SmartPSS Lite Video Intercom Solution

User's Manual

V1.0.3

Foreword

General

This manual introduces the functions and operations of the video intercom solution of the SmartPSS Lite (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
V1.0.3	Updated the person management and permission management.	January 2024
V1.0.2	● Updated the intercom configuration function. ● Updated the intercom management function.	April 2023
V1.0.1	● Updated personnel management function. ● Updated intercom configuration function.	December 2022
V1.0.0	First release.	August 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 Person Management

1.1 Adding Company

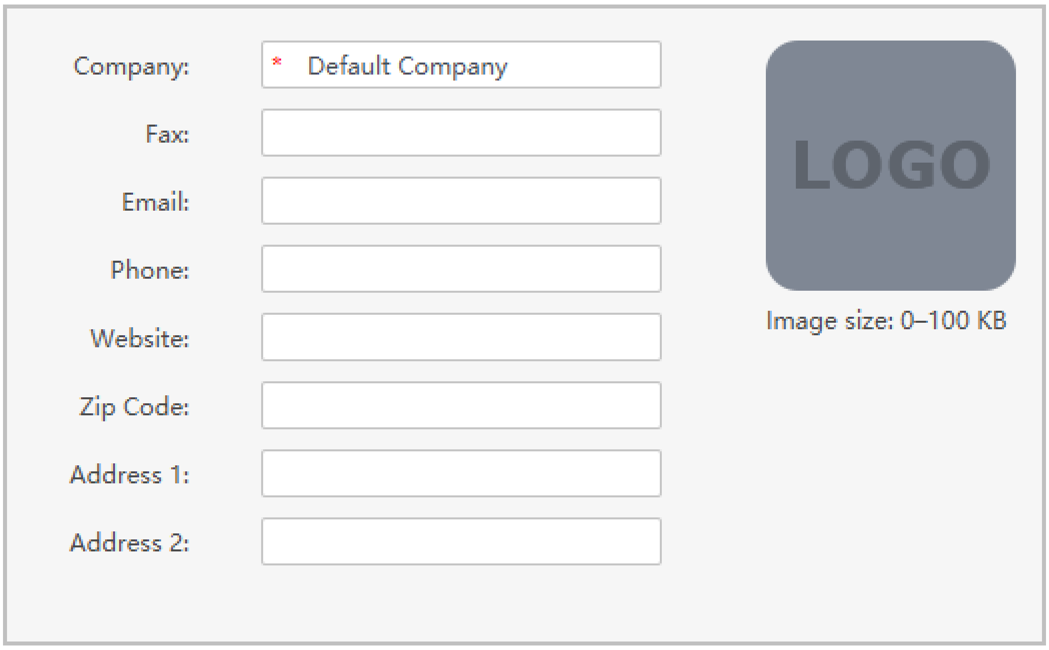
Procedure

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

Step 2 Configure the company information.

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

Figure 1-1 Add company



Company:	* Default Company
Fax:	
Email:	
Phone:	
Website:	
Zip Code:	
Address 1:	
Address 2:	

Image size: 0–100 KB

1.2 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.

1.2.1 Adding Departments

Procedure

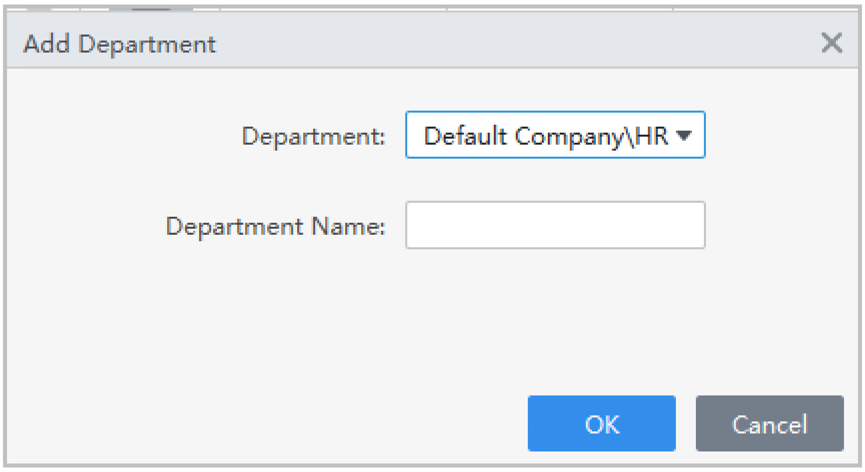
Step 1 Select **Person** > **Person Management**.

Step 2 In the department organization tree, click +.

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

Step 4 Click **OK**.

Figure 1-2 Add departments



Department: Default Company\HR

Department Name:

Related Operations

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

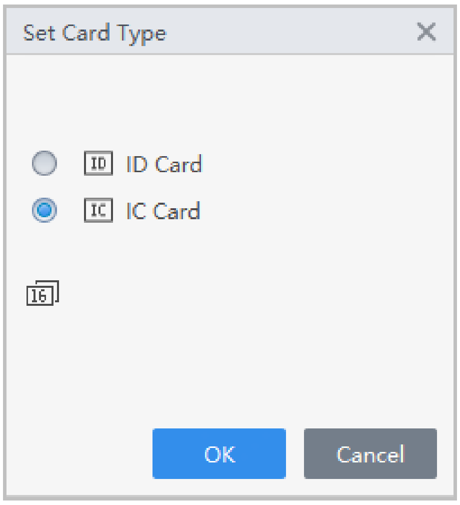
1.2.2 Setting Card Type

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 1-3 Set card type



○ ID Card

● IC Card

1.2.3 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.

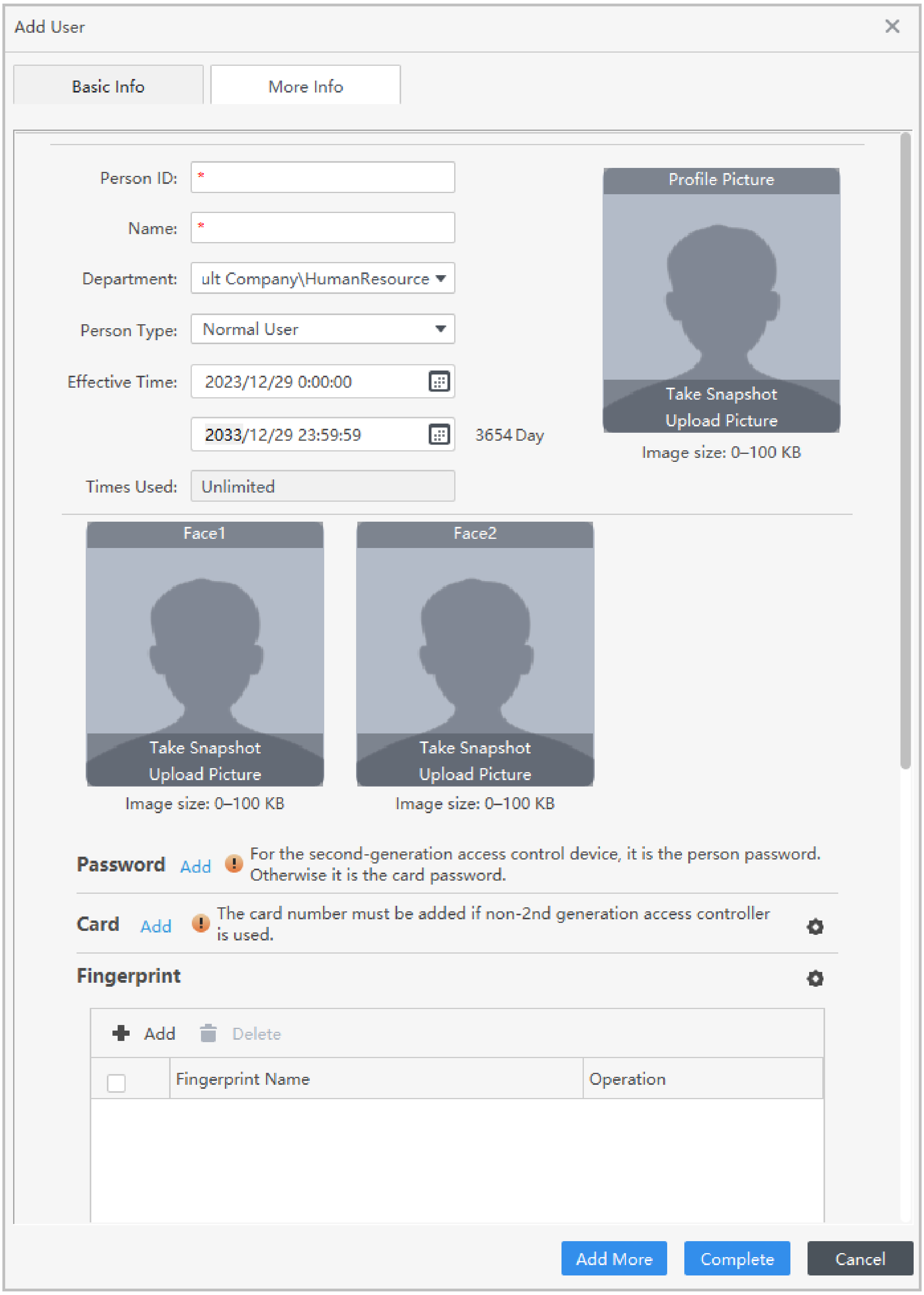
- Configure fingerprint

  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 1-4 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.

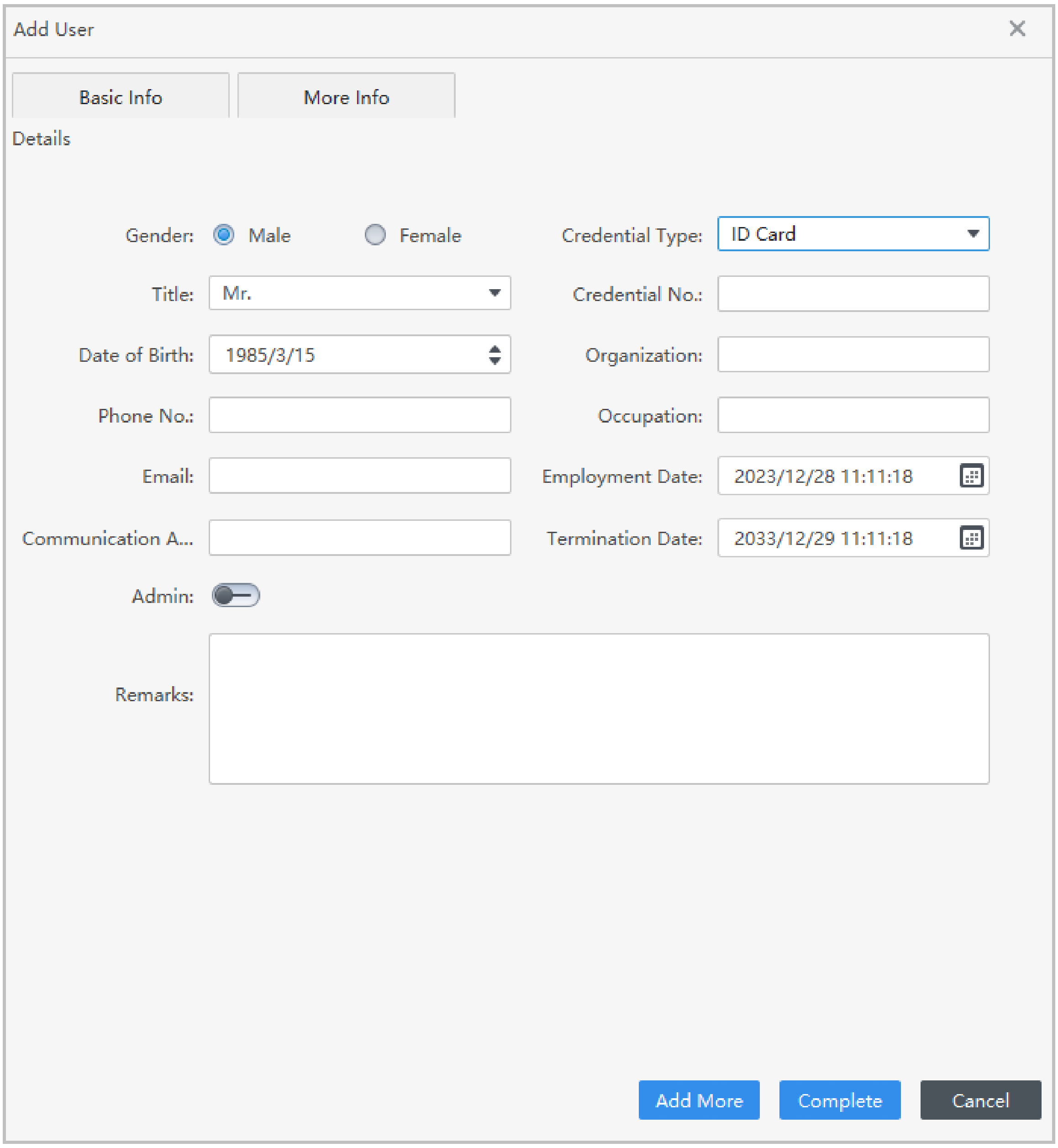
Card Add The card number must be added if non-2nd generation access controller is used.

Fingerprint

□	Fingerprint Name	Operation

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

Figure 1-5 Add more information



Details

Gender: ● Male ○ Female

Credential Type: ID Card

Title: Mr.

Credential No.:

Date of Birth: 1985/3/15

Organization:

Phone No.:

Occupation:

Email:

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

Communication A...:

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

Admin:

Remarks:

Step 4 Click **Complete**.

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

Related Operations

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

1.2.4 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.

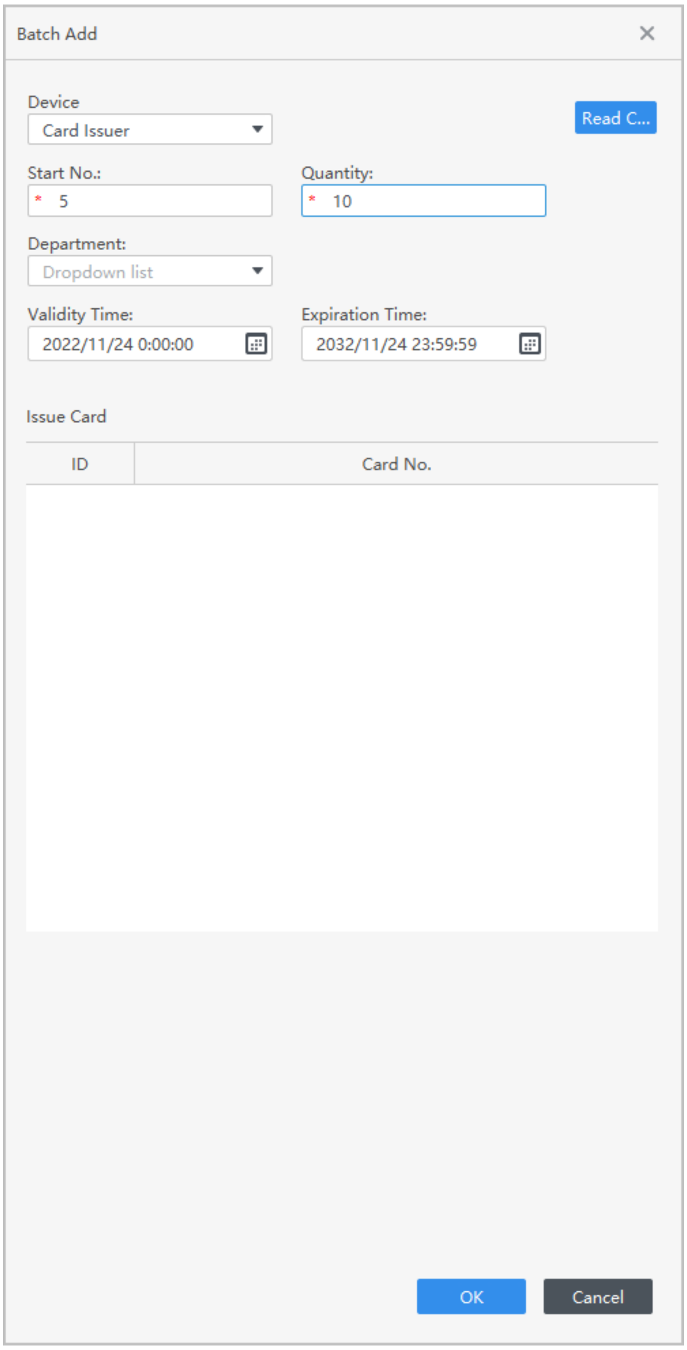
Step 4 Click **Read Card No.**.

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 1-6 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.

1.2.5 Other Operations

1.2.5.1 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**.

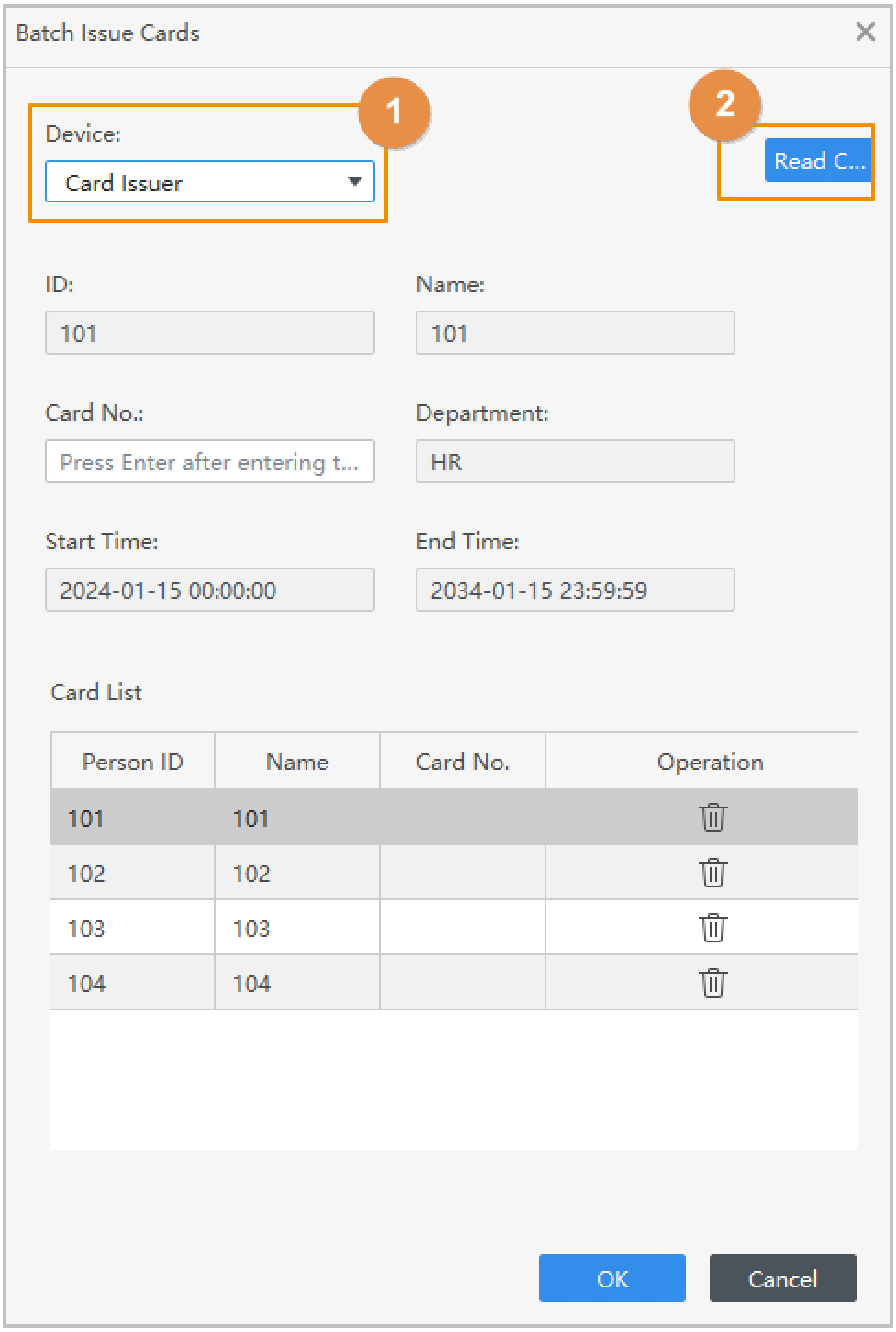
Step 2 Select personnel, and then select **Batch Update** > **Batch Issue Card** .

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 1-7 Read automatically



Batch Issue Cards

Device: Card Issuer

ID: 101

Name: 101

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

Department: HR

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

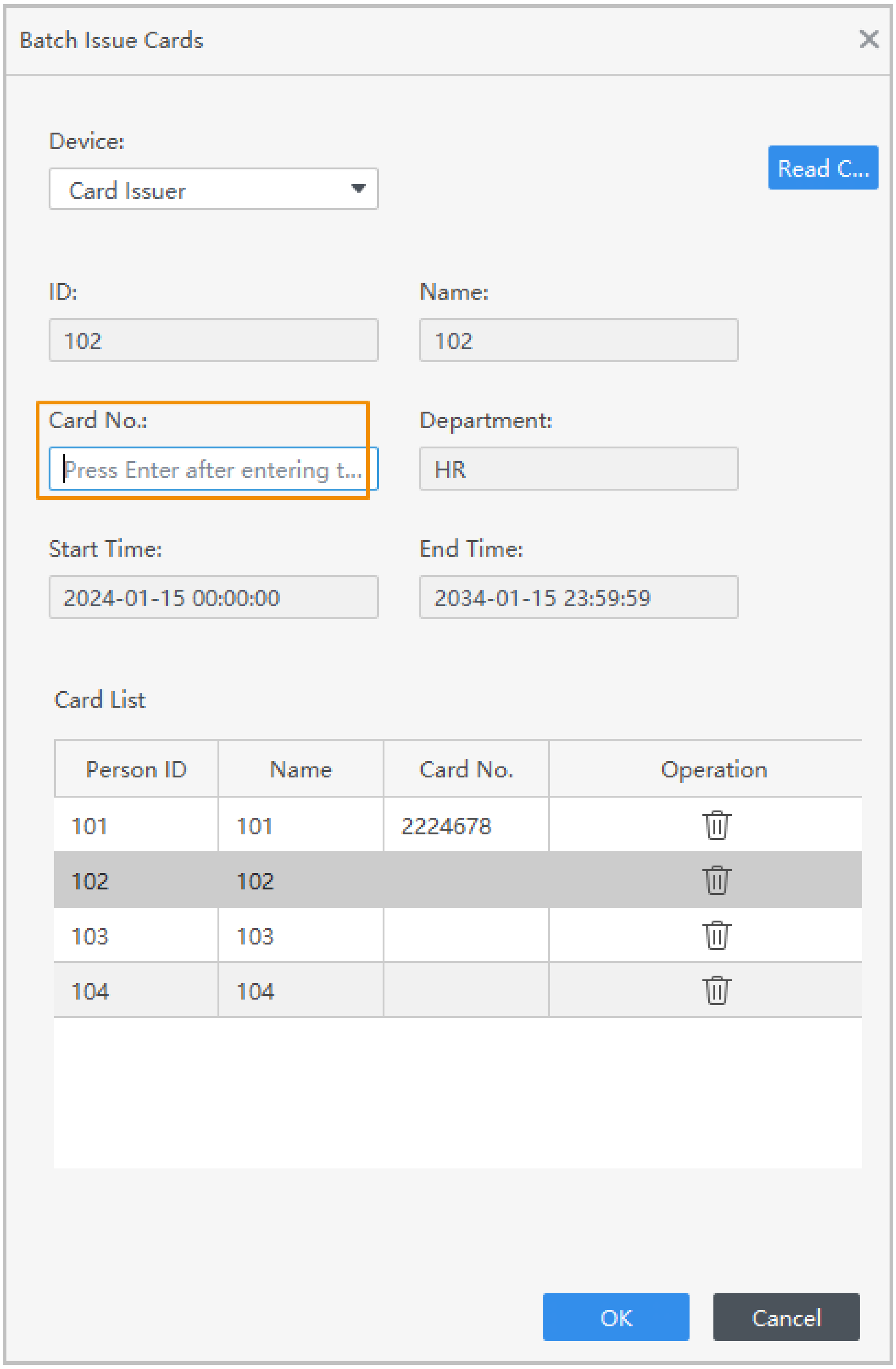
End Time: 2034-01-15 23:59:59

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 1-8 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**.

1.2.5.2 Extracting Personnel Information

Extract users from devices to the platform.

Procedure

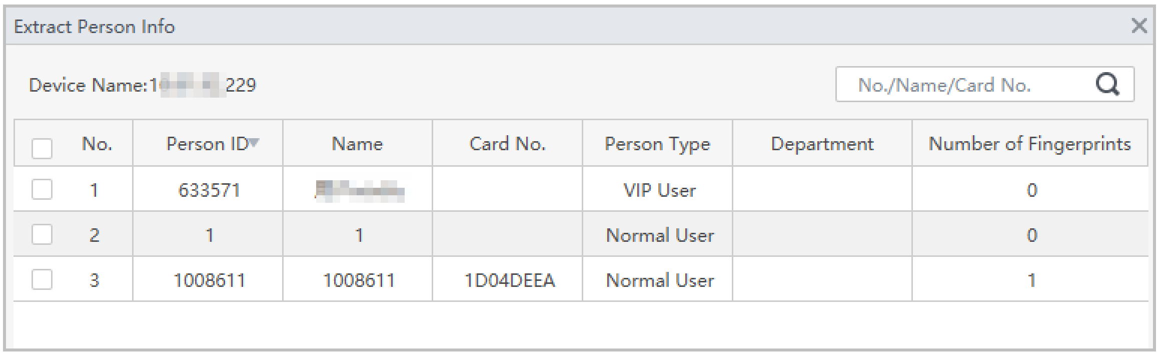
Step 1 Select **Person** > **Person Management**, and then click **Extract**

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 1-9 Extract users



Extract Person Info

Device Name:1[redacted]229

No./Name/Card No.

□ 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.

1.2.5.3 Importing Personnel Information

Import personnel information to the platform.

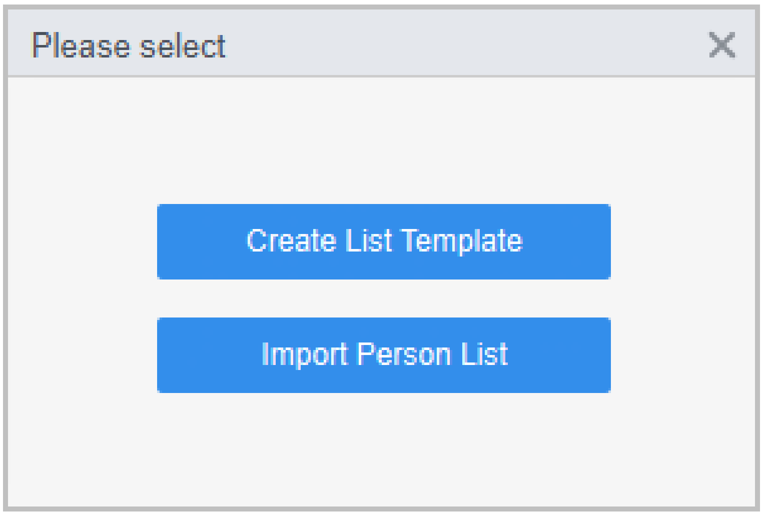
Procedure

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 1-10 Import staff information



1.2.5.4 Exporting Personnel Information

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

1.2.5.5 Searching for Personnel

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

Figure 1-11 Search for staff

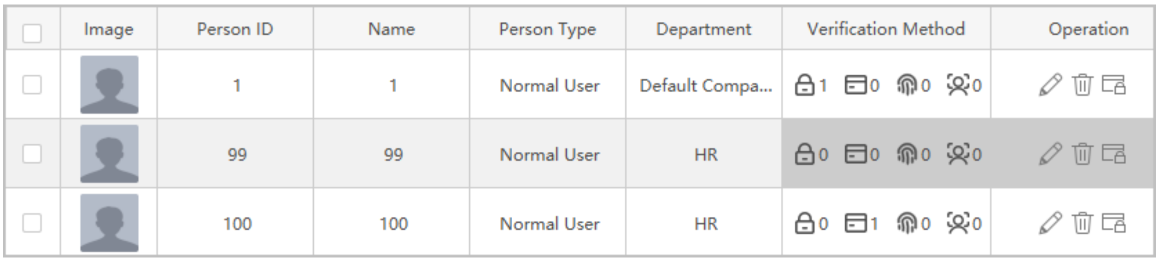
ID / Name / Card

1.2.5.6 Personnel Display

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

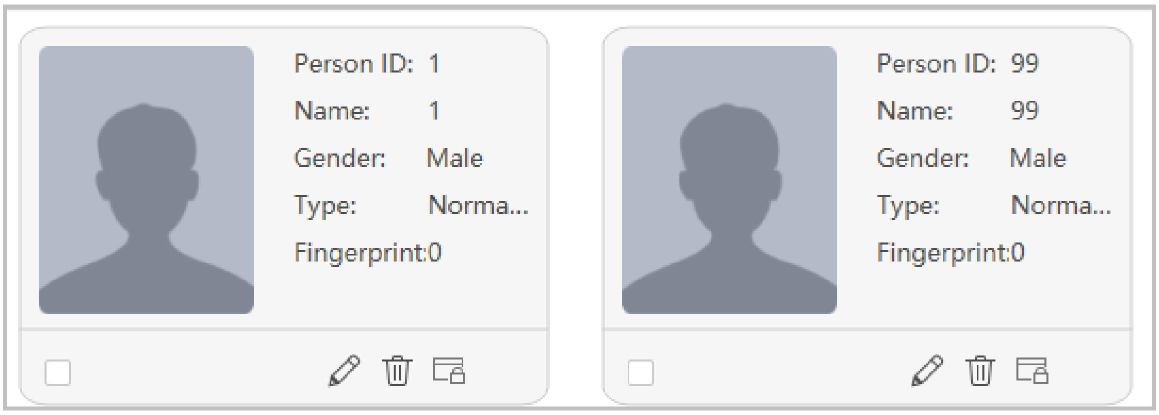
Click ⊞ to display in cards; click ☰ to display in list.

Figure 1-12 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 1-13 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
□ ✎ 🗑 ▭

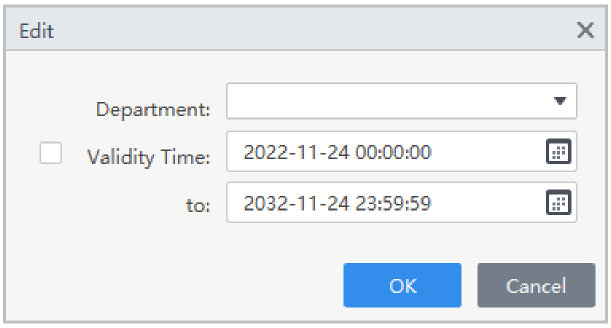
1.2.5.7 Editing Personnel in Batches

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 1-14 Edit department



Edit ✕

Department: ▾

□ Validity Time: 2022-11-24 00:00:00

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

1.3 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.

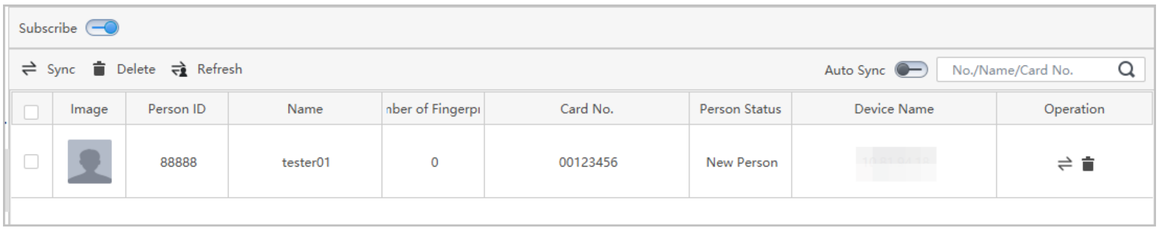
Procedure

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 1-15 Subscribe users

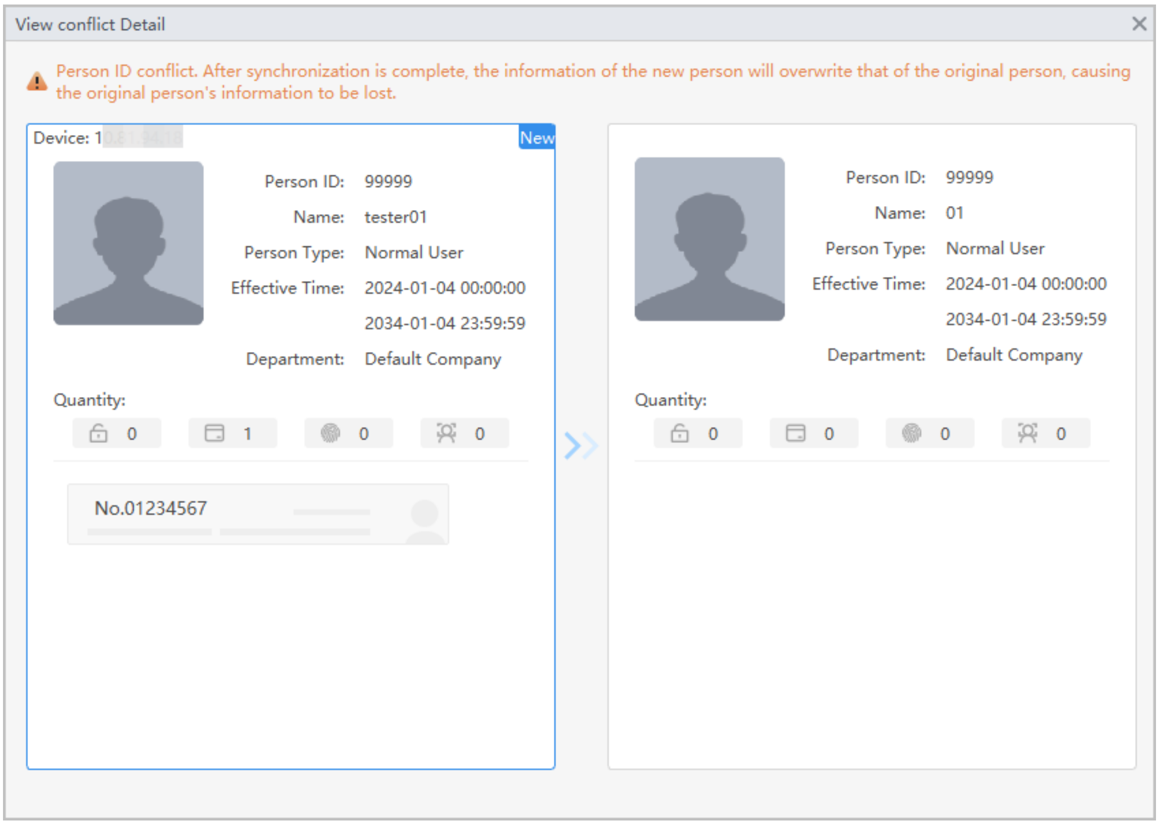


□	Image	Person ID	Name	nber of Fingerpı	Card No.	Person Status	Device Name	Operation
□		88888	tester01	0	00123456	New Person		⇌ 🗑

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 1-16 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

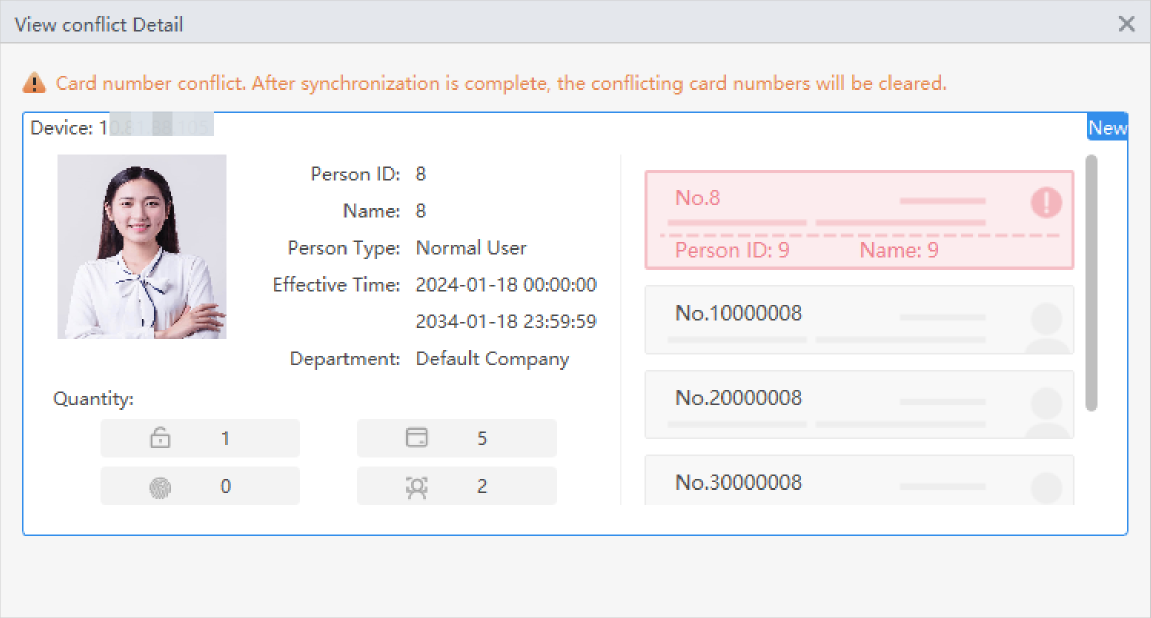
Person Type: Normal User

Effective Time: 2024-01-04 00:00:00
2034-01-04 23:59:59

Department: Default Company

Quantity: 0 0 0 0

Figure 1-17 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

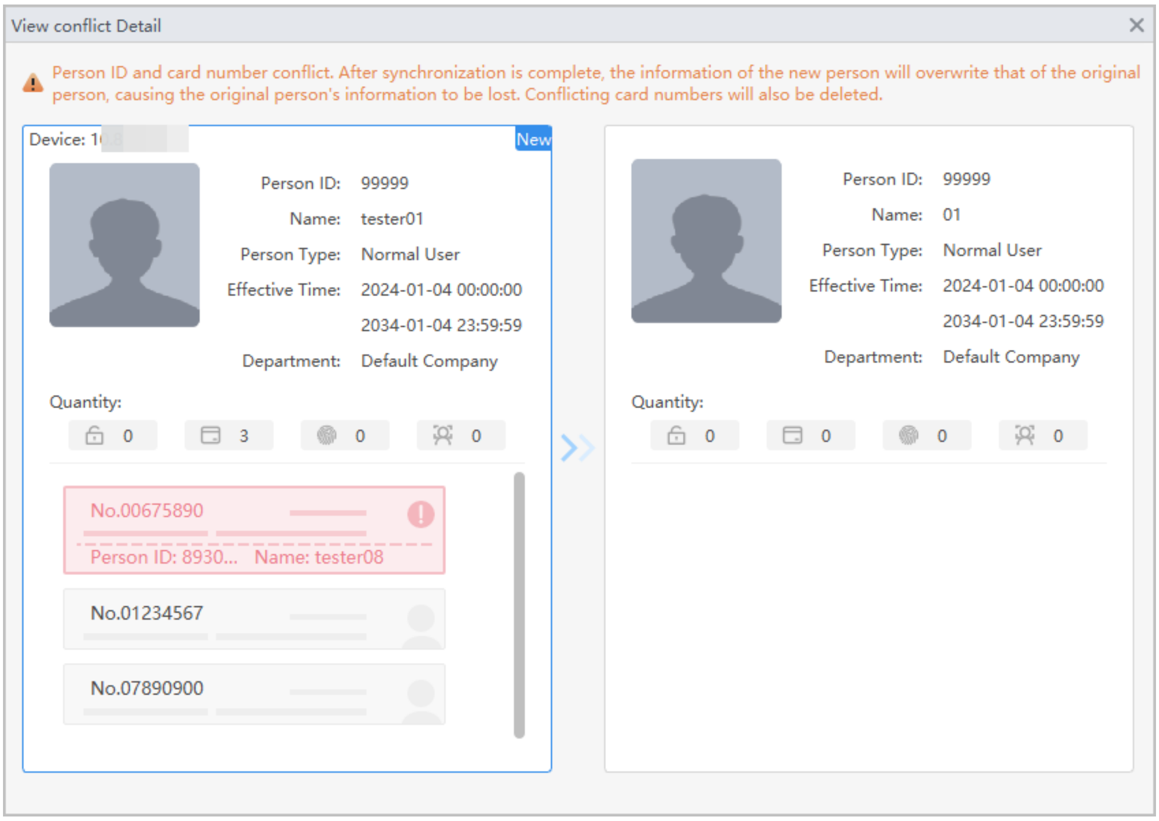
No.8
Person ID: 9 Name: 9

No.10000008

No.20000008

No.30000008

Figure 1-18 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.

2 Permission Configuration

2.1 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**.

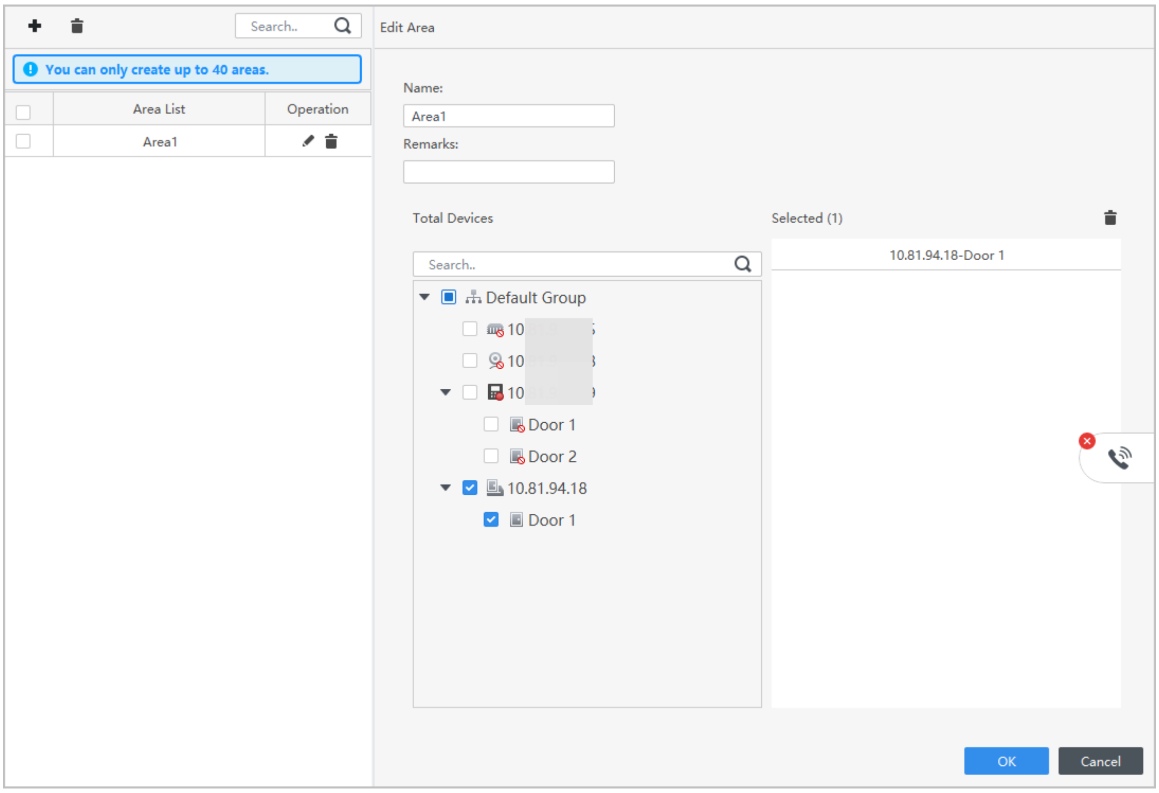
Step 2 Click ✚ to add a permission area.

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 2-1 Add permission area



You can only create up to 40 areas.

□	Area List	Operation
□	Area1	✎ 🗑

Edit Area

Name: Area1

Remarks:

Total Devices

- ☑ 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.

2.2 Assigning Permissions

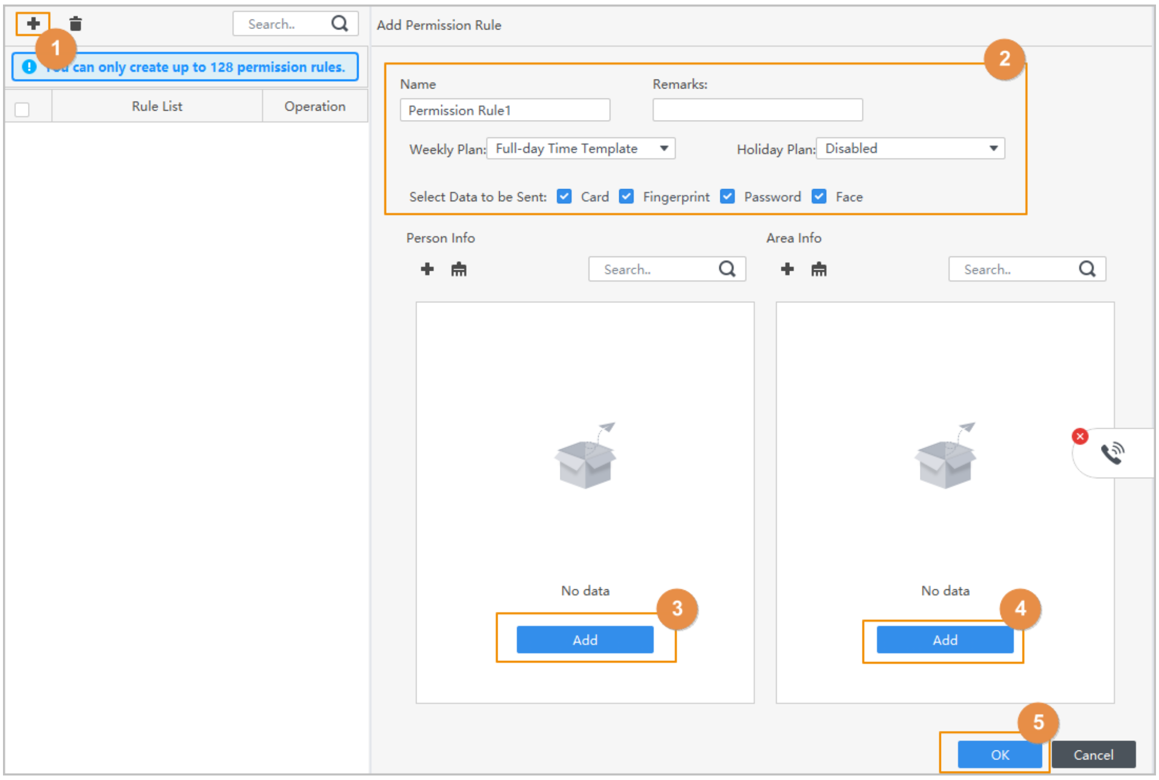
The method to configure permission for department and for personnel is similar, and here uses department as an example.

Procedure

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

Step 2 Click + to add a permission rule.

Figure 2-2 Assign permissions rules



You can only create up to 128 permission rules.

Name: Permission Rule1

Remarks:

Weekly Plan: Full-day Time Template

Holiday Plan: Disabled

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

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

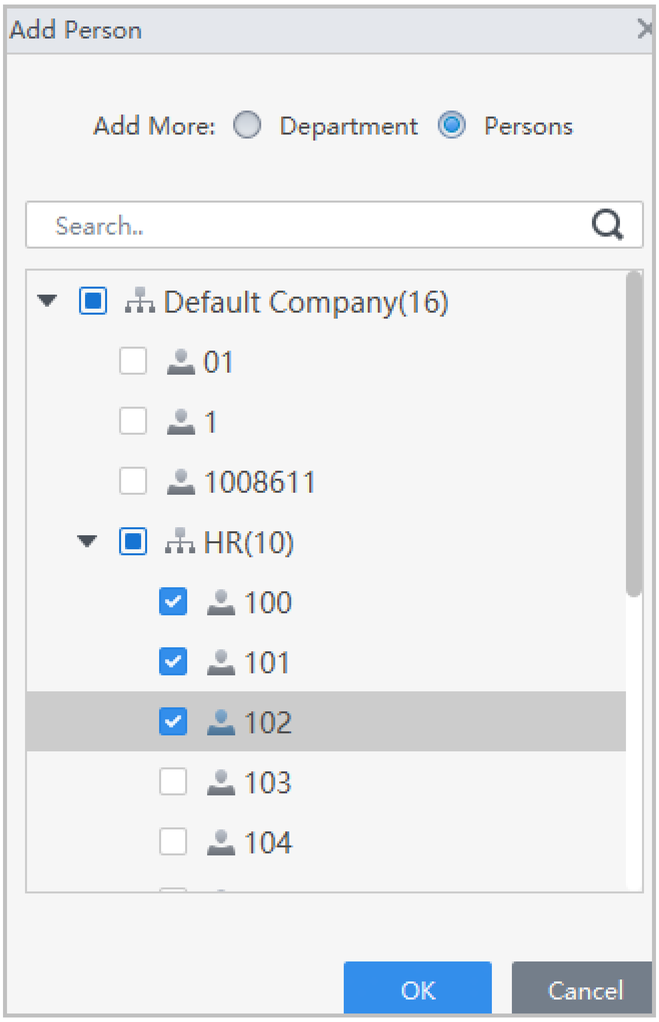
Step 4 In the **Person Info** area, click **Add** to select personnel, and then click **OK**.

You can select personnel on the department or individual users.

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

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

Figure 2-3 Add users



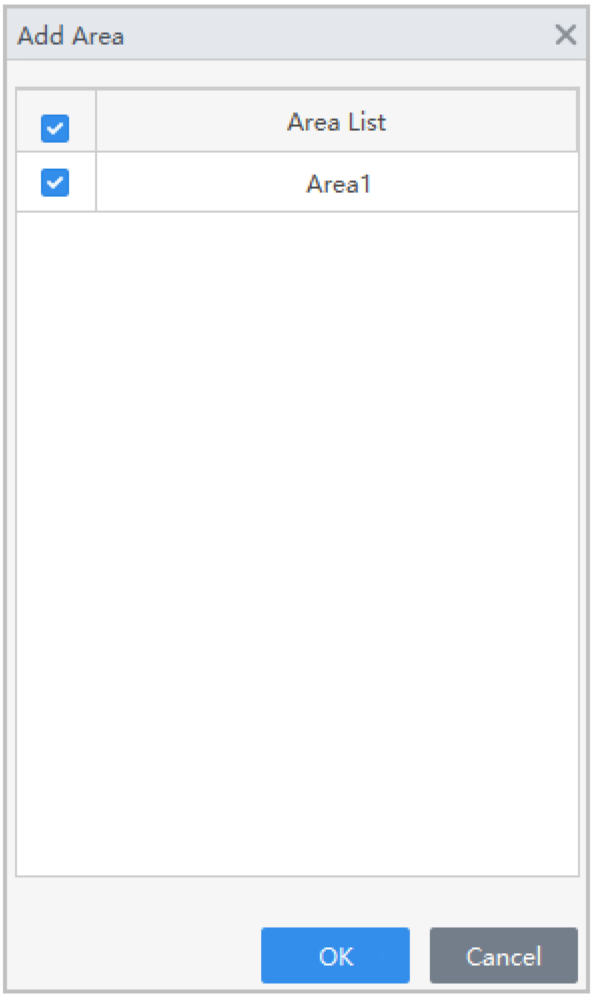
Add More: ○ Department ● Persons

- ■ 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 "2.1 Adding Permission Areas".

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

Figure 2-4 Add area

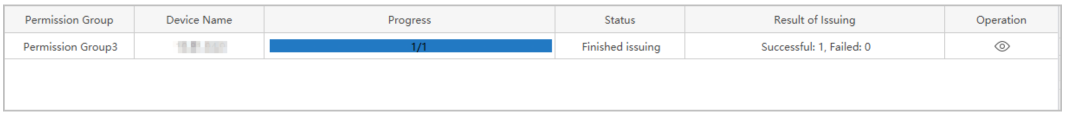

Add Area

☑	Area List
☑	Area1

Step 6 Click **OK**.

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

Figure 2-5 Authorization progress



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

2.3 Viewing Authorization Progress

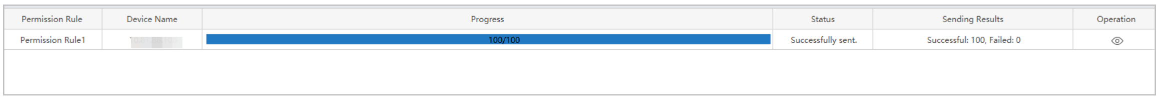
After you assign access permissions to users, you can view the authorization process.

Procedure

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

Step 2 View the authorization progress.

Figure 2-6 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.

3 Intercom Configuration

You can manage organizations and phone numbers, configure call settings and release information.

Click **Device Manager** on the home page, and then add video intercom devices to the Platform.

For details, see *SmartPSS Lite General User's Manual*. Select 👤 > **Help Manual** on the upper-right corner of the page to obtain the help manual.

3.1 Building Management

Create a compound organization. You can add buildings, units under it.

Prerequisites

This section uses how to create the organization at the unit level as an example.

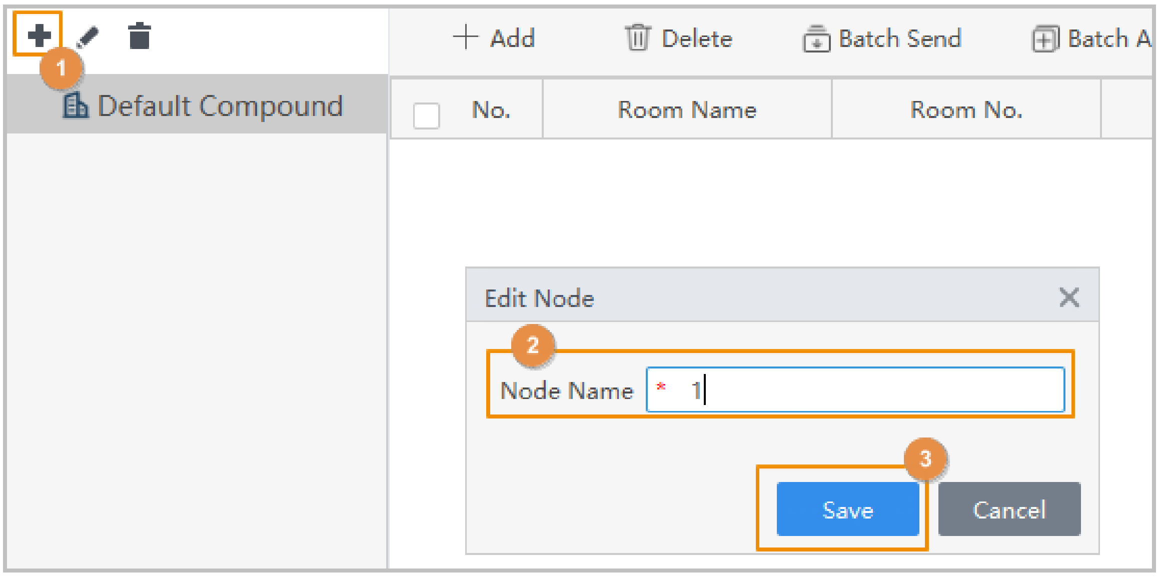
Procedure

Step 1 Select , **Intercom Config** > **Building Management**.

Step 2 Add buildings under the compound level.

You can click ✎ to edit the name of the default compound.

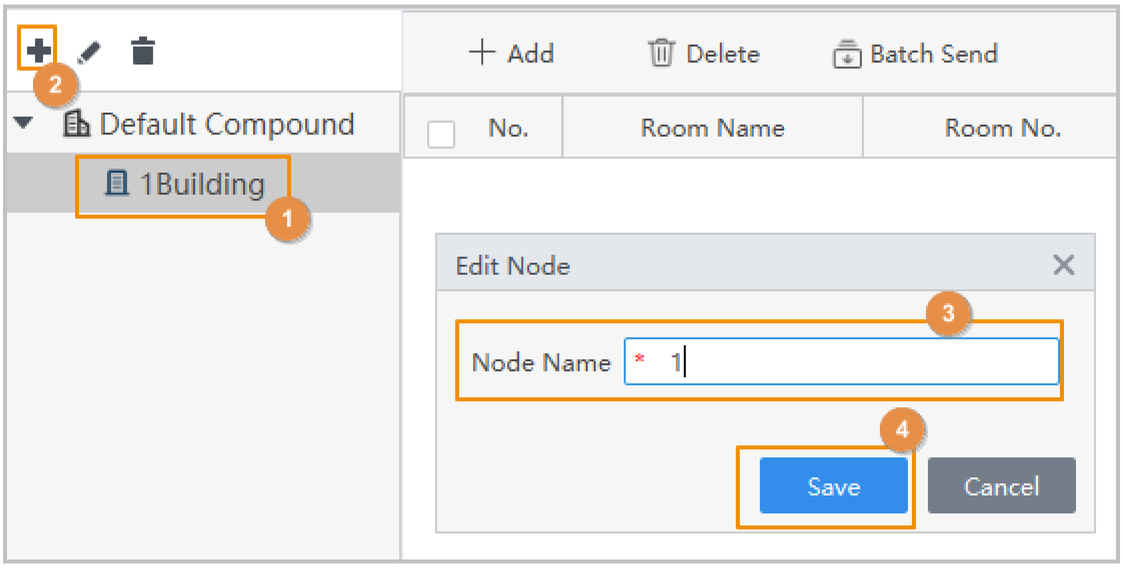
Figure 3-1 Add buildings



Node Name * 1

Step 3 Add units under the building level.

Figure 3-2 Add units

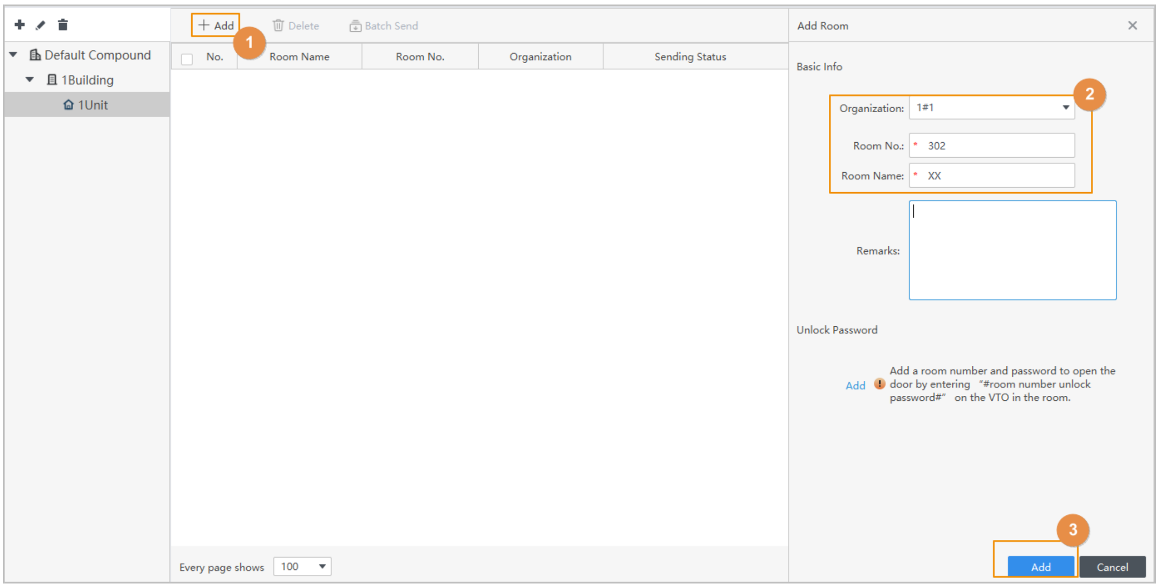


Node Name: * 1

Step 4 Add rooms under the unit level.

1. Click **Add**.
2. Select a unit from the organization.
3. Enter the number of the room and the name of the room.
4. If you want to control access by entering the room password in the VTH, you can configure an unlock password. For details, see "3.3 Configuring Unlocking Through Password".
5. Click **Add**.

Figure 3-3 Add rooms



Organization: 1#1

Room No.: * 302

Room Name: * XX

Add a room number and password to open the door by entering "#room number unlock password#" on the VTO in the room.

Every page shows 100

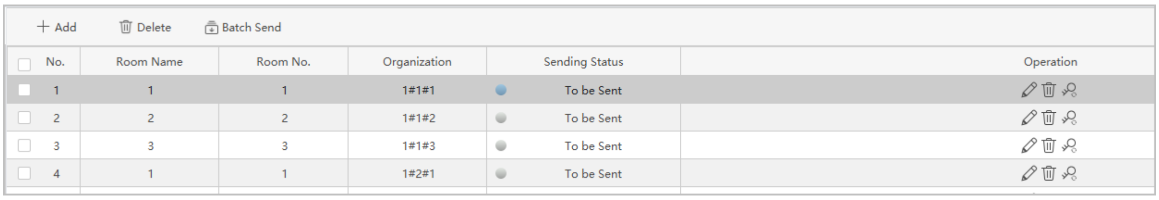
Results

The organization is created.

- Organization: Displays the exact organization level of the room. For example, 01#01#302 means building 01, unit 01 and room 302.
- Sending Status: If an unlock password is added for a room, the password will be sent to the VTO and VTH automatically, and the sending status will be displayed.

- 🔑: Manually sends the unlock passwords that were set to the devices.

Figure 3-4 Created organization



+ Add 🗑 Delete Batch Send

□	No.	Room Name	Room No.	Organization	Sending Status	Operation
□	1	1	1	1#1#1	● To be Sent	✎ 🗑 🔑
□	2	2	2	1#1#2	● To be Sent	✎ 🗑 🔑
□	3	3	3	1#1#3	● To be Sent	✎ 🗑 🔑
□	4	1	1	1#2#1	● To be Sent	✎ 🗑 🔑

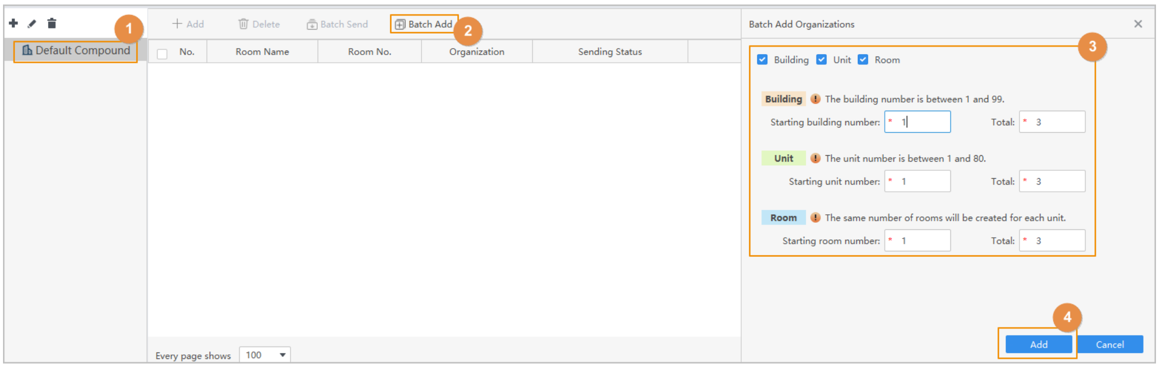
Related Operations

- Create organizations in batches.

  Only when no organizations were created, you can add organization in batches.

  1. Select the root node, and then click **Batch Add**.

  Figure 3-5 Add organizations in batches



Default Compound

+ Add 🗑 Delete Batch Send Batch Add

□	No.	Room Name	Room No.	Organization	Sending Status

Every page shows 100

Batch Add Organizations ×

☑ Building ☑ Unit ☑ Room

Building: The building number is between 1 and 99.
Starting building number: * 1 Total: * 3

Unit: The unit number is between 1 and 80.
Starting unit number: * 1 Total: * 3

Room: The same number of rooms will be created for each unit.
Starting room number: * 1 Total: * 3

Add Cancel

  2. Enable the organization level, and then enter the number.
  3. Click **OK**.

     The organizations will be automatically added as desired.

- On the organization list, you can perform the following operations.
  - Change the name of the organization.
  - Delete the organizations. If rooms were associated with the organization, the organization cannot be deleted.
- For added rooms, you can perform the following operations.
  - ✎: Edit the information of the room.
  - 🗑: Deletes the room.
  - 🔑: Sends the unlock password to the VTO and VTH. For details on how to configure unlock password, see "2.3 Configuring Unlocking Through Password".
  - Batch Send: Send unlock password of all selected rooms.

3.2 Dial Management

Configure the registration number for the devices for them to call each other through the registration numbers.

Prerequisites

The organization was created. For details, see "3.1 Building Management".

Procedure

Step 1 Click **Intercom Config** > **Dial Management**.

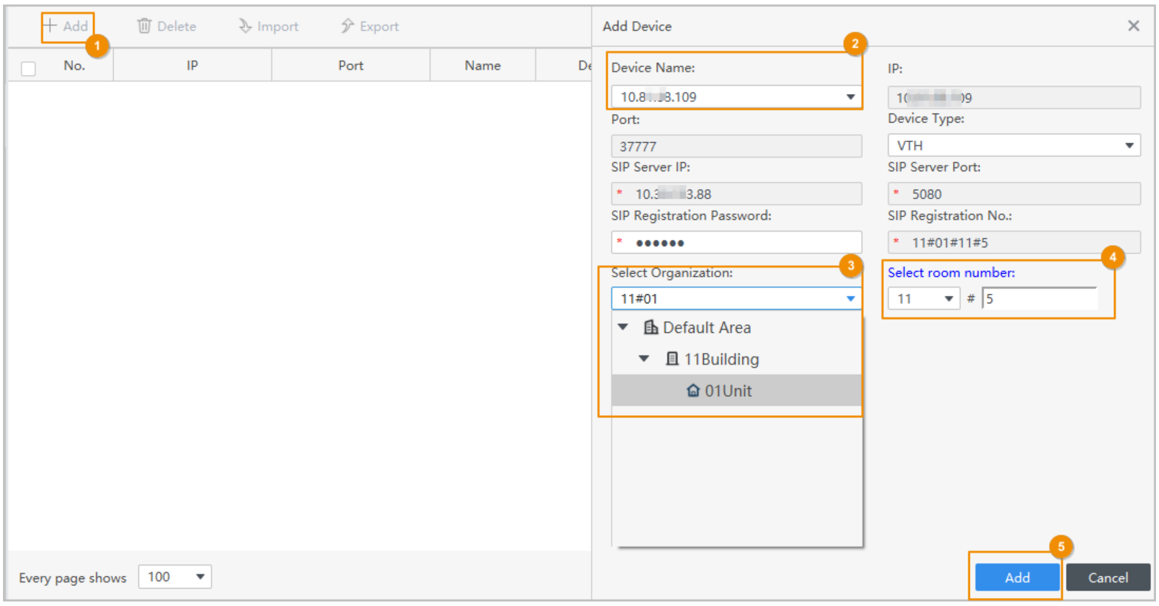
Step 2 Add registration number for VTH.

1. Click **Add**.
2. Select a VTH from the drop-down list.
3. Select the organization.

   If you have added units to the organization, you can only select a unit.
4. Select a room from the list, and then enter the number of the extension if there are more than one VTH in the room.
5. Click **Add**.

   The registration number is automatically generated based on the number of building, unit, room and extension (if any). For example, 11#01#11#5 means building 11, unit 01, room 11 and extension No.5.

Figure 3-6 Add registration number for VTH



Device Name: 10.8[redacted]8.109

IP: 10[redacted]9

Port: 37777

Device Type: VTH

SIP Server IP: * 10.3[redacted]3.88

SIP Server Port: * 5080

SIP Registration Password: * ••••••

SIP Registration No.: * 11#01#11#5

Select Organization: 11#01

Default Area

11Building

01Unit

Select room number: 11 # 5

Every page shows 100

Step 3 Add registration number for VTO.

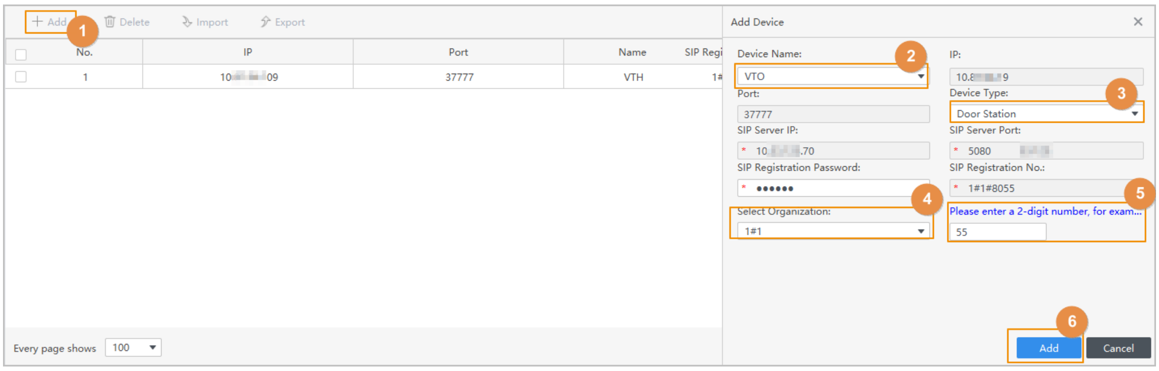
1. Click **Add**.
2. Select a VTO from the drop-down list, and select the device type.
3. Select the organization.

   If you have added units in the organization, you can only select a unit.
4. Enter a 2-digit number.

   The 2-digit number must be same to the last two digits of the number of VTO. For example, if the number of VTO is 8055, the 2-digit number must be 55.
5. Click **Add**.

   The registration number is automatically generated. For example, 1#01#8055 means building 1, unit 01 and the number of VTO is 8055.

Figure 3-7 Add registration number for VTO



No.	IP	Port	Name	SIP Regi
1	10[redacted]09	37777	VTH	1#

Every page shows 100

Device Name: VTO

IP: 10.8[redacted]9

Port: 37777

Device Type: Door Station

SIP Server IP: * 10[redacted].70

SIP Server Port: * 5080 [redacted]

SIP Registration Password: * ••••••

SIP Registration No.: * 1#1#8055

Select Organization: 1#1

Please enter a 2-digit number, for exam...

55

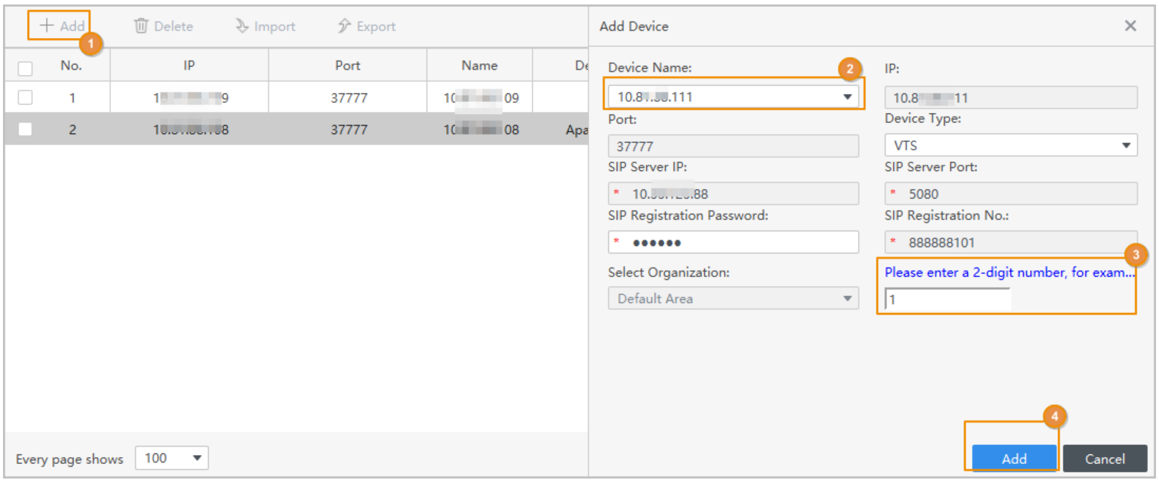
Step 4 Add registration number for VTS.

1. Click **Add**.
2. Select a VTS from the drop-down list.
3. Enter a 2-digit number.

   The 2-digit number must be same to the last two digits of the number of VTS. For example, if the number of VTS is 101 by default, the 2-digit number must be 01.
4. Click **Add**.

   The registration number is automatically generated.

Figure 3-8 Add registration number for VTS



No.	IP	Port	Name	De
1	1[redacted]9	37777	10[redacted]09	
2	10[redacted]8	37777	10[redacted]08	Apa

Every page shows 100

Device Name: 10.8[redacted].111

IP: 10.8[redacted]11

Port: 37777

Device Type: VTS

SIP Server IP: * 10.[redacted].88

SIP Server Port: * 5080

SIP Registration Password: * ••••••

SIP Registration No.: * 888888101

Select Organization: Default Area

Please enter a 2-digit number, for exam...

1

Related Operations

- Import devices through SmartPSS Lite.

  1. Click **Export** to export devices from the platform.
  2. Save the exported file to your local computer.
  3. Log in to the another platform, click **Import** > **Import SmartPSS Lite** to upload the exported file to another platform.
- Import devices through ConfigTool.

  1. Select **Import** > **Create ConfigTool Template** to download a template.
  2. Fill the information of devices in the template, and then save it to your local computer.
  3. Click **Import CofigTool**, and then import the file to the platform.

3.3 Configuring Unlocking Through Password

If the VTO is wired to door locks, you can control access by setting unlock password.

Prerequisites

- Rooms were added. For details, see"3.1 Building Management".
- VTH and VTO were registered. For details, see "3.1 Building Management".

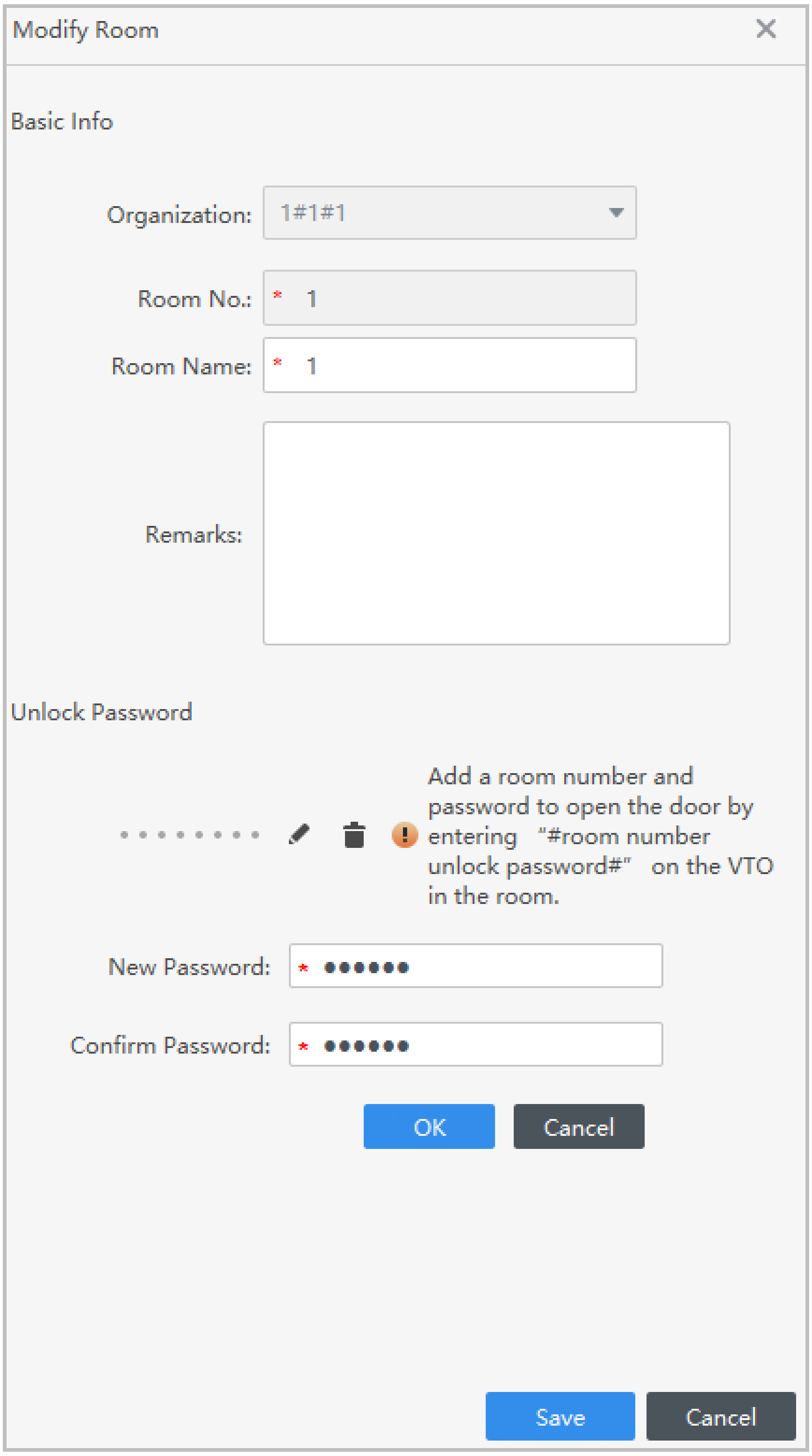
Procedure

Step 1 Click **Intercom Config** > **Building Management**.

Step 2 Select a room, and then click ✎ to add a unlock password.

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

Figure 3-9 Configure unlock password



Modify Room

Basic Info

Organization: 1#1#1

Room No.: * 1

Room Name: * 1

Remarks:

Unlock Password

Add a room number and password to open the door by entering "#room number unlock password#" on the VTO in the room.

New Password: * ●●●●●●

Confirm Password: * ●●●●●●

The password will be sent to the VTO and VTH automatically, and the sending status will be displayed.

Step 3 You can click to manually send the unlock passwords that were set to the devices.

Results

Enter **room number + unlock password** in the VTO, and door will be unlocked. For example, if the room number is 11, and the unlock password is set as 888888, enter 000011888888 in the VTO to unlock the door.

3.4 Call Group

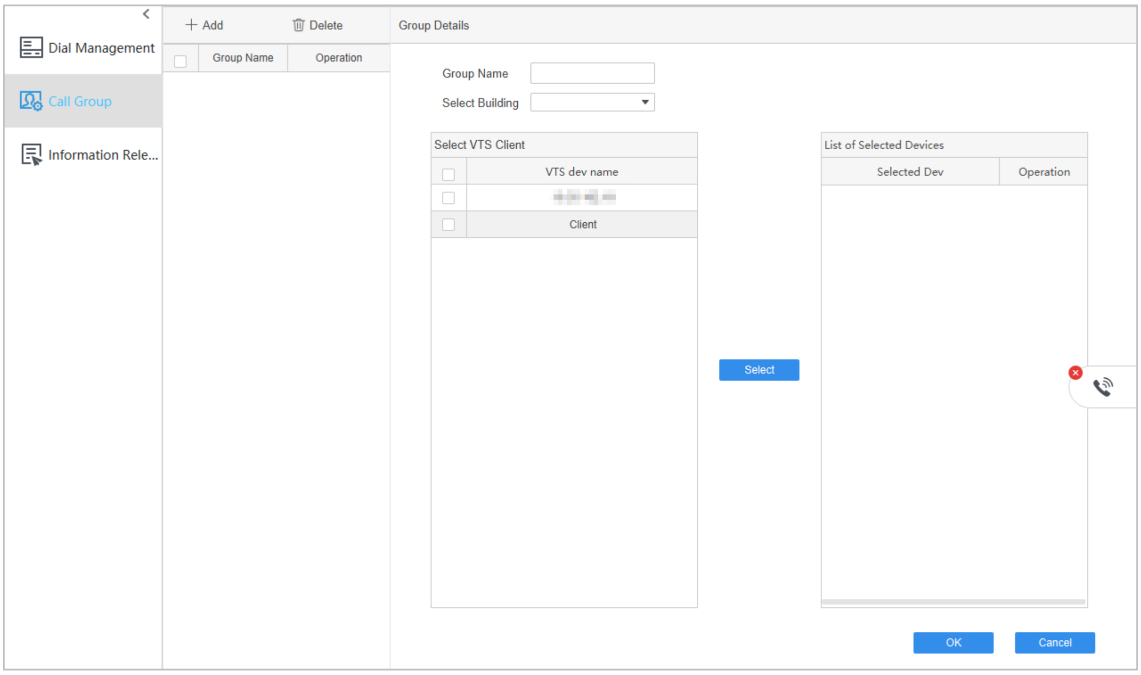
The call group function groups the VTS and the manager client, and then assigns them to the corresponding buildings, so that the buildings can call the corresponding VTS and manager client in sequence.

Procedure

Step 1 Open the **Video Intercom** solution.

Step 2 Select **Intercom Config** > **Call Group**.

Figure 3-10 Priority manager page



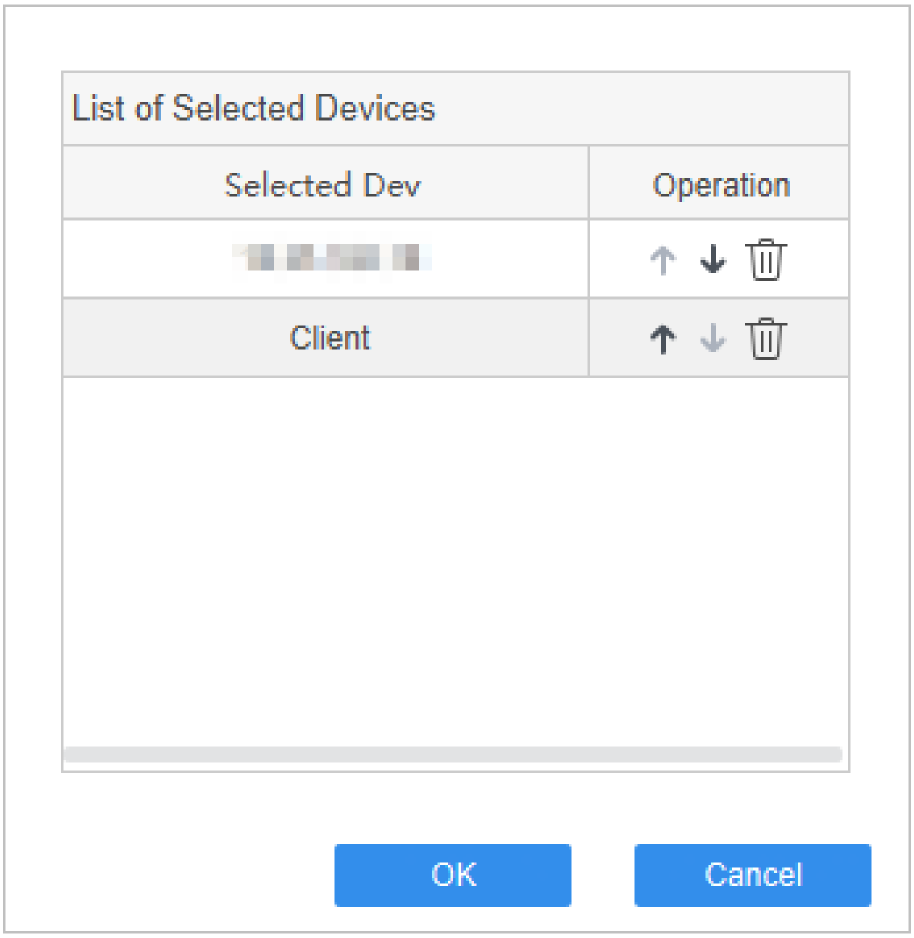
Step 3 Enter the **Group Name**, and then select the building from the drop-down list.

Step 4 Select the manager client you need to add, click **Select** , and then the device displays on the **List of Selected Devices**.

- Click ↑ to give priority to calling this device.
- Click ↓ to lower the device priority.
- Click 🗑 to delete the device information.

When no group is added to the building, the Platform will uniformly answer the call from the device under the building; the call from the fence station can only be answered by the Platform; the VTS cannot make calls.

Figure 3-11 List of selected devices



List of Selected Devices

Selected Dev	Operation
[redacted]	↑ ↓ 🗑
Client	↑ ↓ 🗑

Step 5 Click **OK**.

Related Operations

- Click **Add** to add multiple groups.
- Click 🗑 corresponding to the group, or select the group to be deleted, and then click **Delete** to delete the group information.

3.5 Information Release

Background Information

This function is only supported by the devices whose device type is VTO or VTH and whose numbers are bound to the Platform.

Procedure

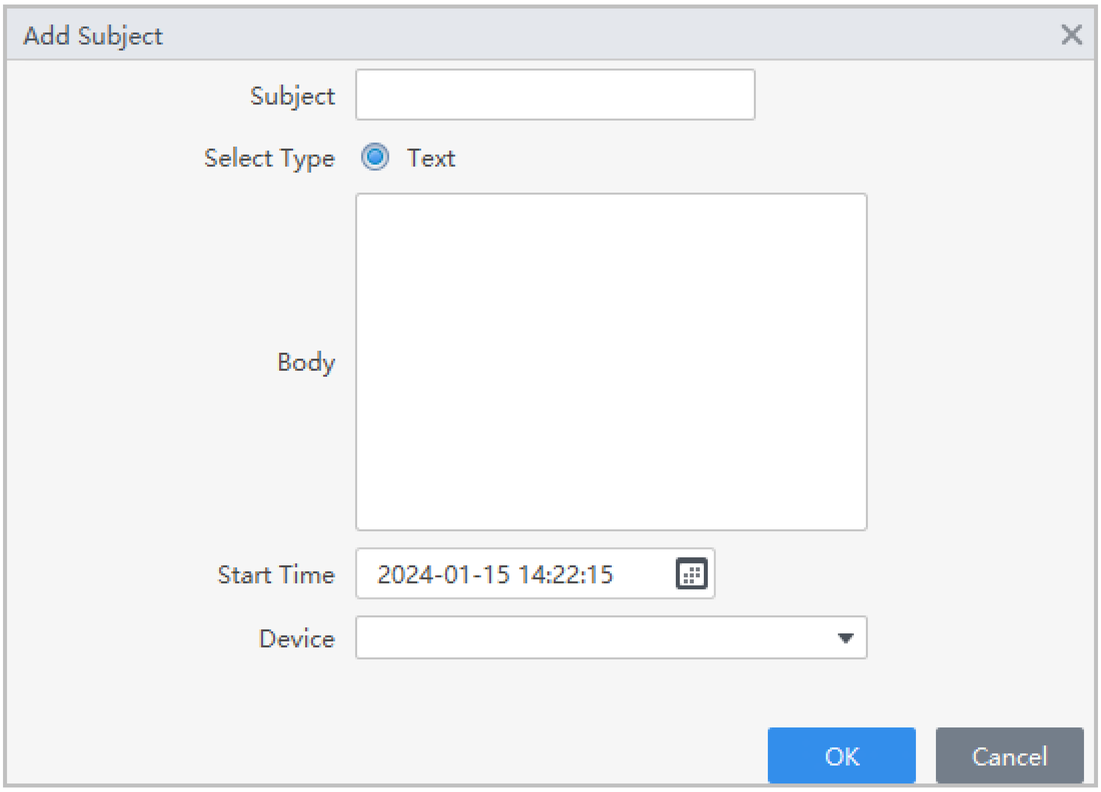
Step 1 Select **Intercom Config** > **Information Release**.

Step 2 Click **Add** to add the subject.

Step 3 Enter the text, and then set the **Start Time**.

Step 4 Select the device from the drop-down list, and then click **OK**.

Figure 3-12 Add topic



Add Subject

Subject

Select Type ● Text

Body

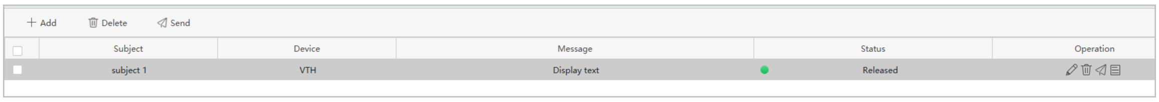
Start Time 2024-01-15 14:22:15

Device

Step 5 Click ◁ to release the subject.

Step 6 View the added subject.

Figure 3-13 View the added subject



□	Subject	Device	Message		Status	Operation
□	subject 1	VTH	Display text	●	Released	✎ 🗑 ◁ ☰

Related Operations

- Click ✎ to modify the subject.
- Click 🗑 to delete the subject.
- Click ☰ to view the details of the subject.

4 Intercom Management

You can make video calls with VTO, fence station, VTS, villa door station and VTH and the Platform. You can also perform remote unlock, view recent records and make quick calls.

Prerequisites

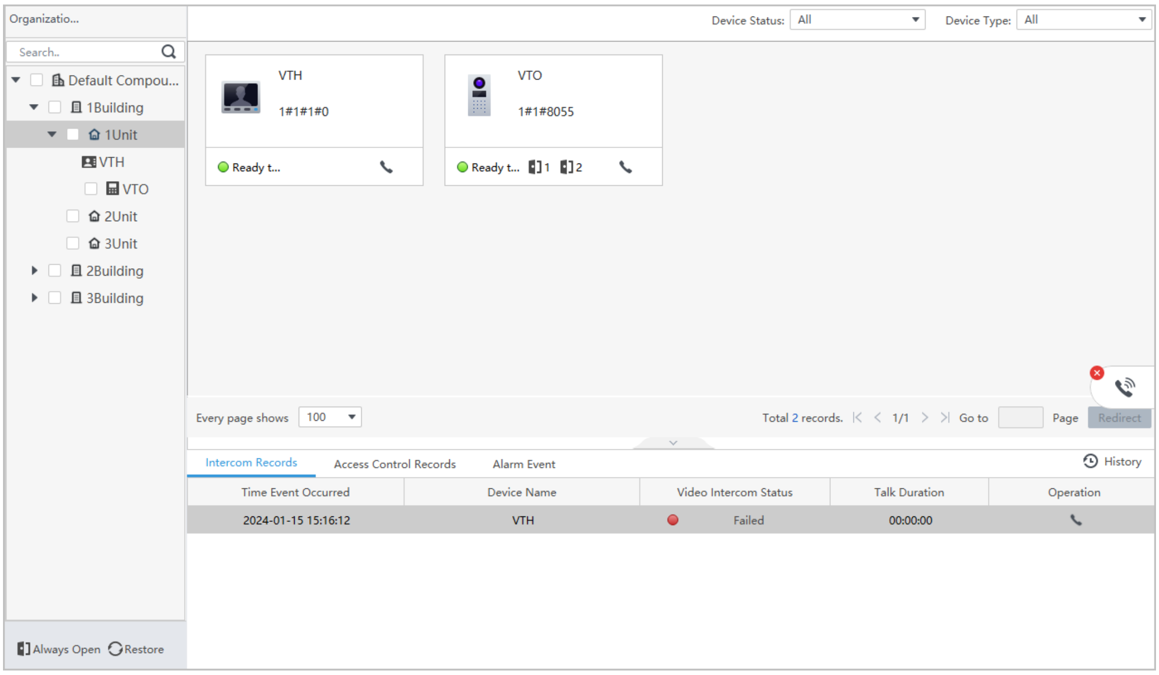
- VTH and VTO were added to the platform.
- VTH and VTO were registered. For details, see "3.1 Building Management".

Procedure

Step 1 Click **Intercom Management** on the home page, and then select the intercom device in the organization tree.

The organization tree is displayed at the unit level by default.

Figure 4-1 Intercom management page



Time Event Occurred	Device Name	Video Intercom Status	Talk Duration	Operation
2024-01-15 15:16:12	VTH	● Failed	00:00:00	☎

- ▯1 ▯2: Displays the number of doors. It means the device is connected to 2 doors. You can also click the door to unlock the door.
- Ready to call: Click ☎ to make a video call.
- Search for devices: search for devices based on devices status and device type.
- Video call request from the device: When the device clicks the property or the management center calls the platform, you can operate the Platform according to actual needs.

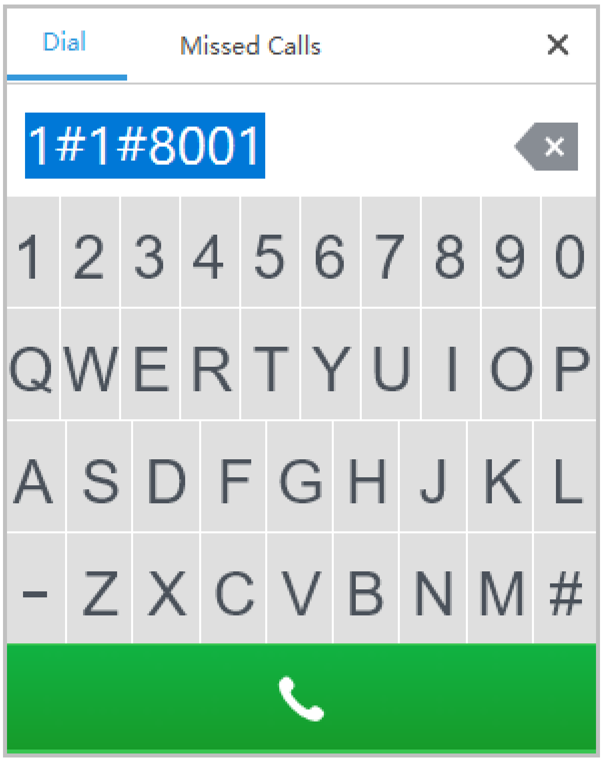
1. Click the floating window to accept the call and enter the video intercom page.
2. Click ✖ to reject the call.

- Call the intercom device.

Click ☎ to display the dial page, and then enter a number to call the corresponding intercom device.

The dial page only supports full number calls, the room number calls are not supported; if you want to call VTH, you need to enter the number and the extension number.

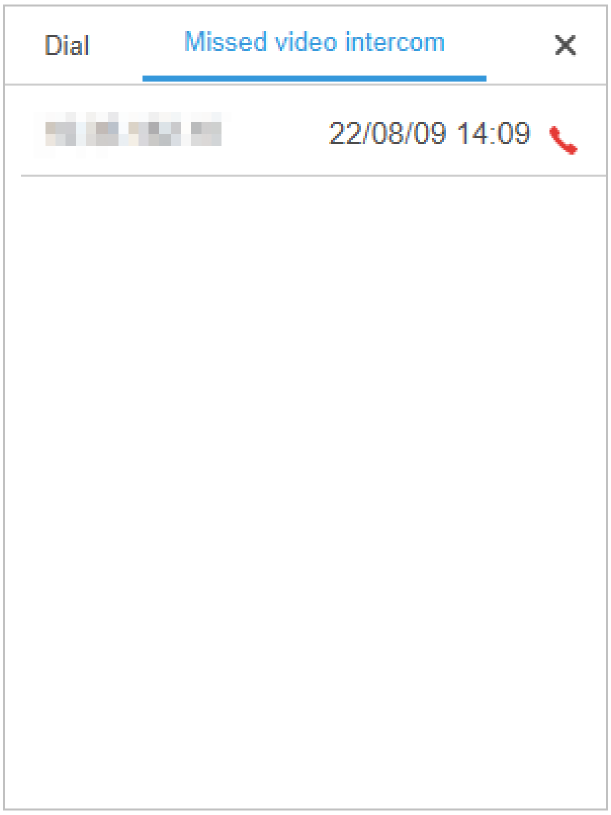
Figure 4-2 Dial page



1#1#8001

Click **Missed Calls** to view the missed video intercom calls.

Figure 4-3 Missed video intercom call



- Call back missed video intercom call.

  When there is a missed or rejected call record, you can click ☎ behind the record to call back, or click the floating window, and then click ☎ behind the corresponding call to call back.

Step 2 Perform operations during a video intercom call according to actual needs.

The Platform automatically records the switch status, and it will take effect in the next intercom.

Figure 4-4 Video intercom page

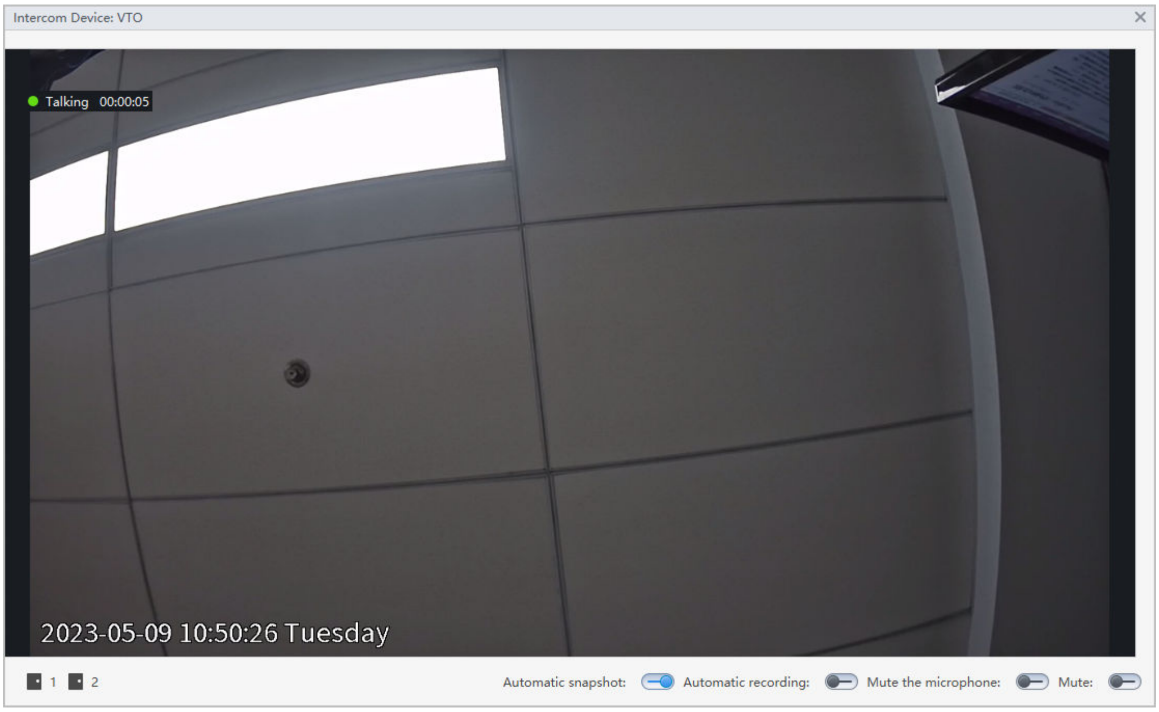


Table 4-1 Description of video intercom page parameters

Parameter	Description
■ 1 ■ 2	Open the door of the device.
Automatic snapshot	After enabling, every time the device connects to the video intercom, the Platform will capture a snapshot of the call and save it to the video intercom record.
Automatic recording	After enabling, every time the device connects to the video intercom, the Platform will record the call video and save it to the video intercom record. Only one recording can be retained for per call.
Mute the microphone	After enabling, your microphone will be muted.
Mute	After enabling, the device microphone will be muted.

Step 3 Click × on the upper-right corner to close the video intercom page and terminate the call.

Related Operations

- Click ◉ on the call record page to view the pictures and videos saved during the video intercom call.
- Call event, access event and alarm events will be recorded in real time in the record list on the bottom of the page. The record list only displays the latest 100 call records, access control records and alarm records. Click **History** to go to the **Intercom Records** page to view all records.
- Always Open: All doors remain open.
- Restore: Restore door status back to normal.

5 Intercom Records

You can view and export call records, access control records or alarm events.

Procedure

Step 1 Click **Intercom Records**.

Step 2 Select the type of records.

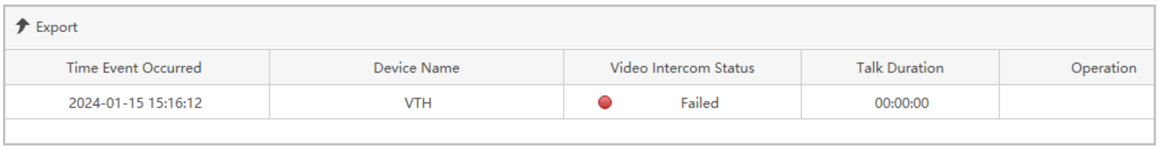
- Intercom records
- Access control records
- Alarm event

Step 3 Select the device in the organization tree, and then set the time.

For intercom records, you need set the status.

Step 4 Click **Search**.

Figure 5-1 View call records



Time Event Occurred	Device Name	Video Intercom Status	Talk Duration	Operation
2024-01-15 15:16:12	VTH	● Failed	00:00:00	

Step 5 (Optional) You can click **Export** to export all the records to your computer.

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.