**.

Step 3 Select a door channel.

Figure 6-1 Add first-card holders



First-card Unlock Config

Door: Door 1

Weekly Plan: Full-day Time Template

Holiday Plan: Holiday Time Template 1

Status: Normal

Select Person

■	ID	Name
☑	100	100
☑	101	101
□	102	102
□	103	103
□	104	104
□	105	105
□	106	106
□	107	107
□	108	108

Selected(2)

ID	Name	Operation
100	100	🗑
101	101	🗑

Step 4 Select the weekly plan and the holiday plan.

First-card is valid only during the defined time.

Step 5 Select the door status.

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

Step 6 Select first-card users, and then click **Save**.

6.2 Configuring Multi-card 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

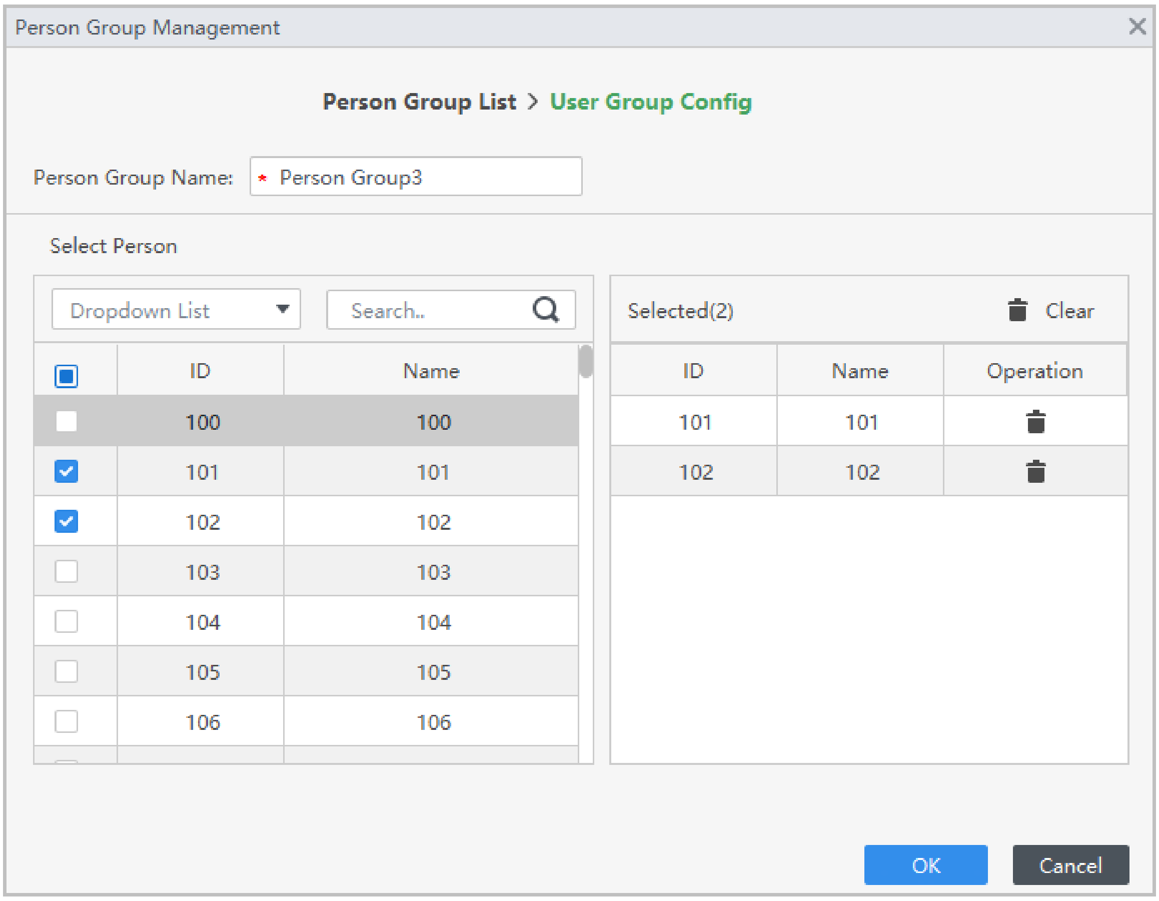
Step 1 Select **Access Control Config** > **Multi-card Unlock**.

Step 2 Click **Add** to add doors to the device list.

Step 3 Click **Person Group** , 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 6-2 Add groups



Person Group Management

Person Group List > User Group Config

Person Group Name: * Person Group3

Select Person

☑	ID	Name
□	100	100
☑	101	101
☑	102	102
□	103	103
□	104	104
□	105	105
□	106	106

Selected(2)

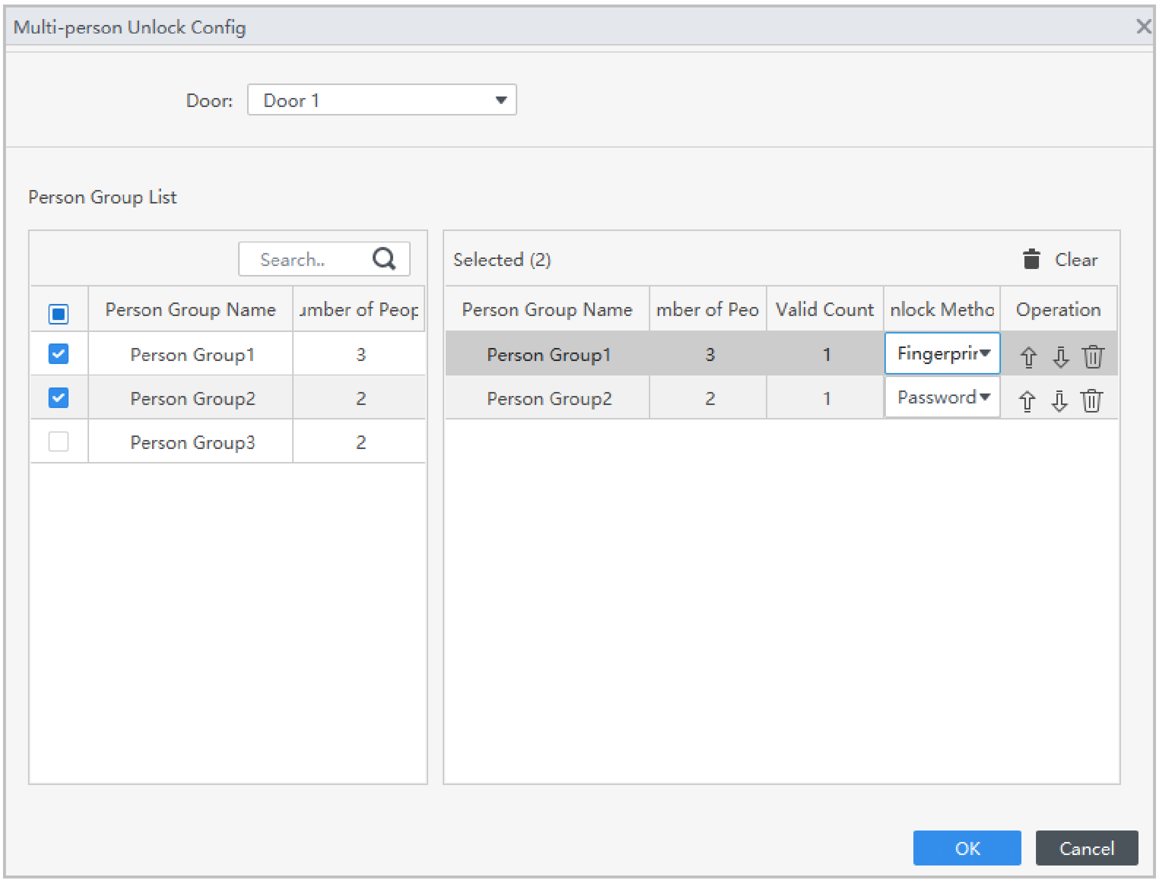
ID	Name	Operation
101	101	🗑
102	102	🗑

Step 4 Click + Add, and the select a door.

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.

Figure 6-3 Configure multi-person unlock



Multi-person Unlock Config

Door: Door 1

Person Group List

Search..

☑	Person Group Name	umber of Peop
☑	Person Group1	3
☑	Person Group2	2
□	Person Group3	2

Selected (2) Clear

Person Group Name	mber of Peo	Valid Count	nlock Metho	Operation
Person Group1	3	1	Fingerprir	⇧ ⇩ 🗑
Person Group2	2	1	Password	⇧ ⇩ 🗑

Step 6 Configure the parameters of multi- unlock.

1. Enter the valid count.

   The valid count 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 count 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 ⇧ or ⇩ to change the sequence of groups.

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

Step 7 Click **OK**.

6.3 Anti-passback

6.3.1 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 they attempt to enter again, and access is denied at the same time.

Procedure

Step 1 Select **Access Control Config** > **Anti-pass back**.

Step 2 Click **Anti-pass Back** tab, and then click **Add**.

Step 3 Select an access control device, and then enter a name for the anti-passback group.

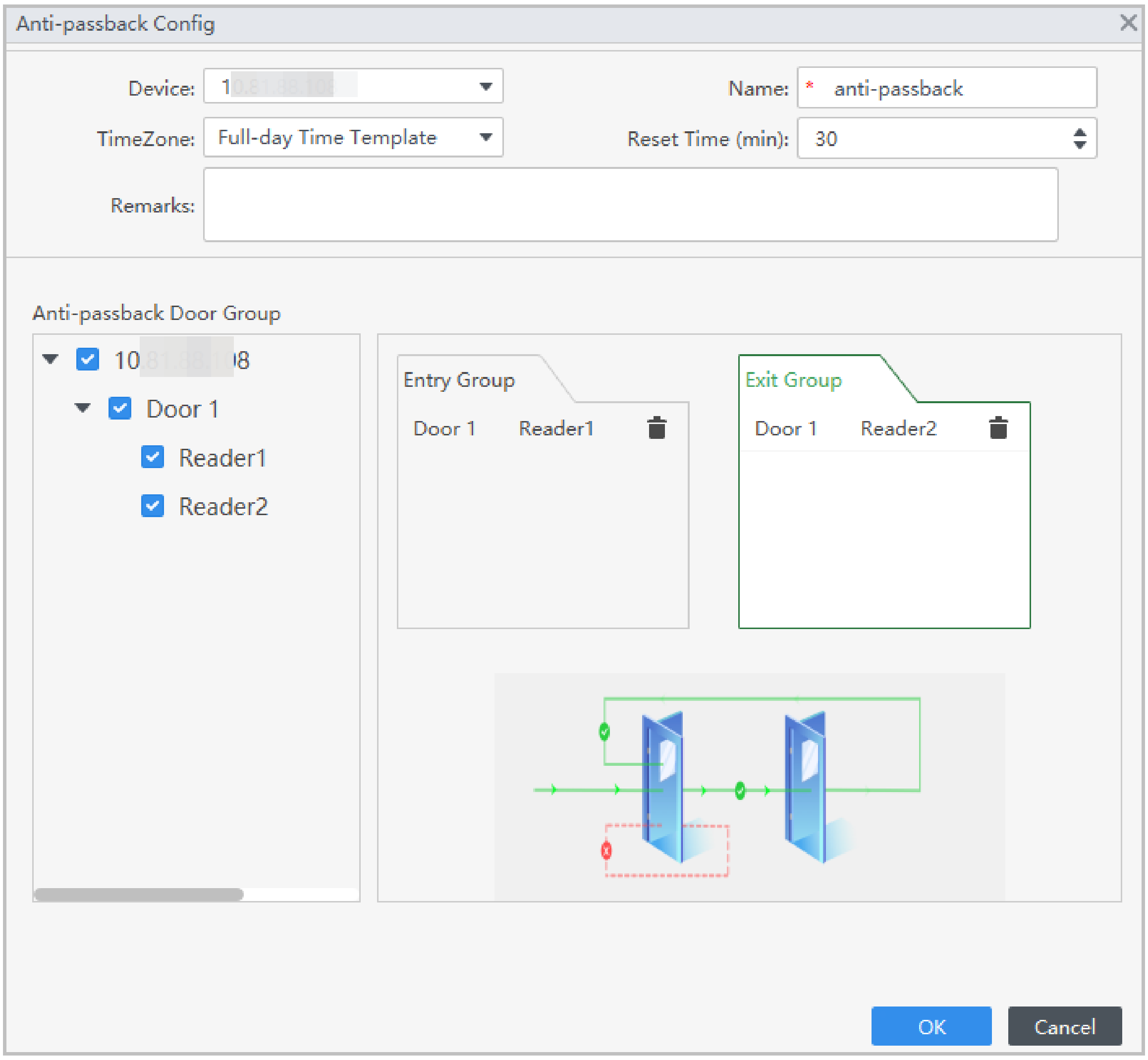
Step 4 Select a timezone.

Anti-passback is effective during the defined time.

Step 5 Enter the reset time.

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

Figure 6-4 Configure anti-passback



Anti-passback Config

Device: 1[redacted]

Name: * anti-passback

TimeZone: Full-day Time Template

Reset Time (min): 30

Remarks:

Anti-passback Door Group

- ☑ 10[redacted]8
  - ☑ Door 1
    - ☑ Reader1
    - ☑ Reader2

Entry Group

Door 1	Reader1

Exit Group

Door 1	Reader2

Step 6 Select the entry group, and then select card readers.

Step 7 Select the exit group, and then select card readers.

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

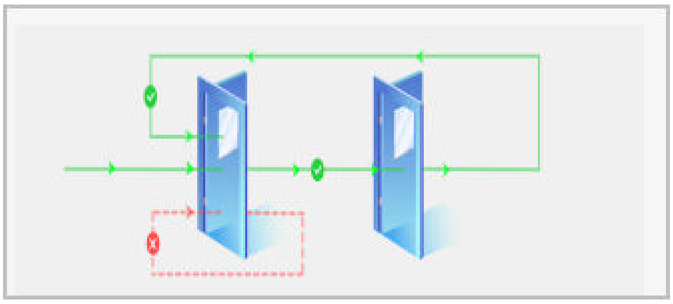
You can add more than one readers in a group, and users can swipe at any one of the readers to gain access.

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 entry group 1, and then at a reader in exit group 2. As long as you swipe card following the established sequence, the system works fine.

Figure 6-5 Anti-passback function



6.3.2 Configuring Global Anti-passback

Users need to verify their identities on devices following the established sequence, otherwise an anti-passback alarm will be triggered.

Procedure

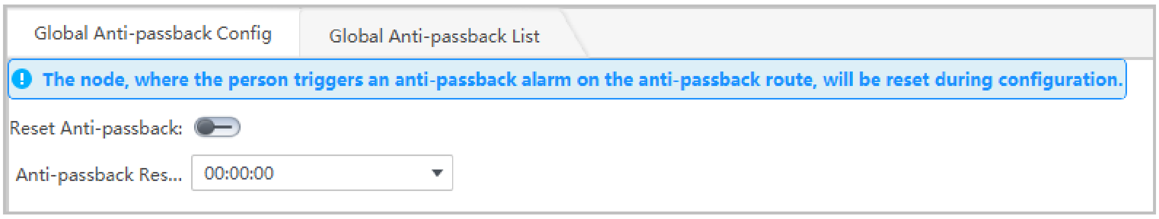
Step 1 Select **Access Control Config** > **Anti-pass Back**.

Step 2 Click **Global Anti-passback** tab, and then click **Global Anti-passback Config**.

Step 3 Enable reset Anti-passback function, and enter the reset time.

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

Figure 6-6 Reset anti-passback



Global Anti-passback Config | Global Anti-passback List

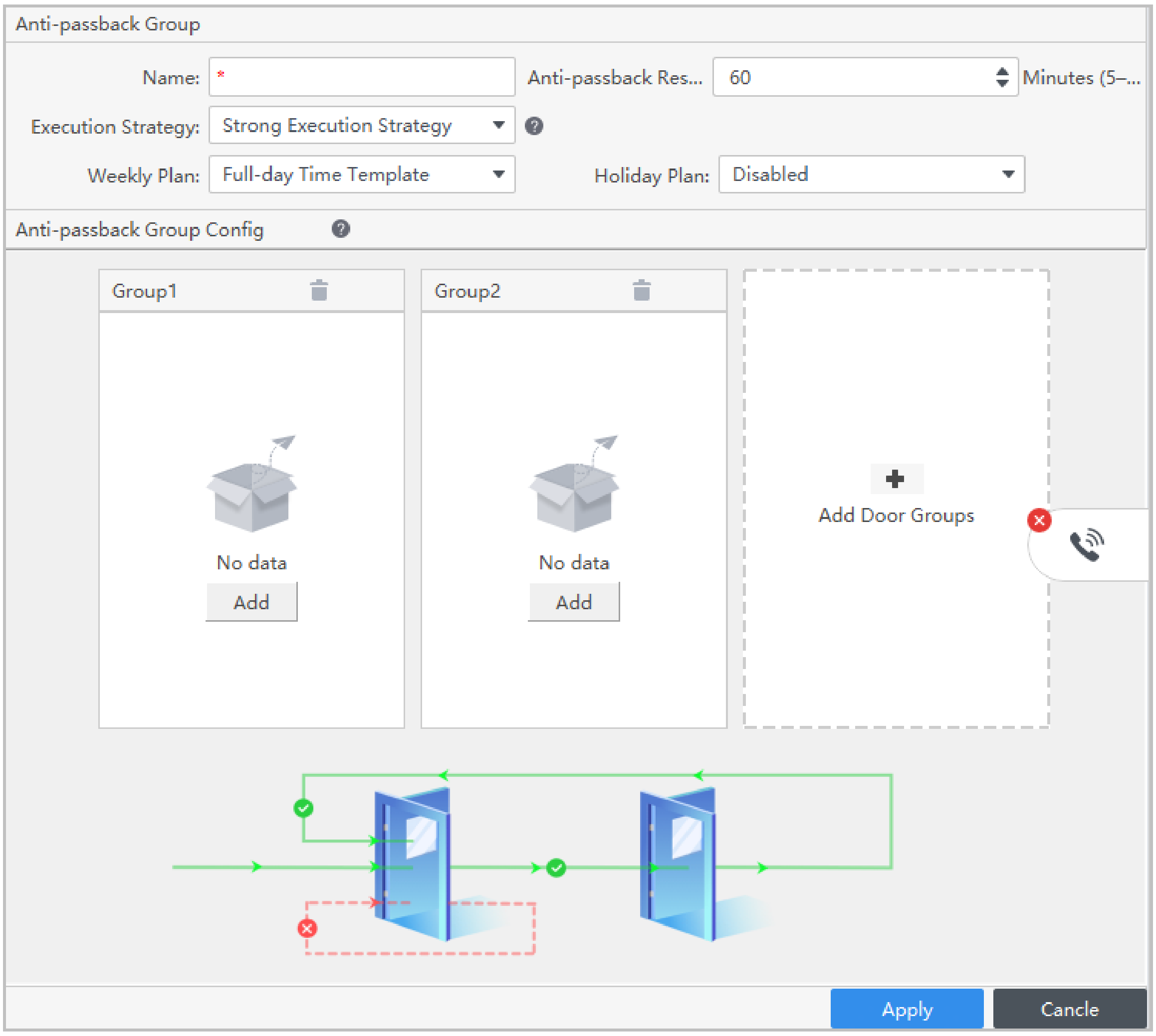
The node, where the person triggers an anti-passback alarm on the anti-passback route, will be reset during configuration.

Reset Anti-passback:

Anti-passback Res... 00:00:00

Step 4 Click **Global Anti-passback List** , and then click **Add**.

Figure 6-7 Configure anti-passback



Anti-passback Group

Name: *

Anti-passback Res... 60 Minutes (5–...

Execution Strategy: Strong Execution Strategy

Weekly Plan: Full-day Time Template

Holiday Plan: Disabled

Anti-passback Group Config

Step 5 Enter the name, and set the reset time.

Specify a time when the anti-passback status of all personnel will be reset. For example, if the reset time is set to 30 minutes, when an anti-passback alarm is triggered, the user need to wait 30 minutes before they can swipe to open the door.

Step 6 Select the execution mode.

- Strong execution: The device perform the anti-passback function even when they go offline.
- Weak execution: The device do not perform the anti-passback function when they go offline.

Step 7 Select the weekly plan and holiday plan.

Anti-passback is effective during the defined time.

Step 8 In group 1, click **Add**, and then select card readers.

Step 9 In group 2, click **Add**, and then select card readers.

At least 2 groups must be added.

Step 10 (Optional) You can click **Add Door Groups** to add more groups.

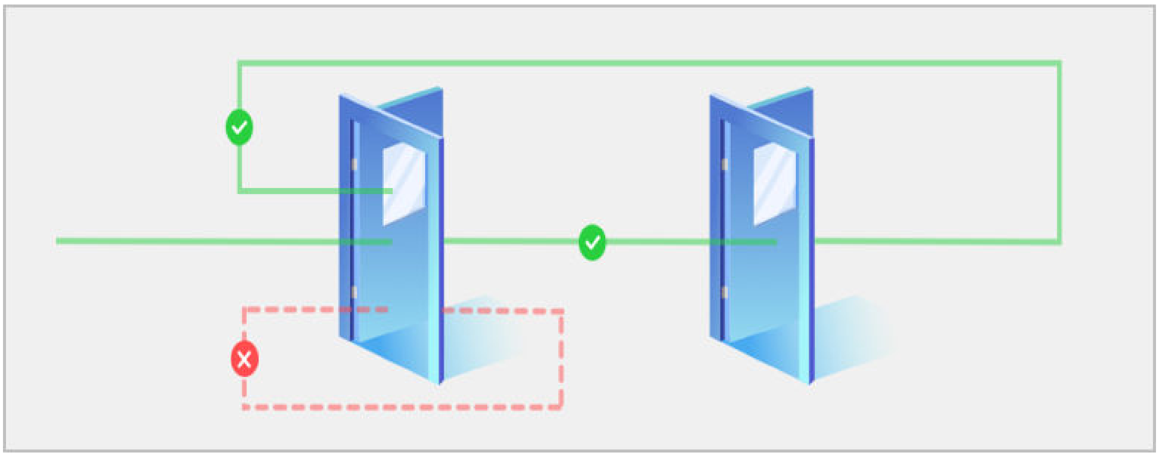
You can add more than one readers in a group, and users can swipe at any one of the readers to gain access.

Step 11 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 6-8 Anti-passback function



6.4 Configuring Interlock between Groups

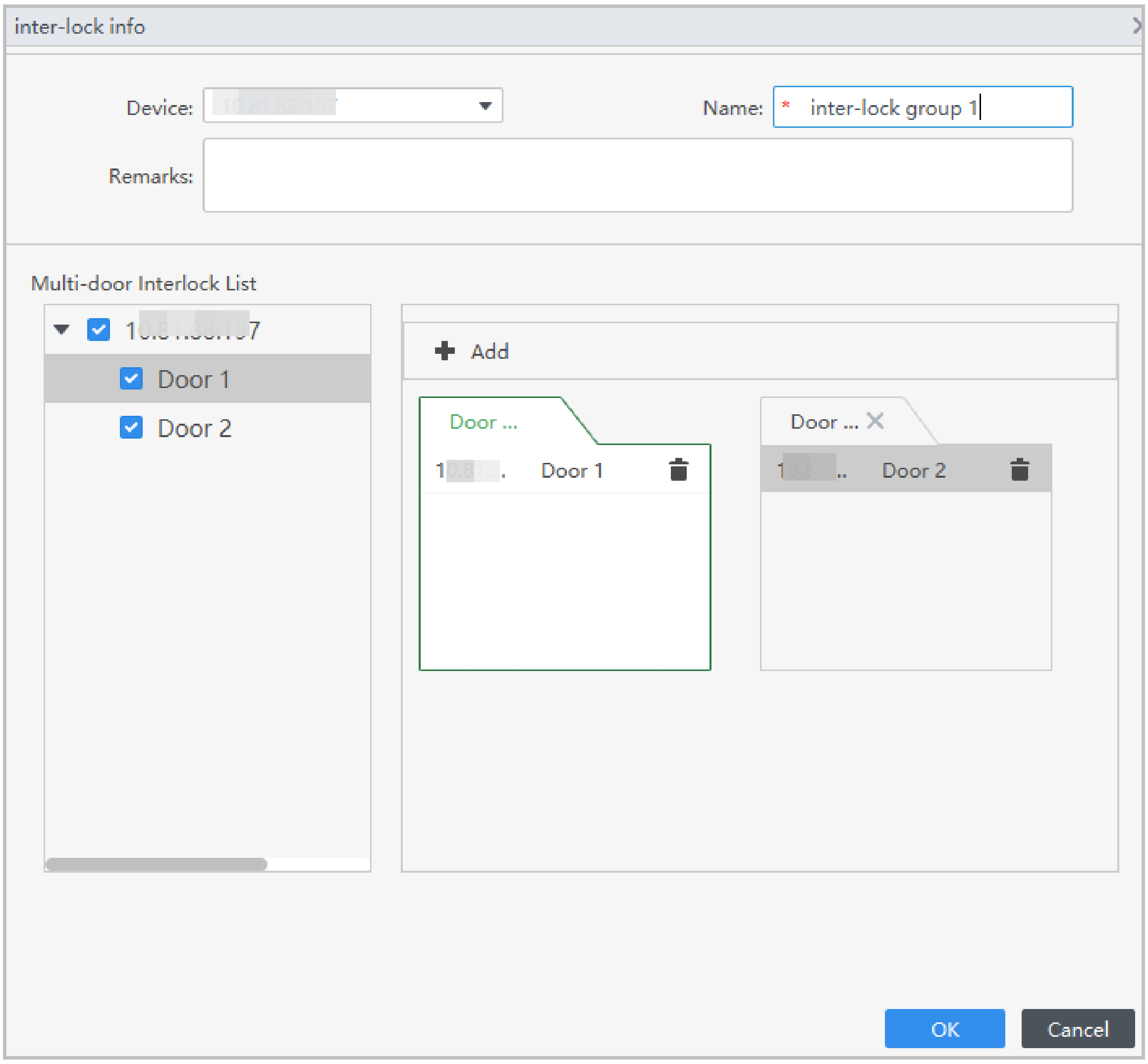
If any doors in a group is unlocked, the doors in the other groups cannot open.

Procedure

Step 1 Select **Access Control Config** > **Inter Door Lock**.

Step 2 Click **Add**, and then add an interlock group.

Figure 6-9 Interlock between groups



inter-lock info

Device: [redacted]

Name: * inter-lock group 1

Remarks:

Multi-door Interlock List

☑ [redacted]

☑ Door 1

☑ Door 2

Step 3 Select a access control device, and then enter a name for the inter-lock group.

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.

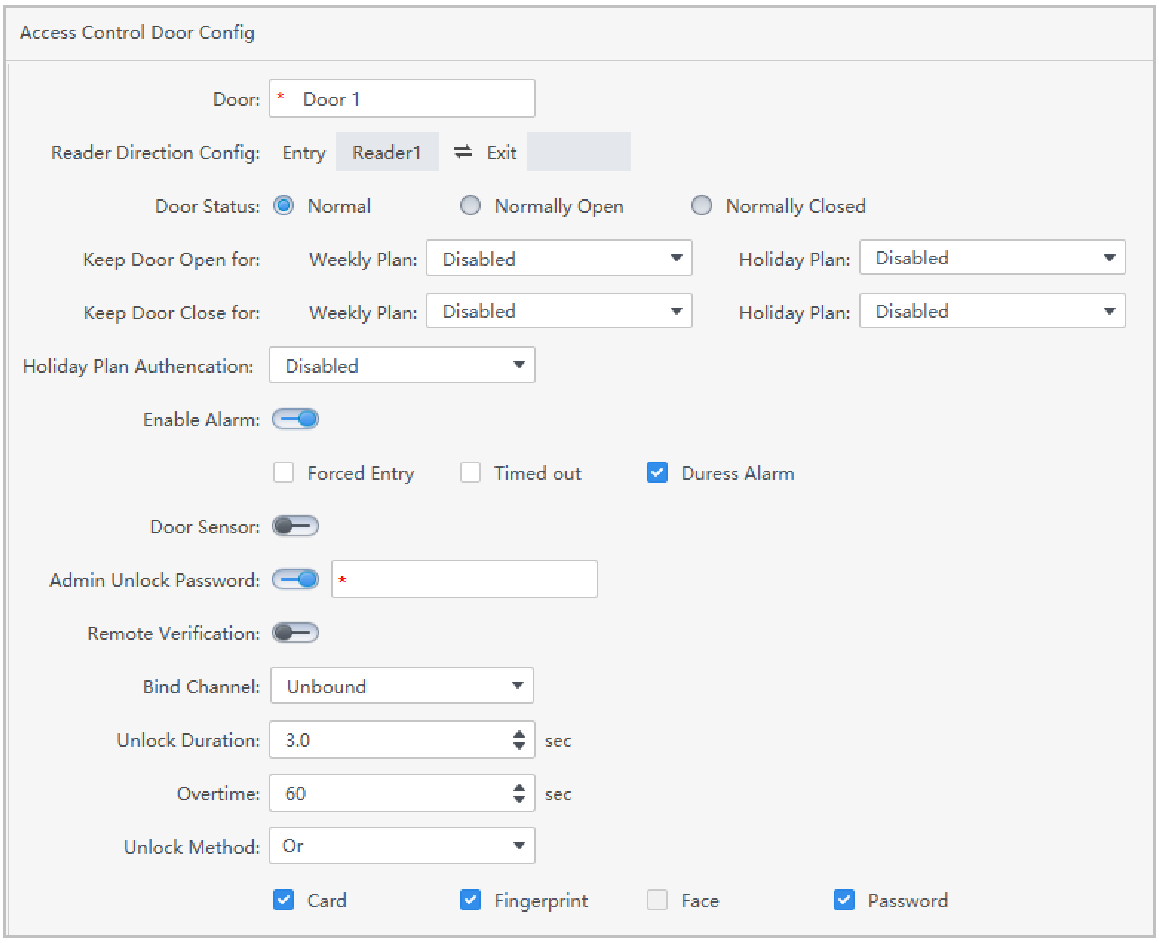
7 Configuring Door Parameters

Procedure

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

Step 2 Configure basic parameters for the access control.

Figure 7-1 Basic parameters



Access Control Door Config

Door: * Door 1

Reader Direction Config: Entry Reader1 ⇌ Exit

Door Status: ● Normal ○ Normally Open ○ Normally Closed

Keep Door Open for: Weekly Plan: Disabled Holiday Plan: Disabled

Keep Door Close for: Weekly Plan: Disabled Holiday Plan: Disabled

Holiday Plan Authencation: Disabled

Enable Alarm: On

□ Forced Entry □ Timed out ☑ Duress Alarm

Door Sensor: Off

Admin Unlock Password: On *

Remote Verification: Off

Bind Channel: Unbound

Unlock Duration: 3.0 sec

Overtime: 60 sec

Unlock Method: Or

☑ Card ☑ Fingerprint □ Face ☑ Password

Table 7-1 Basic parameters description

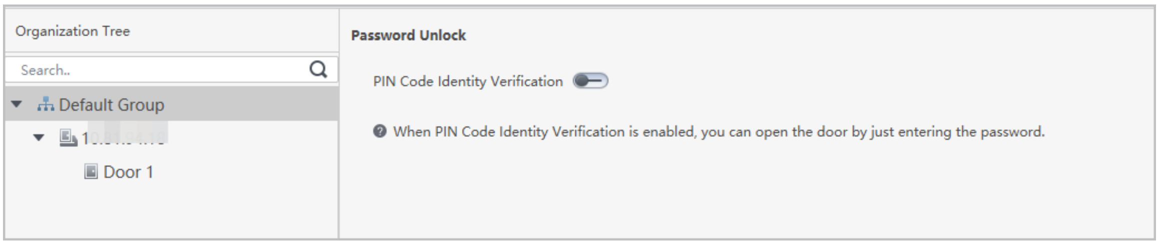
Parameter	Description
Name	The name of the door.
Reader Direction	Click ⇌ to set the reader to a "in" card reader or a "out" card reader.
Door Status	Set the door status. ● **Normal** : The door unlocks only after valid identity verification. ● **Always Open** : The door remains unlocked all the time. ● **Always Closed** : The door remains locked all the time.
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.

Parameter	Description
Holiday Plan Authentication	The door status is **Normal** in holiday when this function is enabled. The priority is as follows: keep door open for holiday plan > keep door closed for holiday plan > holiday plan authentication > keep door open for week plan > keep door closed for week plan.
Enable Alarm	● Forced Entry: When the door detector is enabled, an intrusion alarm will be triggered if the door is opened abnormally. ● Timed out: A timeout alarm is triggered when the door remains unlocked for longer than the defined value. ● Duress: An alarm will be triggered when a duress card, duress password or duress fingerprint is used to unlock the door.
Door Sensor	When door detector is enabled, an intrusion alarm will be triggered if the door is opened abnormally.
Admin Unlock Password	You can unlock the door by simply entering the Admin unlock password.
Remote Verification	The administrator needs to grant access on the platform after personnel verify their identities on the device, and then the door will open.
Bind Channel	Select a video channel, and then you can view the live video that is associated with the door.
Door 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 Method	Supports unlocking through card, fingerprint, face or password.

Related Operations

Pin code identity verification: When this function is enabled, people can unlock the door by simply entering the password.

Figure 7-2 Pin code identity verification



Organization Tree

Search..

Default Group

1[redacted]

Door 1

Password Unlock

PIN Code Identity Verification

When PIN Code Identity Verification is enabled, you can open the door by just entering the password.

8 Viewing Access Control Records

History door events include those occur on the SmartPSS Lite client and door devices. Before viewing events, extract history events on the door devices to ensure that all events are searched.

Procedure

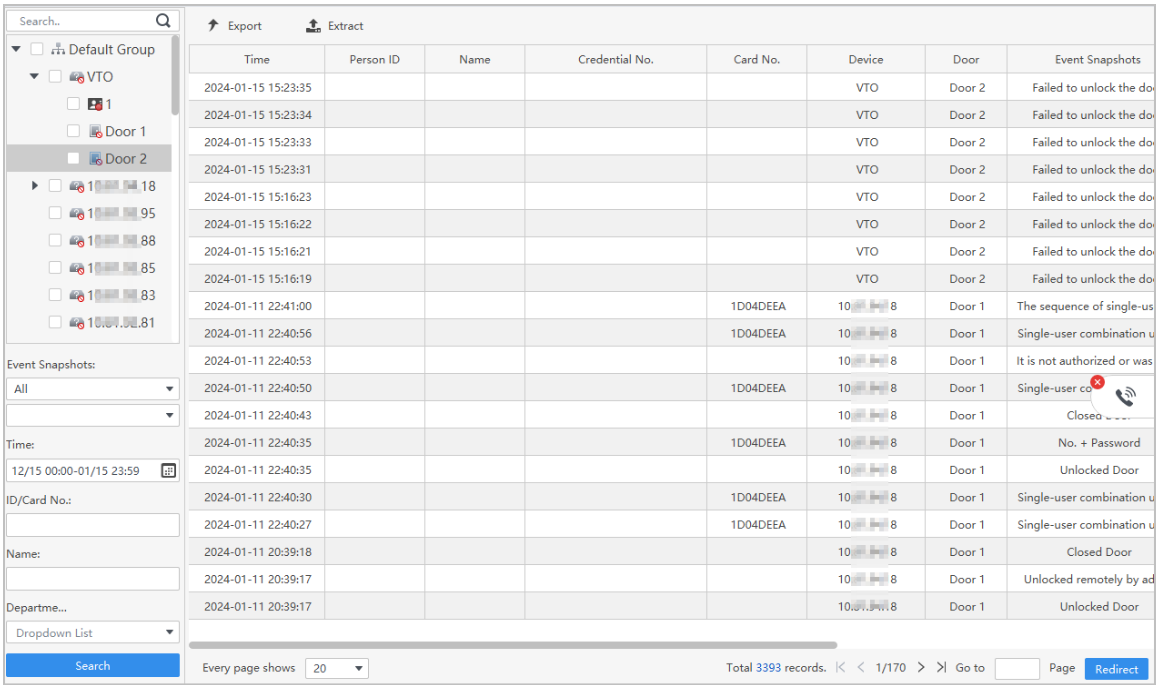
Step 1 Click **Access Control Record** on the home page.

Step 2 Click **Extract** , set the time, select the access control device, and then click **Extract Now**.

Access control events on the devices will be extracted to the platform.

- You can select multiple devices at one time to extract events.
- If the time zone of the computer supports DST (Daylight Saving time), the access event reported to the platform will be 1 hour behind the device UTC (Universal Time Coordinated) time.

Figure 8-1 Extract events



Event Snapshots: All

Time: 12/15 00:00-01/15 23:59

ID/Card No.:

Name:

Departme...: Dropdown List

Time	Person ID	Name	Credential No.	Card No.	Device	Door	Event Snapshots
2024-01-15 15:23:35					VTO	Door 2	Failed to unlock the do
2024-01-15 15:23:34					VTO	Door 2	Failed to unlock the do
2024-01-15 15:23:33					VTO	Door 2	Failed to unlock the do
2024-01-15 15:23:31					VTO	Door 2	Failed to unlock the do
2024-01-15 15:16:23					VTO	Door 2	Failed to unlock the do
2024-01-15 15:16:22					VTO	Door 2	Failed to unlock the do
2024-01-15 15:16:21					VTO	Door 2	Failed to unlock the do
2024-01-15 15:16:19					VTO	Door 2	Failed to unlock the do
2024-01-11 22:41:00				1D04DEEA	10[redacted]8	Door 1	The sequence of single-us
2024-01-11 22:40:56				1D04DEEA	10[redacted]8	Door 1	Single-user combination u
2024-01-11 22:40:53					10[redacted]8	Door 1	It is not authorized or was
2024-01-11 22:40:50				1D04DEEA	10[redacted]8	Door 1	Single-user co
2024-01-11 22:40:43					10[redacted]8	Door 1	Closed
2024-01-11 22:40:35				1D04DEEA	10[redacted]8	Door 1	No. + Password
2024-01-11 22:40:35					10[redacted]8	Door 1	Unlocked Door
2024-01-11 22:40:30				1D04DEEA	10[redacted]8	Door 1	Single-user combination u
2024-01-11 22:40:27				1D04DEEA	10[redacted]8	Door 1	Single-user combination u
2024-01-11 20:39:18					10[redacted]8	Door 1	Closed Door
2024-01-11 20:39:17					10[redacted]8	Door 1	Unlocked remotely by ad
2024-01-11 20:39:17					10[redacted]8	Door 1	Unlocked Door

Every page shows 20

Total 3393 records. 1/170 Go to Page

Step 3 Select a device, and set filter conditions, and then click **Search**.

Step 4 (Optional) Click **Export**, and then save it to your computer.

9 Access Control Monitoring

Procedure

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

Step 2 Manage the door.

Figure 9-1 Monitor the door

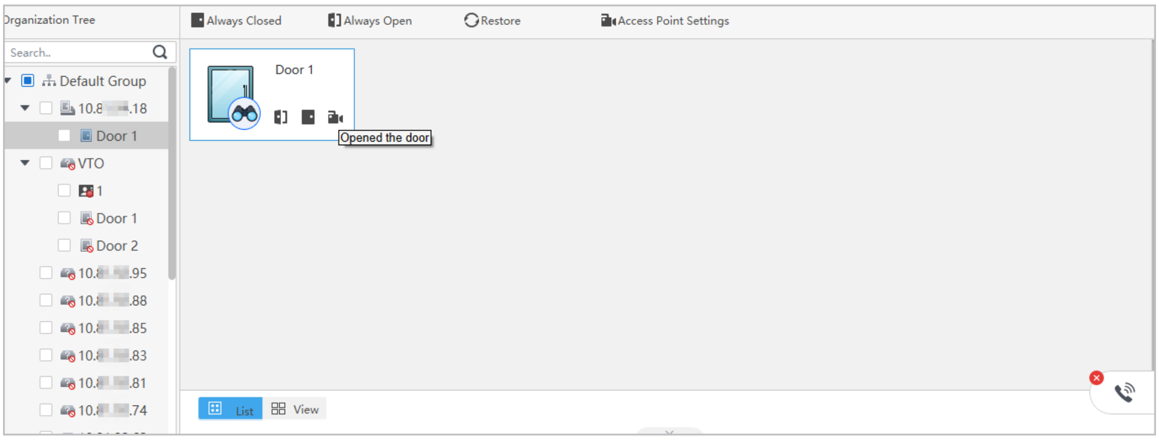


Table 9-1 Parameters description

Function	Description
Remotely control the door	Remotely control the door. ● Method 1: Right-click a door, and then select **Open** or **Close**. ● Method 2: Click ◨ or ■ to open or close the door.
🎥	View the video captured by the camera of the access controller or the linked external camera. If you cannot view real-time video, it means that the access control device has no camera and is not connected to an external camera. Please configure an external camera for access controller. For details, see "7 Configuring Door Parameters". If you want to view multiple live videos at the same time, click ⊞ View, and then drag the access control device in the organization tree to windows, or double-click the access control device in the organization tree.
Always Open	After setting always open or always closed, the door is open or closed all the time and cannot be controlled manually. If you want to manually control the door again, click **Normal** to reset the door status.
Always Closed	
Restore	
Access Point Settings	Set devices (NVR, IPC, IVSS and more) that support target recognition as the access control point. After setting, the door unlock records will be uploaded to the platform.

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

Figure 9-2 Manage the device

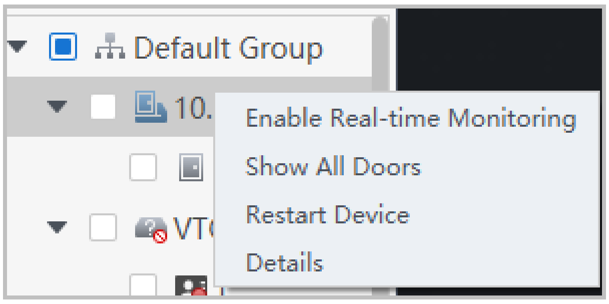


Table 9-2 Parameters description

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

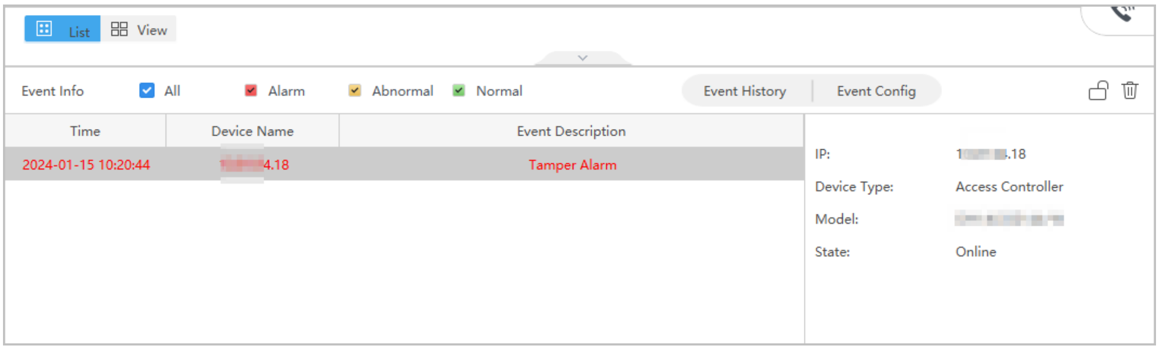
Step 4 View door status on **Event Info** list. For details, see "8 Viewing Access Control Records".

Related Operations

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

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

Figure 9-3 Event information



Event Info ☑ All ☑ Alarm ☑ Abnormal ☑ Normal

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

IP: 1[redacted].18

Device Type: Access Controller

Model: [redacted]

State: Online

Appendix 1 Cybersecurity Recommendations

The necessary measures to ensure the basic cyber security of the platform:

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. **Customize the Answer to the Security Question**

   The security question setting should ensure the difference of answers, choose different questions and customize different answers (all questions are prohibited from being set to the same answer) to reduce the risk of security question being guessed or cracked.

Recommendation measures to enhance platform cyber security:

1. **Enable Account Binding IP/MAC**

   It is recommended to enable the account binding IP/MAC mechanism, and configure the IP/MAC of the terminal where the commonly used client is located as an allowlist to further improve access security.
2. **Change Passwords Regularly**

   We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.
3. **Turn On Account Lock Mechanism**

   The account lock function is enabled by default at the factory, and it is recommended to keep it on to protect the security of your account. After the attacker has failed multiple password attempts, the corresponding account and source IP will be locked.
4. **Reasonable Allocation of Accounts and Permissions**

   According to business and management needs, reasonably add new users, and reasonably allocate a minimum set of permissions for them.
5. **Close Non-essential Services and Restrict the Open Form of Essential Services**

   If not needed, it is recommended to turn off NetBIOS (port 137, 138, 139), SMB (port 445), remote desktop (port 3389) and other services under Windows, and Telnet (port 23) and SSH (port 22) under Linux. At the same time, close the database port to the outside or only open to a specific IP address, such as MySQL (port 3306), to reduce the risks faced by the platform.
6. **Patch the Operating System/Third Party Components**

   It is recommended to regularly detect security vulnerabilities in the operating system and third-party components, and apply official patches in time.
7. **Security Audit**

   - Check online users: It is recommended to check online users irregularly to identify whether there are illegal users logging in.
   - View the platform log: By viewing the log, you can get the IP information of the attempt to log in to the platform and the key operation information of the logged-in user.
8. **The Establishment of a Secure Network Environment**

   In order to better protect the security of the platform and reduce cyber security risks, it is recommended that:

   - Follow the principle of minimization, restrict the ports that the platform maps externally by firewalls or routers, and only map ports that are necessary for services.

- Based on actual network requirements, separate networks: if there is no communication requirement between the two subnets, it is recommended to use VLAN, gatekeeper, etc. to divide the network to achieve the effect of network isolation.