

SmartPSS Lite Video Intercom Solution

User's Manual








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
V1.1.0	Updated the person management.	December 2024
V1.0.4	<ul style="list-style-type: none">Added palm vein verification.Updated adding person.	September 2024
V1.0.3	Updated the person management and permission management.	January 2024
V1.0.2	<ul style="list-style-type: none">Updated the intercom configuration function.Updated the intercom management function.	April 2023
V1.0.1	<ul style="list-style-type: none">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

Foreword.....	I
1 Person Management.....	1
1.1 Adding Company.....	1
1.2 Adding Person.....	1
1.2.1 Adding Departments.....	1
1.2.2 Setting Card Type.....	2
1.2.3 Adding Personnel One by One.....	3
1.2.4 Adding Personnel in Batches.....	5
1.2.5 Other Operations.....	6
1.3 Person Collection.....	11
2 Permission Configuration.....	14
2.1 Adding Permission Areas.....	14
2.2 Assigning Permissions.....	15
2.3 Viewing Authorization Progress.....	16
3 Intercom Configuration.....	18
3.1 Building Management.....	18
3.2 Dial Management.....	20
3.3 Configuring Unlocking Through Password.....	23
3.4 Call Group.....	25
3.5 Information Release.....	26
4 Intercom Management.....	28
5 Intercom Records.....	32
Appendix 1 Security Recommendation.....	33

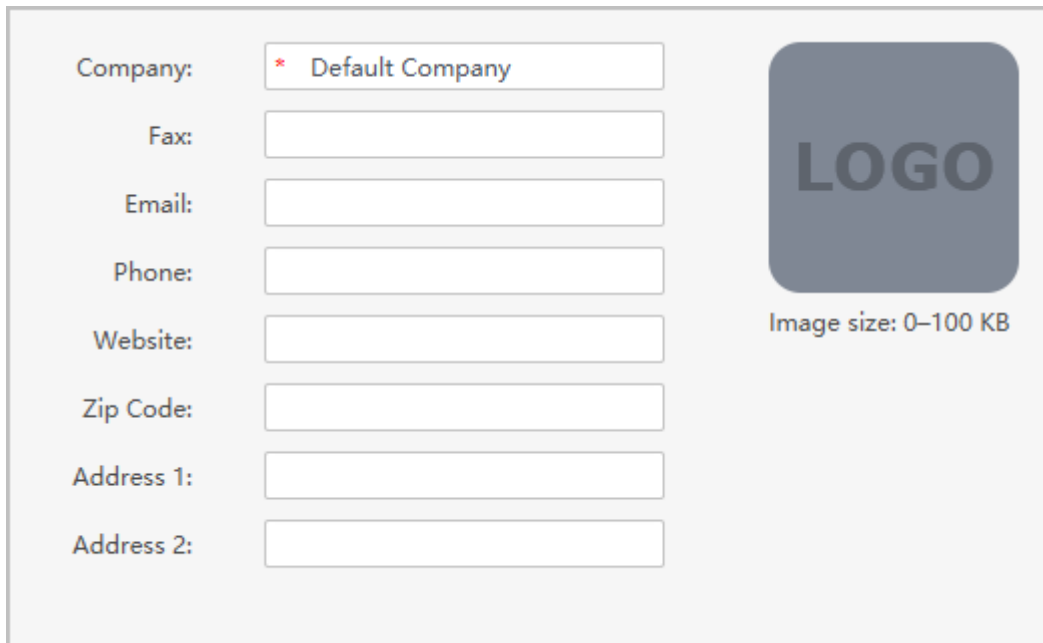
1 Person Management

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



The screenshot shows a web form for adding a company. On the left, there are several input fields stacked vertically, each with a label to its left: 'Company:', 'Fax:', 'Email:', 'Phone:', 'Website:', 'Zip Code:', 'Address 1:', and 'Address 2:'. The 'Company:' field contains the text '* Default Company'. To the right of these fields is a large square area for a logo. Inside this area is a grey rounded rectangle with the word 'LOGO' in white capital letters. Below the logo area, the text 'Image size: 0-100 KB' is displayed.

1.2 Adding Person

Select one of the methods of adding staff.

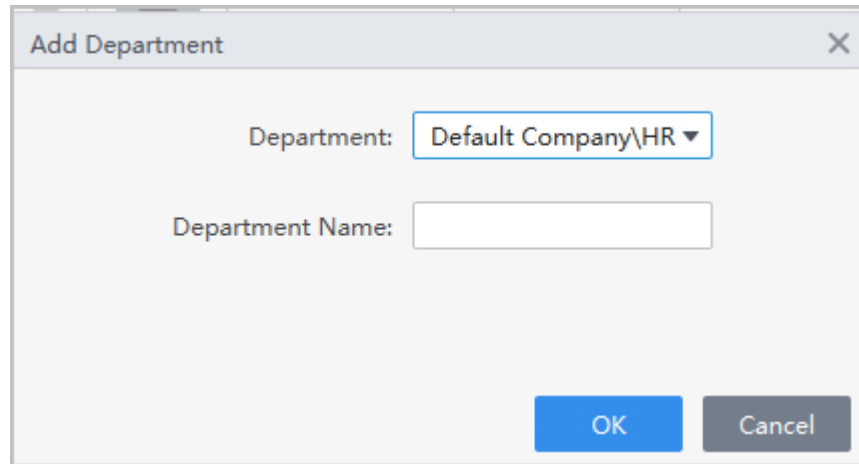
- Add staff one by one manually.
- Add staff in batches.
- Extract staff information from other devices.
- Import staff information from the local.

1.2.1 Adding Departments



Procedure

- Step 1 Select **Person** > **Person Management**.
- Step 2 In the department organization tree, click **+**.
- Step 3 Select an existing department, and then enter the name of the new department.
- Step 4 Click **OK**.

Figure 1-2 Add departments



Related Operations

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

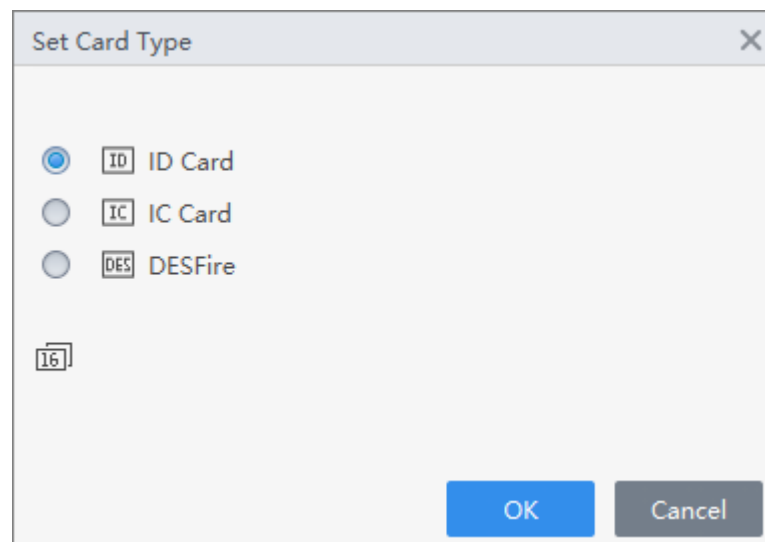
1.2.2 Setting Card Type

Before issuing cards, set the card type first as needed.


Procedure

- Step 1 Select **Person** > **Person Management**, and then click **Card Type**.
- Step 2 Configure the card type.

Figure 1-3 Set card type



- ID Card: The ID card is public and cannot be written.
- IC Card: The IC card is a kind of integrated chip that can be read and written.
- DESFire: Select DESFire, and then you need to enter a password (consisting of 0–15 digitals and characters) used to encrypt DESFire card.

- Step 3 (Optional) Click  to change the number system from hexadecimal number (by default) to decimal number.

1.2.3 Adding Personnel One by One

Procedure

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

Step 2 Enter the basic information of personnel.

1. Click **Basic Info** tab.
2. Add the basic information of personnel.
3. Click **Take Snapshot** or **Upload Picture** to set the profile picture.
4. Configure identity verifications.

- Set password.

Click **Add** to add the password.



- ◇ For second-generation devices, set the personal password; while for non-second-generation devices, set the card password.
- ◇ The new password must consist of 6–8 digits.

- Configure the cards.

- a. Click  to select **Device** or **Card Issuer** as the card reader, and then click **OK**.








If the card type is set as **DESFire**, the card reader here you can select must support DESFire card to read and write.

- b. Click **Add** to add cards, and then click **OK**.



If the card type is set as **DESFire**, place the card on the device for 5 seconds, and then the device will write the card number.

- c. Operate the cards.

- ◇ Click  or  to set the card as main card or duress card.
- ◇ Click  to change the card number.
- ◇ Click  to delete the card.
- ◇ 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 the fingerprints.

- a. Click  to select **Device** or **Fingerprint Scanner** as the fingerprint collector.
- b. Add fingerprints.

Select **Add** > **Add Fingerprint**, and then place one of your fingers on the scanner for 3 times continuously.

- Configure the palm veins.

- a. Click  to select a device, and then click **OK**.
- b. Add palm veins.

Select **Add** > **Add Palm Vein**, place your palm over the scanner, and then follow the instructions of the scanner to complete addition.

Figure 1-4 Add basic information

Person ID: * 1

Name: *

Department: Default Company

Person Type: Normal User

Effective Time: 2024/8/28 0:00:00
2034/8/28 23:59:59 3653 Day

Times Used: Unlimited

Profile Picture
Image size: 0-100 KB

Face1
Image size: 0-100 KB

Face2
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

<input type="checkbox"/>	Fingerprint Name	Operation
--------------------------	------------------	-----------

Palm Vein

<input type="checkbox"/>	HandPrint Name	Operation
--------------------------	----------------	-----------

Buttons: Add More, Complete, Cancel

Step 3 Click **More Info** tab to add more information of the personnel.

Figure 1-5 Add more information





The screenshot shows a window titled "Add User" with a close button (X) in the top right corner. Below the title bar are two tabs: "Basic Info" and "More Info". The "More Info" tab is active. Underneath the tabs is a "Details" section. The form contains the following fields and controls:

- Gender: Radio buttons for "Male" (selected) and "Female".
- Title: A dropdown menu with "Mr." selected.
- Date of Birth: A date picker showing "1985/3/15".
- Phone No.: An empty text input field.
- Email: An empty text input field.
- Communication A...: An empty text input field.
- Admin: A toggle switch currently turned off.
- Remarks: A large empty text area.
- Credential Type: A dropdown menu with "ID Card" selected.
- Credential No.: An empty text input field.
- Organization: An empty text input field.
- Occupation: An empty text input field.
- Employment Date: A date and time picker showing "2024/8/27 15:33:56".
- Termination Date: A date and time picker showing "2024/8/28 15:33:56".

At the bottom right of the window are three buttons: "Add More" (blue), "Complete" (blue), and "Cancel" (grey).

Step 4 Click **Complete**.

Related Operations

- Click  to modify information or add more details in the list of personnel.
- Click  to delete all information of the personnel.
- Click  to freeze the cards, and then the cards cannot be used normally.
- Click  to unfreeze the cards, and then the cards can be used normally.

1.2.4 Adding Personnel in Batches

Procedure

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

Step 2 Click **Batch Update**, and then click **Batch Add**.

Step 3 Select the device type, and then set the start number and the quantity of cards.



If the card type is set as **DESFire**, the card reader here you can select must support DESFire card to read and write.

Step 4 Set the department, the validity time, and the expiration time of cards.

Step 5 Click **Read Card No.**

- Step 6 Place cards on the card issuer or the card reader.
The card numbers will be read or filled in automatically.
- Step 7 Click **OK**.

Figure 1-6 Add personnel in batches

The screenshot shows a 'Batch Add' dialog box with the following fields and controls:

- Device:** A dropdown menu currently showing 'Card Issuer'. To its right is a blue button labeled 'Read C...'.
- Start No.:** A text input field containing an asterisk (*).
- Quantity:** A text input field containing an asterisk (*).
- Department:** A dropdown menu currently showing 'Dropdown List'.
- Validity Period:** A date and time picker showing '2024/8/28 0:00:00'.
- Expiration Time:** A date and time picker showing '2034/8/28 23:59:59'.
- Issue Card:** A section containing a table with two columns: 'ID' and 'Card No.'. The table is currently empty.
- Buttons:** At the bottom right, there are two buttons: a blue 'OK' button and a grey 'Cancel' button.

1.2.5 Other Operations

1.2.5.1 Issuing Cards in Batches

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

Procedure

- Step 1 Select **Person** > **Person Management**.
- Step 2 Select personnel, and then select **Batch Update** > **Batch Issue Cards**.
- Step 3 Issue cards in batches. Card number can be read automatically by card reader or entered manually.

- Use a card issuer or a card reader to automatically read card number.
 1. Select the card issuer or a card reader, and then click **Read Card No.**



If the card type is set as **DESFire**, the card reader here you can select must support DESFire card to read and write.

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 Read C...

ID: Name:

Card No.: Department:

Start Time: End Time:

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 Read C...

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		

OK Cancel

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 extract users of **All**, **Succeed** or **failed** 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

<input type="checkbox"/>	No.	Person ID	Name	Card No.	Person Type	Department	Number of Fingerprints
<input type="checkbox"/>	1	633571	[Redacted]		VIP User		0
<input type="checkbox"/>	2	1	1		Normal User		0
<input type="checkbox"/>	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.

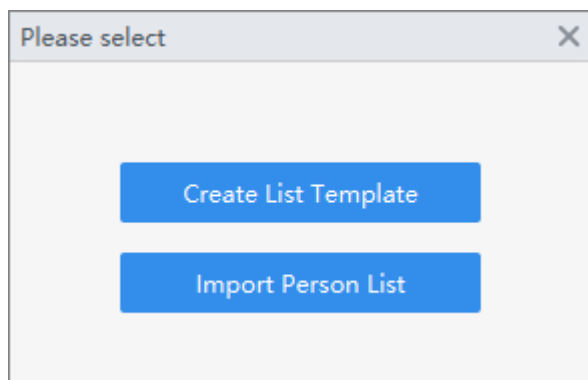
Procedure

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**, and then search for personnel by person ID, name or card ID.

Figure 1-11 Search for staff



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.



You can also view the number of each verification method in the list.

Figure 1-12 Display in list













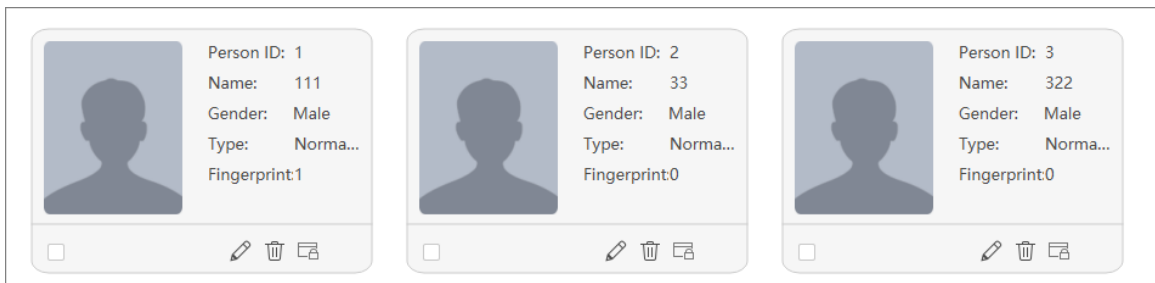
<input type="checkbox"/>	Image	Person ID	Name	Person Type	Department	Verification Method	Operation
<input checked="" type="checkbox"/>		1	111	Normal User	Default Com...	🔒 1 📄 0 🖐️ 1 🖐️ 0 🗑️ 0	  
<input type="checkbox"/>		2	33	Normal User	Default Com...	🔒 0 📄 0 🖐️ 0 🖐️ 0 🗑️ 0	  
<input type="checkbox"/>		3	322	Normal User	Default Com...	🔒 0 📄 0 🖐️ 0 🖐️ 0 🗑️ 0	  

Figure 1-13 Display in card



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 effective time in batches.

Figure 1-14 Batch edit

Step 3 Click **OK**.

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 function of pushing person information is enabled on the access control device.



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

Procedure

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

Step 2 Enable **Subscribe**. If you have added new users or modified user's 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 Fingerpi	Card No.	Person Status	Device Name	Operation
<input type="checkbox"/>		88888	tester01	0	00123456	New Person		

Step 3 Click to synchronize users to person management page.

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

You can click to see details.

Figure 1-16 Person ID conflict

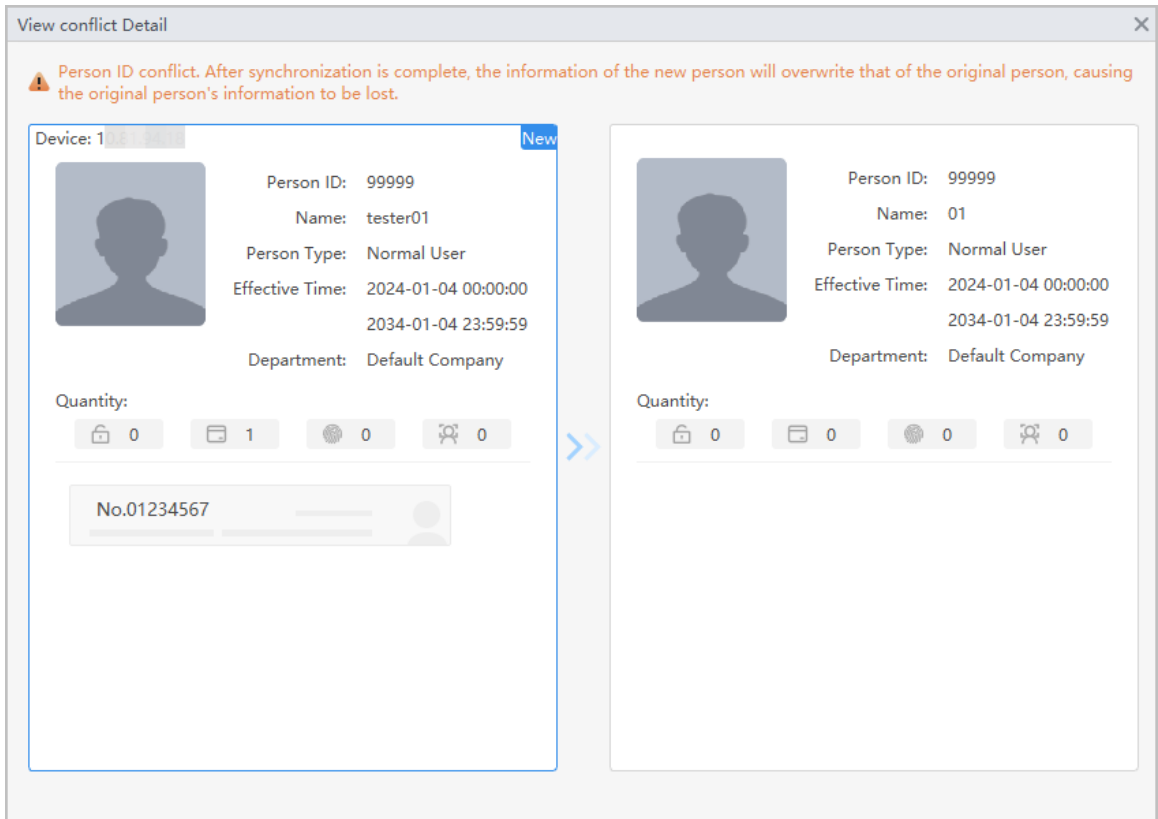


Figure 1-17 Card number conflict

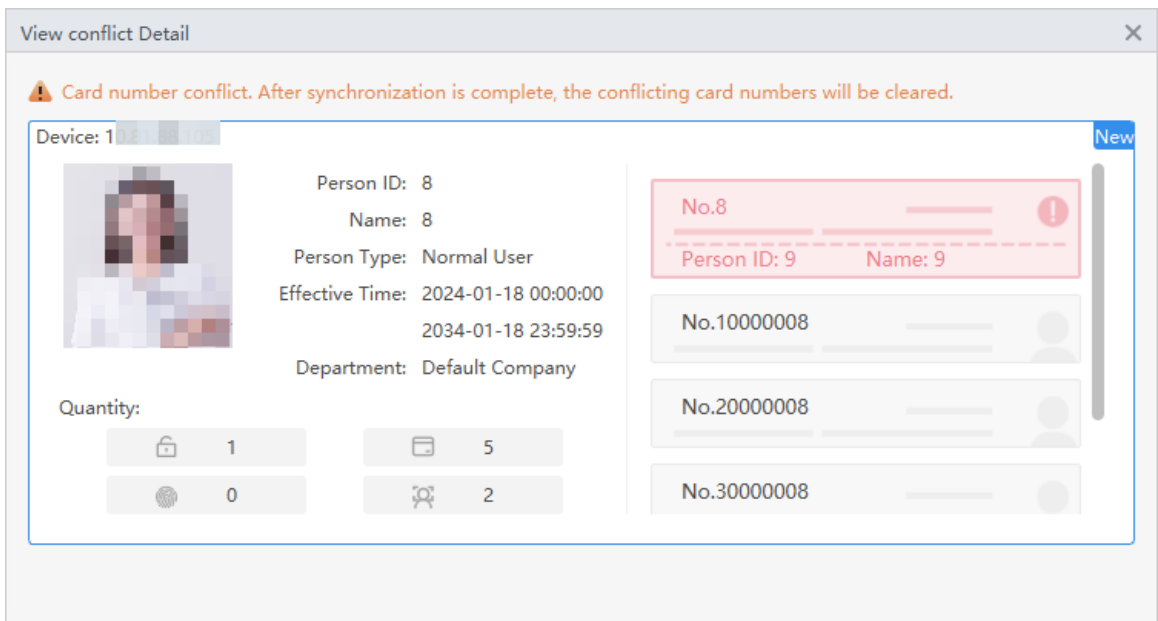
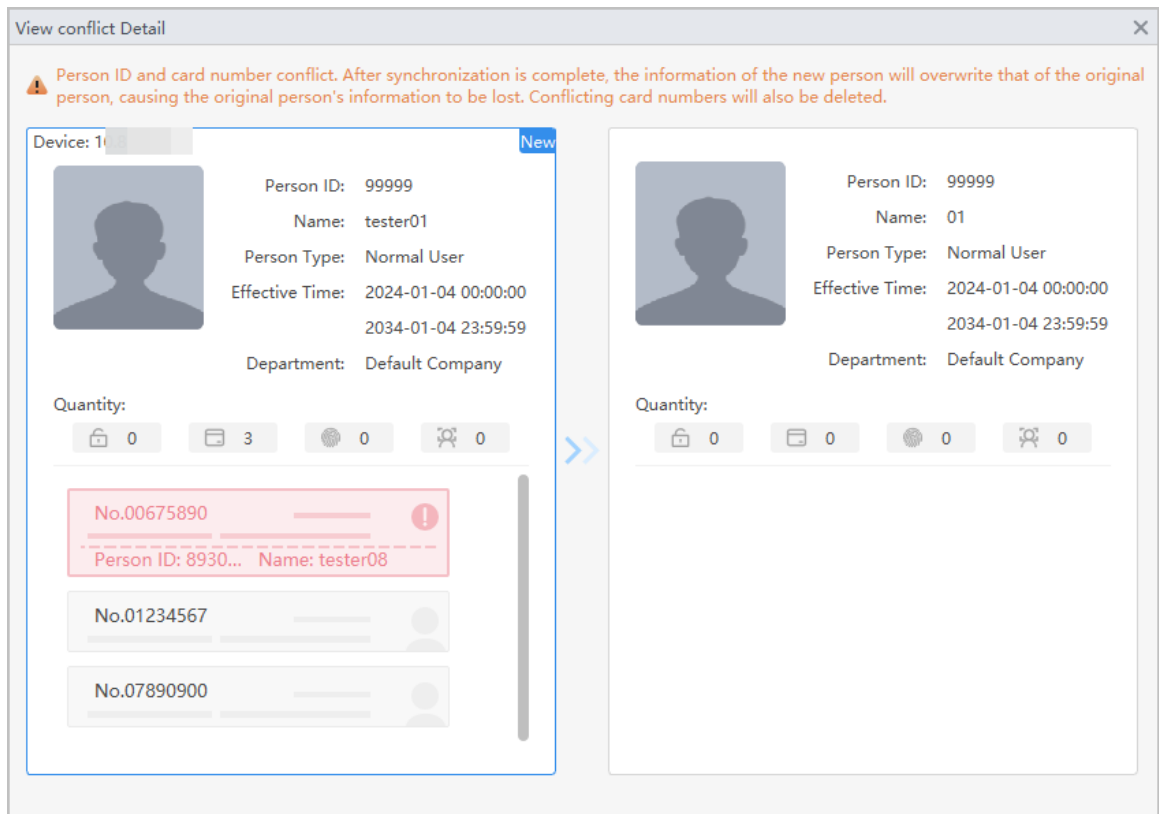


Figure 1-18 Person ID and card number conflict



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 users that are pushed to the platform do not have the same person ID or same card with any existing users in the **Person Management** page, they 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 **Permission > Area Config.**

Step 2 Click **+** to add a permission area.

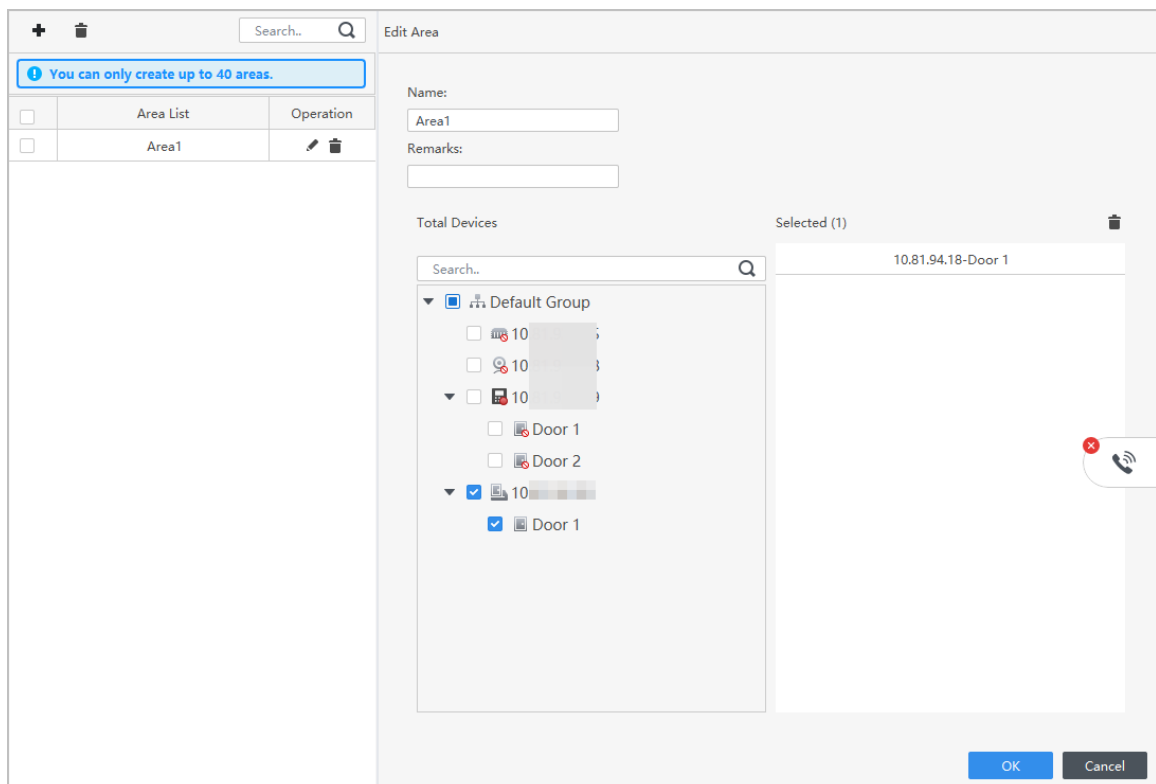


You can only create up to 40 areas.

Step 3 Configure the permission area.

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

Figure 2-1 Add permission area



Related Operations

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

2.2 Assigning Permissions

The method of configuring permissions for department and for personnel is similar, and here takes department as an example.

Procedure

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

Step 2 Click **+** to add new permission rules.



You can only create up to 128 permission rules.

Figure 2-2 Assign permissions rules

- **Weekly Plan/Holiday Plan:** Select plans to be sent to the device, and then personnel can open the door during the selected plans. For more information about configuring plans, see SmartPSS Lite Access Control Solution User's Manual.
- **Select Data to be Sent:** The permission data include card, fingerprint, password, face, and palm vein, which can be sent to the device only when they are selected. After that, personnel can open the door through these verifications.

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

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

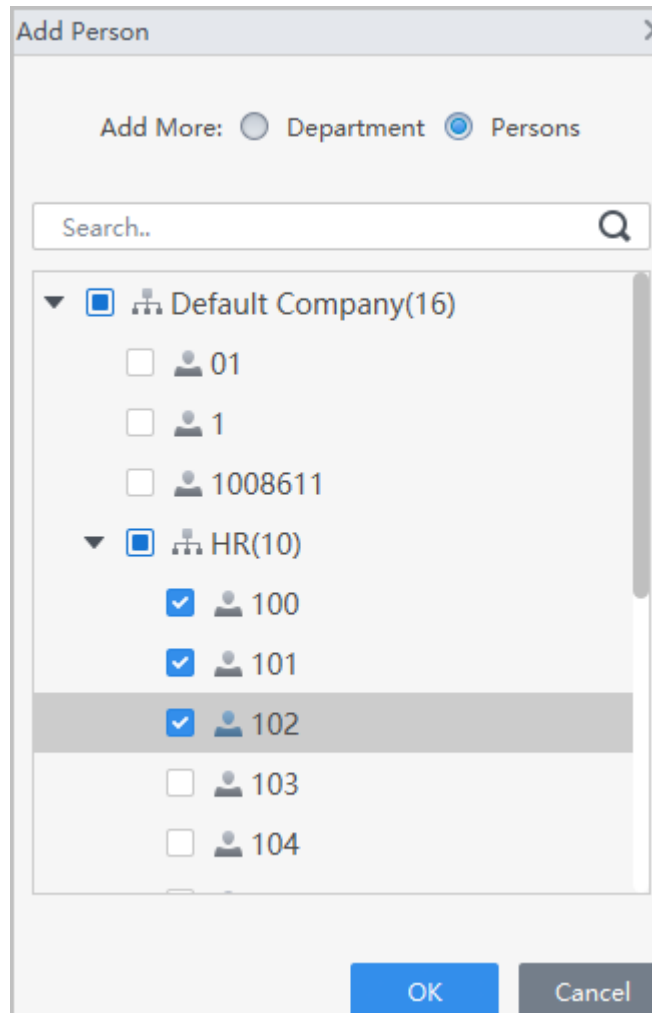
You can select personnel on the department or individual users.

- **Department:** All personnel in the department will be assigned with access permissions.
- **Persons:** Only selected users will be assigned with access permissions.



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

Figure 2-3 Add users



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

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 2-4 Authorization progress

Permission Rule	Device Name	Progress	Status	Sending Results	Operation
Permission Rule1		<div style="width: 100%;"><div style="width: 100%;"></div></div> 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 **Devices** on the home page, and then add video intercom devices to the Platform. For details, see *SmartPSS Lite General User's Manual*.

3.1 Building Management

Create a compound organization. You can add buildings, units under it. Take how to create the organization at the unit level as an example.

Prerequisites

Make sure that the compound organization has been configured in **System > Video Intercom**.



- Enabling the **Building** or **Unit** here, you can create buildings or units in **Building Management** of video intercom.
- The compound organization can be set as **Building**, or **Building** and **Unit**.
- If you want to change the compound organization, clear the organizations first.

Procedure

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

Step 2 Add buildings under the compound level.


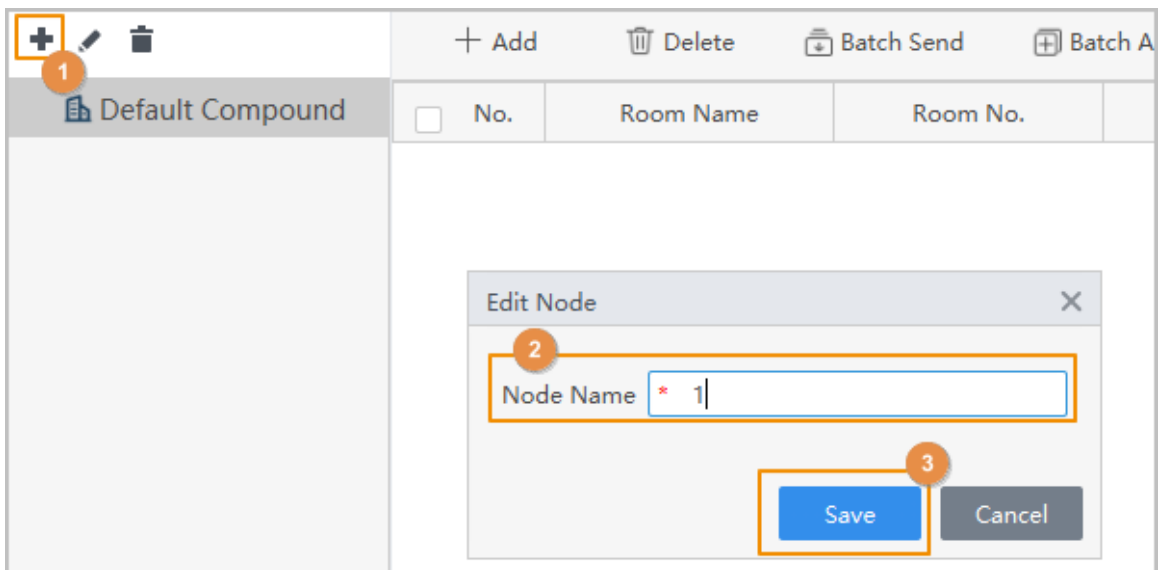
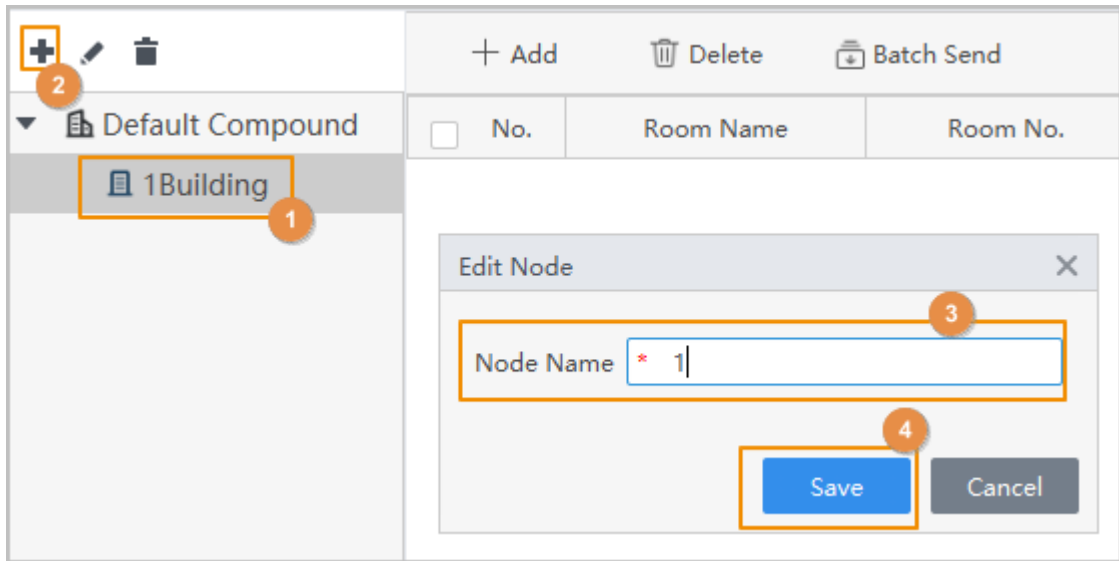
You can click  to edit the name of the default compound.

Figure 3-1 Add buildings



Step 3 Add units under the building level.

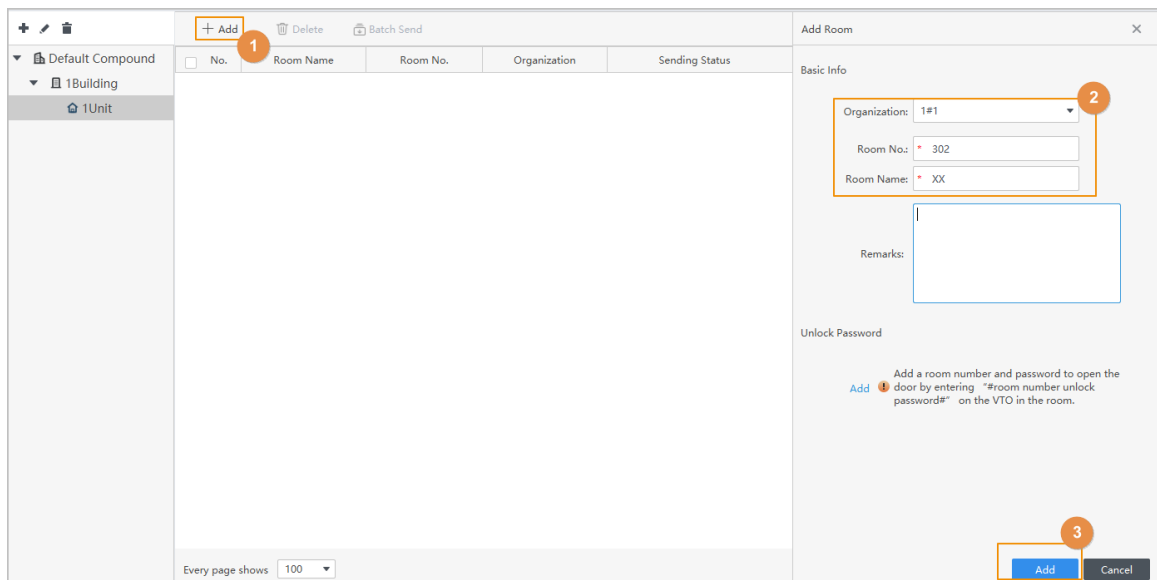
Figure 3-2 Add units



Step 4 Add rooms under the unit level.

1. Click **Add**.
2. Select a unit from the organization.
3. Enter the number 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



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.


- : Synchronize the passwords to the devices.

Figure 3-4 Created organization

No.	Room Name	Room No.	Organization	Sending Status	Operation
<input checked="" type="checkbox"/>	1	1	1#1#1		To be Sent
<input type="checkbox"/>	2	2	1#1#2		To be Sent
<input type="checkbox"/>	3	3	1#1#3		To be Sent
<input type="checkbox"/>	1	1	1#2#1		To be Sent

Related Operations

- Create organizations in batches.








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

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

Figure 3-5 Add organizations in batches

2. Enable the organization levels, 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

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.

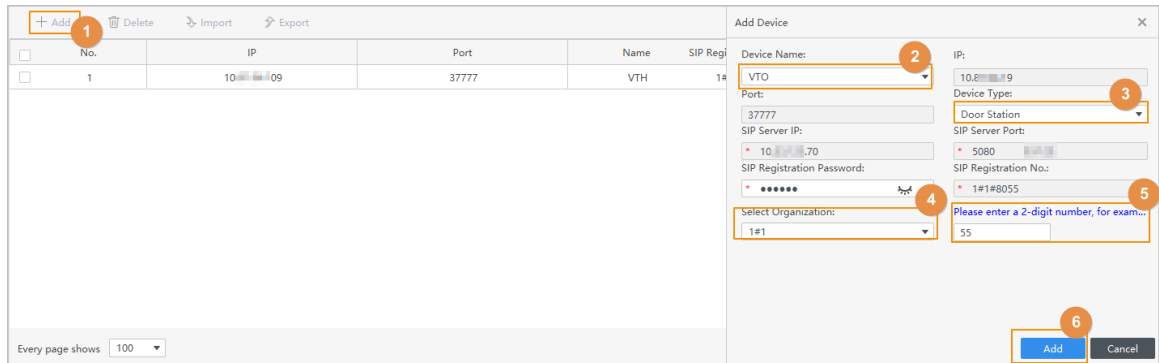
4. Enter a 2-digit number.

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



Step 4 Add registration number for VTS.

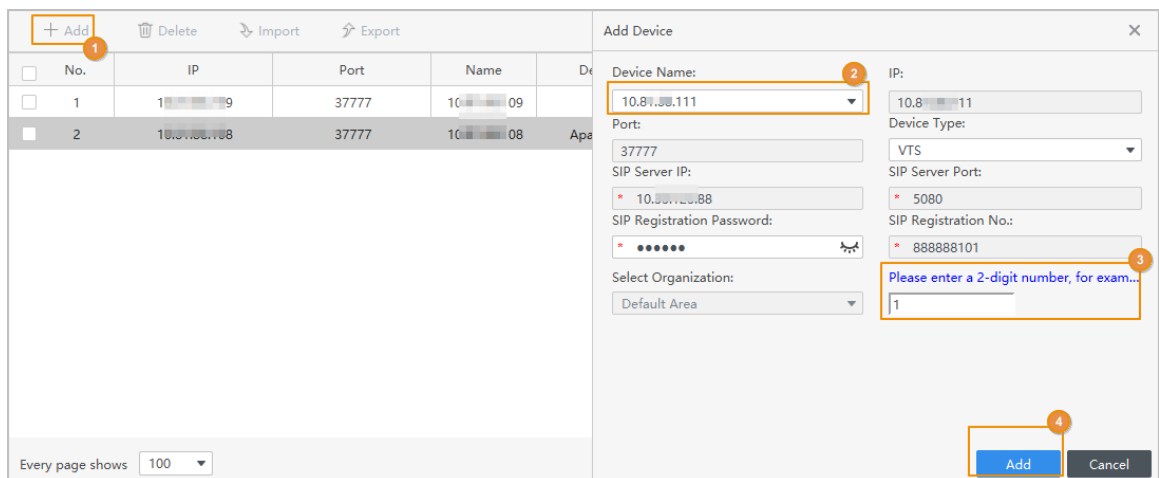
1. Click **Add**.
2. Select a VTS from the drop-down list.
3. Enter a 2-digit number.

The 2-digit number must be the same as 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



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 ConfigTool**, 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 the password.
3. Click **OK**.

Figure 3-9 Configure unlock password

Modify Room

Basic Info

Organization: 1#1#11

Room No.: * 11

Room Name: * 1

Remarks:

Unlock Password

Add ! 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: * ●●●●●●●

OK Cancel

Save Cancel

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**, and then click **Add**.

Figure 3-10 Priority manager page

The screenshot shows the 'Priority manager' page. On the left is a navigation menu with 'Dial Management', 'Call Group', and 'Information Rel...'. The main area is titled 'Group Details' and contains a table with columns 'Group Name' and 'Operation'. Below the table are input fields for 'Group Name' and 'Select Building'. There are two main panels: 'Select VTS Client' and 'List of Selected Devices'. The 'Select VTS Client' panel has a table with columns 'VTS dev name' and 'Client', and a 'Select' button. The 'List of Selected Devices' panel has a table with columns 'Selected Dev' and 'Operation', and 'OK' and 'Cancel' buttons at the bottom. A 'Select' button is also located between the two panels.

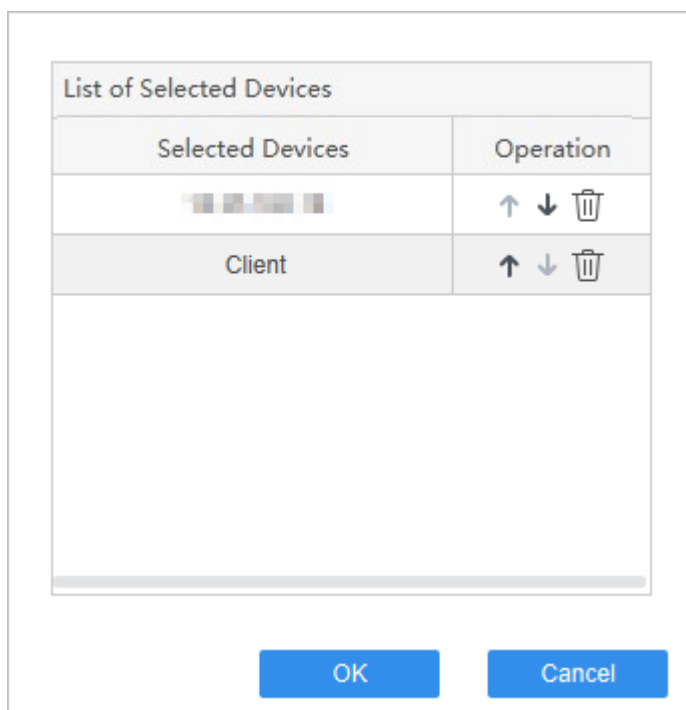
- Step 3 Enter the **Group Name**, and then select the building from the drop-down list.
- Step 4 Select the manager client you need to add, click **Select**, and then the device displays on the **List of Selected Devices**.

- 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



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



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

Dialog box titled "Edit Subject" with a close button (X) in the top right corner. The form contains the following fields:




- Subject:** A text input field containing the value "1".
- Select Type:** A radio button group with "Text" selected.
- Body:** A large text area containing the value "11232345".
- Device:** A dropdown menu currently showing "All".

At the bottom right, there are two buttons: "OK" (blue) and "Cancel" (grey).




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
<input type="checkbox"/>	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, 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".

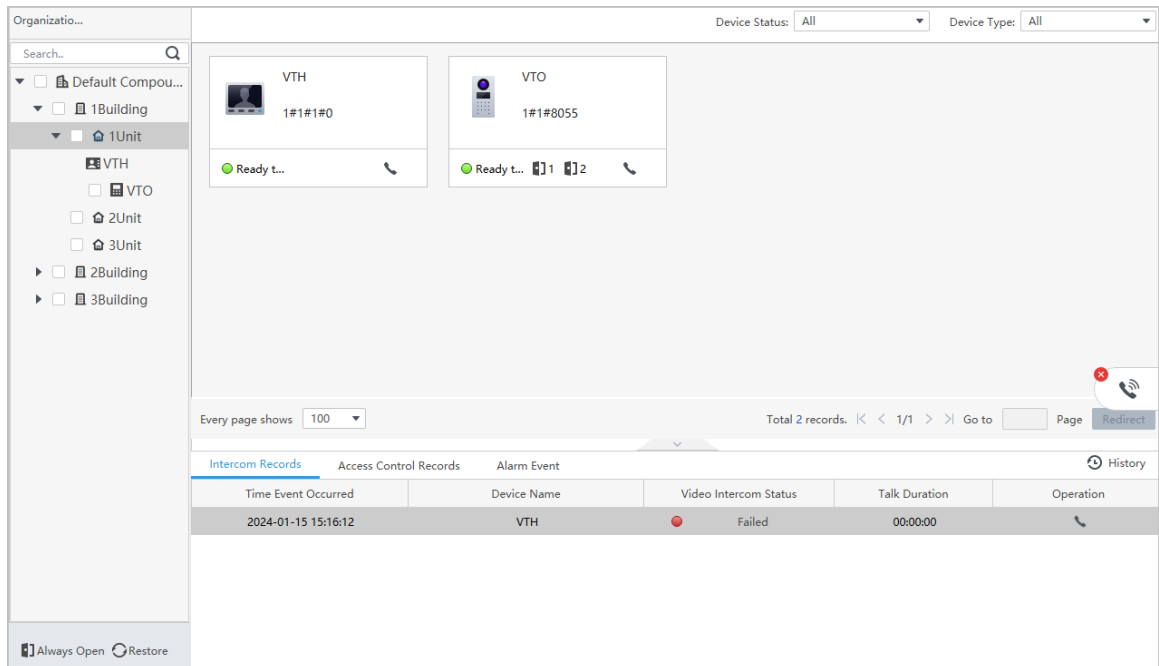
Procedure




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

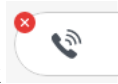


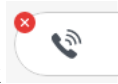
The organization tree is displayed at the unit level by default.

Figure 4-1 Intercom management page



- : 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 device status or 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.



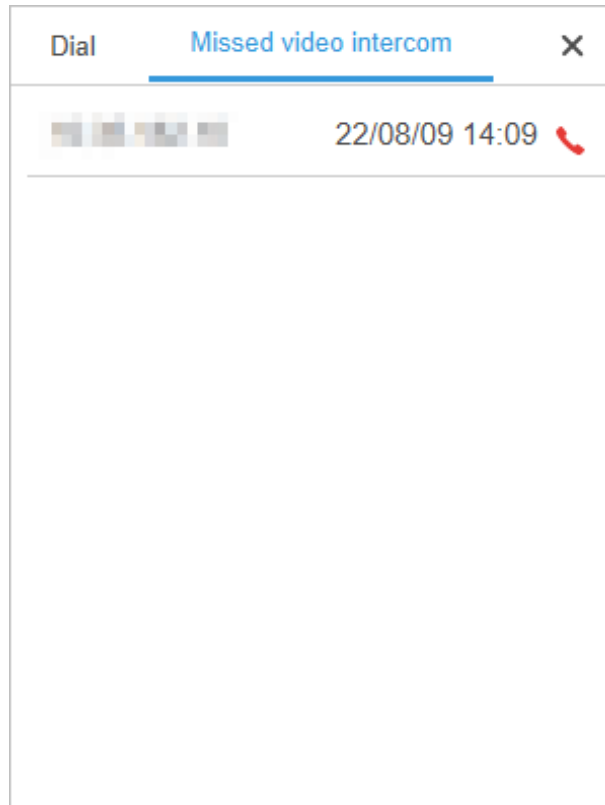
The dial page only supports full number calls, and the room number calls are not supported; if you want to call VTH, you need to enter the number and the extension number.

Figure 4-2 Dial page




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 records, you can click  to call back.

Step 2 Perform operations during a video intercom calling 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
	Open the door of the device.
Auto Capture	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.
Auto 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 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 and status.

Step 4 Click **Search**.

Figure 5-1 View call records

Export					
Time Event Occurred	Device Name	Video Intercom Status		Talk Duration	Operation
2024-09-05 16:38:24	1		Succeed	00:02:00	
2024-09-05 16:36:15	1		Succeed	00:02:00	
2024-09-05 16:33:09	1		Succeed	00:02:00	
2024-09-05 16:30:42	1		Succeed	00:00:14	

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

Appendix 1 Security Recommendation

1. Account Management

a. Use Strong 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.

b. Change Password Regularly

It is suggested to change passwords regularly to reduce the risk of being guessed or cracked.

c. Assign Accounts and Permissions Reasonably

According to business and management needs, reasonably add new users, and reasonably allocate a minimum set of permissions for them.

d. Enable Account Lock

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

e. Set and Update Passwords Reset Information Timely

The platform supports password reset function. To reduce the risk of being attacked, please set up related information for password reset in time. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

f. Enable Account Binding IP/MAC

It is recommended to enable the account binding IP/MAC mechanism to further improve access security.

2. Service Configuration

a. Enable HTTPS

It is suggested to enable HTTPS, so that you visit web service through a secure communication channel.

b. Disable Unnecessary Services and Choose Secure Modes

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

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

- SMTP: Choose TLS to access mailbox server.
- FTP: Choose SFTP, and set up strong passwords.

3. Network Configuration

a. Enable Firewall Allowlist

It is suggested to enable allowlist function to prevent everyone, except those with specified IP addresses, from accessing the system. Therefore, please be sure to add your computer's IP address and the accompanying equipment's IP address to the allowlist.

b. Network Isolation

The network should be isolated by partitioning the video monitoring network and the office network on the switch and router to different VLANs. This prevents attackers from using the office network to launch Pivoting attacks on the video monitoring network.

4. **Security Auditing**

a. **Check Online Users**

It is recommended to check online users irregularly to identify whether there are illegal users logging in.

b. **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.

5. **Physical Protection**

It is suggested to perform physical protection to the device that has installed the platform. For example, place the device in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware.

6. **Perimeter Security**

It is suggested to deploy perimeter security products and take necessary measures such as authorized access, access control, and intrusion prevention to protect the software platform security.