

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
V1.0.2	<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, 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.

Contents

Foreword.....	I
1 Personnel Management.....	1
1.1 Adding Company.....	1
1.2 Department Management.....	1
1.3 Setting Card Type.....	2
1.4 Adding Personnel.....	3
1.4.1 Adding Personnel One by One.....	3
1.4.2 Adding Personnel in Batches.....	7
1.4.3 Extracting Personnel Information.....	8
1.4.4 Importing Personnel Information.....	10
1.5 Issuing Cards in Batches.....	10
1.6 Exporting Personnel Information.....	13
1.7 Searching for Personnel.....	13
1.8 Personnel Display.....	13
1.9 Editing Personnel in Batches.....	14
1.10 Permission Configuration.....	15
1.10.1 Adding Permission Groups.....	15
1.10.2 Configuring Permissions.....	16
2 Intercom Configuration.....	18
2.1 Building Manager.....	18
2.2 Dial Management.....	20
2.3 Configuring Unlocking Through Password.....	22
2.4 Call Group.....	23
2.5 Information Release.....	25
3 Intercom Management.....	27
4 Intercom Records.....	31
4.1 Intercom Records Query.....	31
4.2 Access Control Records Query.....	32
4.3 Alarm Record Query.....	33
Appendix 1 Cybersecurity Recommendations.....	34

1 Personnel Management

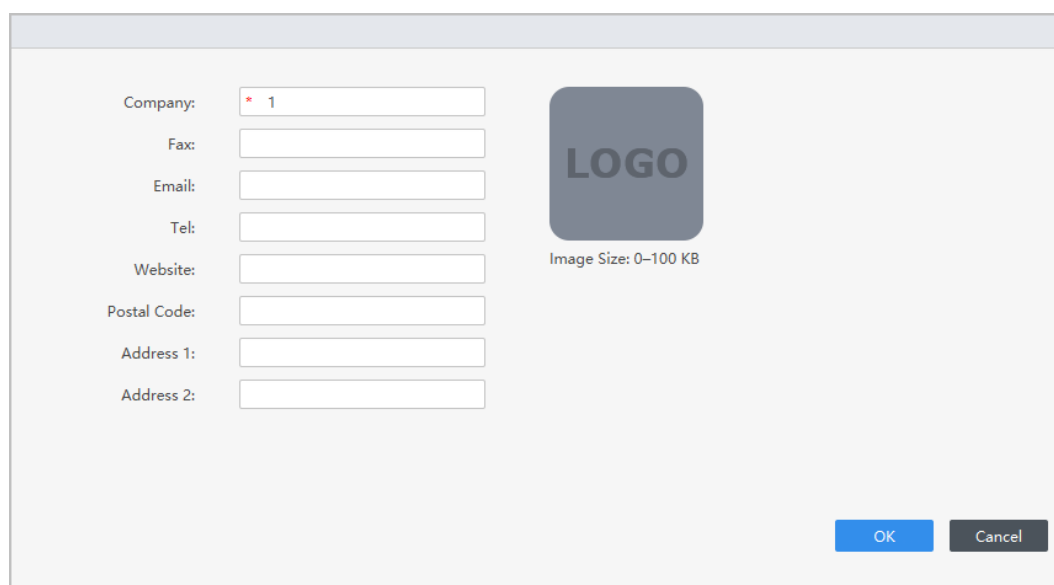
You can manage department information and staff information.

1.1 Adding Company

Procedure

- Step 1 Select **Personnel** > **Company** .
- Step 2 Enter the company name, fax, email, telephone number, website, postal code and address.
- Step 3 Upload the company logo, and then click **OK**.

Figure 1-1 Add company



Company: * 1

Fax:

Email:

Tel:

Website:

Postal Code:

Address 1:

Address 2:

LOGO

Image Size: 0-100 KB

OK Cancel

1.2 Department Management

You can add, modify or delete department. Here uses the department adding as an example.

Procedure

- Step 1 Select **Personnel** > **Personnel Management** .
- Step 2 Click **+** in the **Department List** to add.
- Step 3 Select a superior department, and then add a new sub-department.
- Step 4 Click **OK** to confirm.

Figure 1-2 Add department

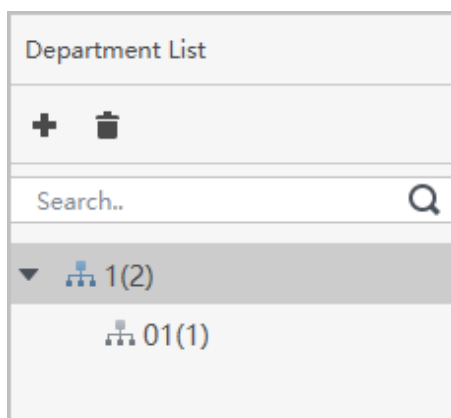
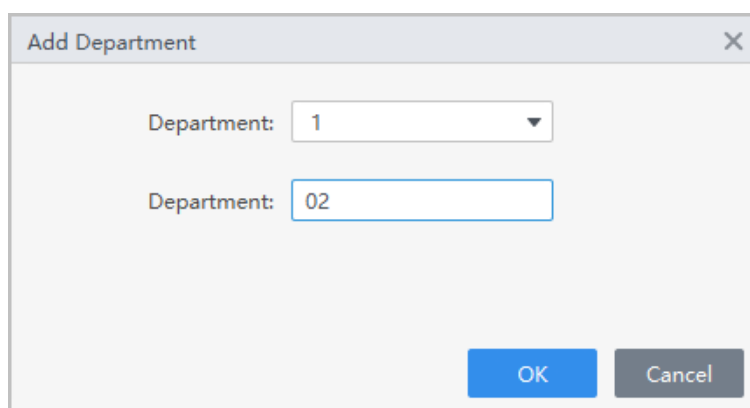




Figure 1-3 Add department information



Related Operations

- (Optional) Click  in the **Department List** to delete.
- (Optional) Select the department, and then click  in the **Department List** to rename the department.

1.3 Setting Card Type

Select **Personnel** > **Personnel Management** > **Card Issuing Type** .

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




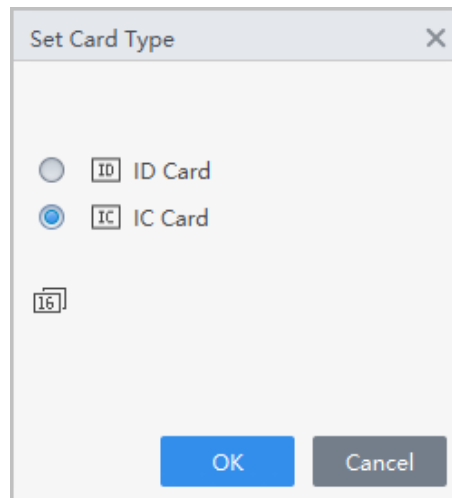
- The system uses hexadecimal card number by default. Click  to change to decimal card number.
- When the card type is changed, the card number in the **Access Manger** , user's card, and **History Event** will also be changed.

Figure 1-4 Set card type



1.4 Adding Personnel

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.

1.4.1 Adding Personnel One by One

Procedure

- Step 1 Select **Personnel** > **Personnel Management** > **Add** .
- Step 2 Enter basic information of personnel.
1. Select **Basic Info**.
 2. Add basic information of personnel.

Figure 1-5 Add basic information

Add User

Basic Info | Extended information | Permission

User ID: *

Name: *

Department: Default Company

User Type: General User

Validity Time: 2022/11/29 0:00:00 2032/11/29 23:59:59 3654 Days

Times Used: Unlimited

Take Snapshot Upload Picture Image Size: 0-100 KB

Take Snapshot Upload Picture Image Size: 0-100 KB

Take Snapshot Upload Picture Image Size: 0-100 KB

Password Add ! For the 2nd-generation access controller, 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
<input type="checkbox"/>		

Add More Finish Cancel

Step 3 Configure authentication methods.

Supports 5 authentication methods, including face recognition, password, card, and fingerprint.

- Configure face recognition: Take snapshots or upload face images in the last 2 image areas.

Figure 1-6 Register face images

- Configure password: The password must consist of 6–8 digits.
- Configure card: The card number can be read automatically or entered manually. To read the card number automatically, select a card reader, and then place the card on the card reader.
 - a. Click to select **Device** or **Card issuer** as card reader.
 - b. Add card. The card number must be added if the non-second generation access controller is used.
 - c. After adding, you can set the card as the 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 fingerprints
 - a. Click to select **Device** or **Fingerprint Scanner** as the fingerprint collector.
 - b. Add fingerprint. Select **Add** > **Add Fingerprint**, and then place the finger on the scanner 3 times in a row.

Step 4 Click **Extended information** to add other information of personnel, and then click **Finish**.

Figure 1-7 Add extended information

The screenshot shows a software window titled "Add User" with a close button (X) in the top right corner. The window has three tabs: "Basic Info", "Extended information" (which is selected), and "Permission". Below the tabs is a section labeled "Details".

Under the "Details" section, there are several input fields and controls:

- Gender:** Two radio buttons, "Male" (selected) and "Female".
- ID Type:** A dropdown menu currently showing "ID".
- Title:** A dropdown menu currently showing "Mr".
- ID No.:** An empty text input field.
- Date of Birth:** A date picker showing "1985/3/15".
- Company:** An empty text input field.
- Tel:** An empty text input field.
- Occupation:** An empty text input field.
- Email:** An empty text input field.
- Employment Date:** A date picker showing "2022/11/28 19:38:45".
- Mailing Address:** An empty text input field.
- Termination Date:** A date picker showing "2032/11/29 19:38:45".
- Administrator:** A toggle switch currently turned on.
- Remark:** A large empty text area.

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

Step 5 Configure permissions.

Permission groups are a collection of time attendance or access control permissions on defined devices. Create a permission group and then associate users with the group, so that users can be granted corresponding permissions.

Figure 1-8 Permission configuration

Add User

Basic Info | Extended information | **Permission**

☒ Group ☐ Device

Permission group is a combination of various devices including attendance check and access control devices. After selecting the permission group, the person information will be sent to corresponding devices and used for functions related to access control and attendance check.





Add Group

<input type="checkbox"/>	Permission Group	Memo
<input type="checkbox"/>	Permission Group1	

Add More **Finish** **Cancel**

Step 6 Click **Finish**.

Related Operations

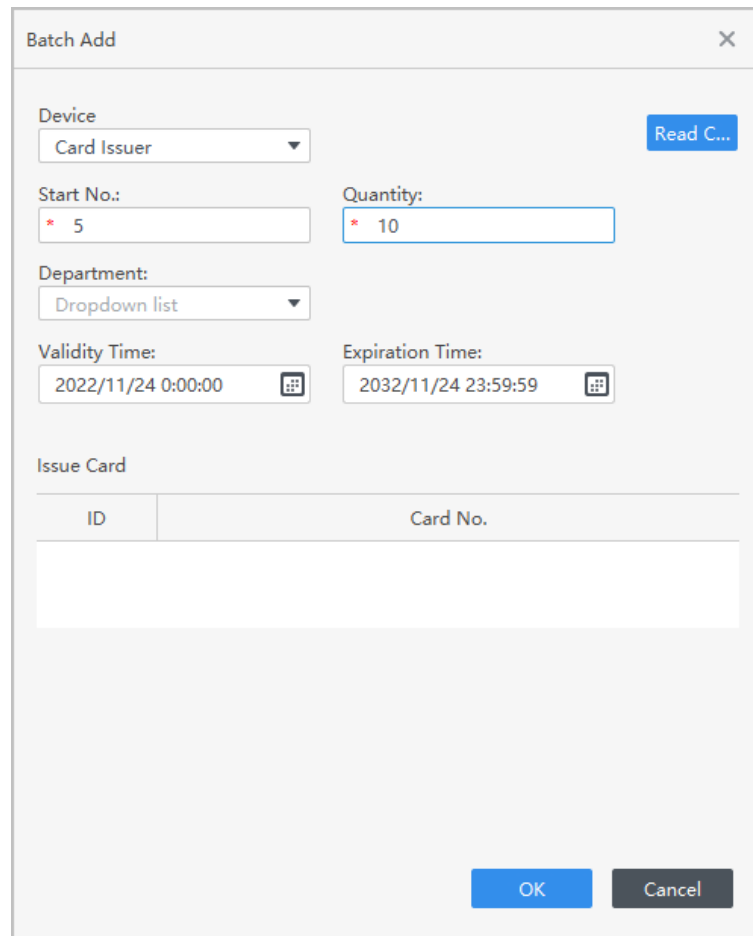
- Click  to modify information of personnel.
- Click  to delete personnel.
- Click  to freeze the card, and then the card cannot be used.
- Click  to configure permissions.

1.4.2 Adding Personnel in Batches

Procedure


- Step 1 Select **Personnel** > **Personnel Management** > **Batch Update** > **Batch Add** .
- Step 2 Select card reader and the department of staff. Set the start number, number of card, effective time and expired time of card.
- Step 3 Click **Read Card No.**, and then the card number will be read automatically.
- Step 4 Click **OK**.

Figure 1-9 Add staff in batches



The 'Batch Add' dialog box contains the following fields and controls:

- Device:** A dropdown menu currently showing 'Card Issuer'. A blue 'Read C...' button is located to its right.
- Start No.:** A text input field containing '5' with a red asterisk icon on the left.
- Quantity:** A text input field containing '10' with a red asterisk icon on the left.
- Department:** A dropdown menu currently showing 'Dropdown list'.
- Validity Time:** A date-time picker showing '2022/11/24 0:00:00'.
- Expiration Time:** A date-time picker showing '2032/11/24 23:59:59'.
- Issue Card:** A section header above a table.
- Table:** A table with two columns: 'ID' and 'Card No.'. The table body is currently empty.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom right.

Step 5 In the list of staff, click  to modify information or add details of staff.

1.4.3 Extracting Personnel Information

Procedure

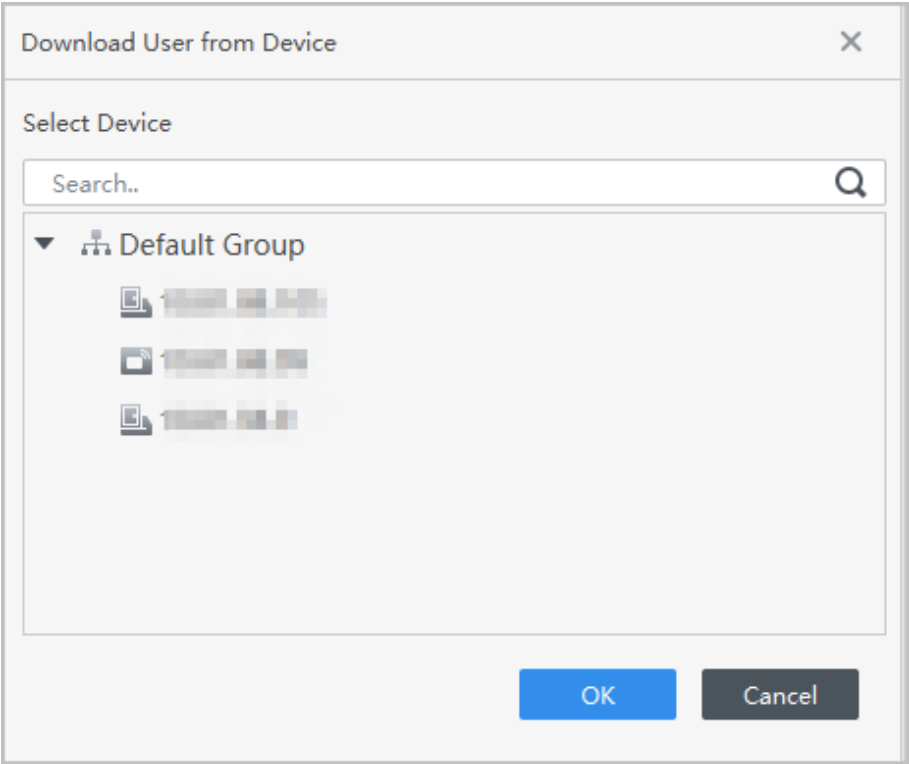
Step 1 Select **Personnel** > **Personnel Management** > **Extract**.

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



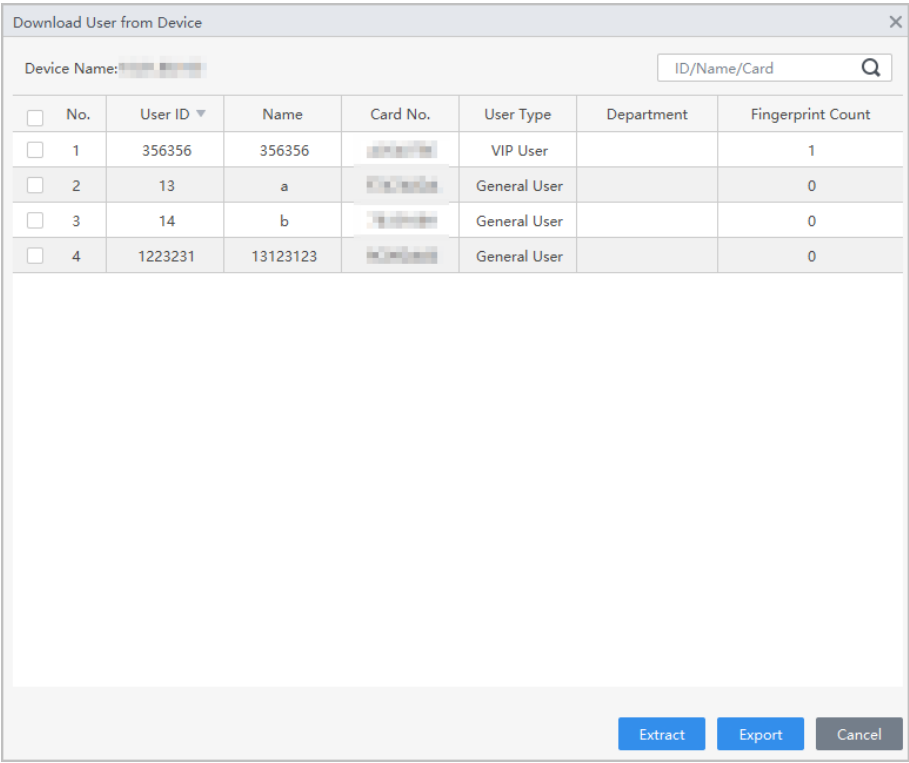
You can select to extract the user of **All**, **Success** or **Failure** from the drop-down list next to **Extract**.


Figure 1-10 Devices with staff information



Step 3 Select the needed staff information, and then click **Extract** to extract the cards to user manager. Click **Export** to export the user information to the computer.

Figure 1-11 Extract users



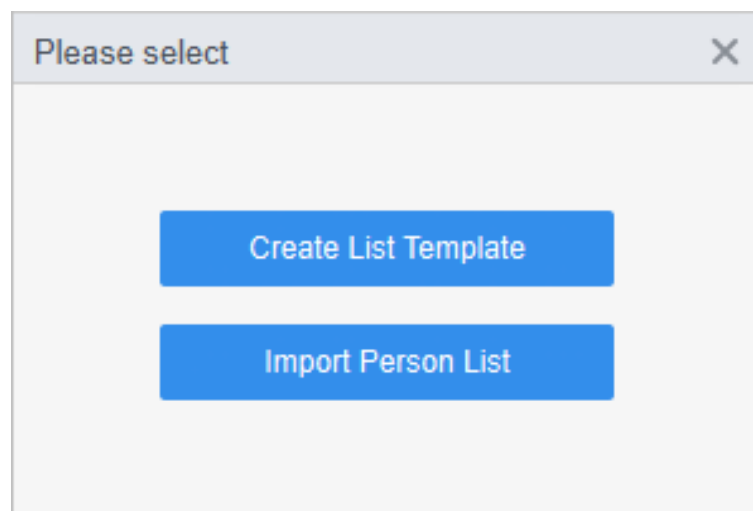
Step 4 In the list of staff, click  to modify information or add details of staff.

1.4.4 Importing Personnel Information

Procedure

- Step 1 Select **Personnel > Personnel Management > Import** .
- Step 2 Import staff information according to instructions.

Figure 1-12 Import staff information



1.5 Issuing Cards in Batches

Issue cards to personnel in batches.

Procedure

- Step 1 Select **Personnel > Personnel Management** .
- Step 2 Select personnel, and then select **Batch Update** .
- Step 3 Issue card in batches. Card number can be read automatically or entered manually.
- Select **Batch Issue Card**, and then select personnel.
 - Select card issuer or card reader device, and then click **Read Card No.**. Make sure a card issuer or a card reader has been connected to your computer.
 - Place the cards on the card reader in sequence.

The card number is read automatically.

Figure 1-13 Issue card in batches

Batch Issue Card

Device:

Card Issuer

Read C...

ID:

1

Name:

1

Card No.:

Press Enter after entering t...

Department:

1

Start Time:

2022-11-23 00:00:00

End Time:

2032-11-23 23:59:59

Card List

User ID	Name	Card No.	Operation
1	1		
2	2		

OK

Cancel

Step 4 Add users in batches.

11

Figure 1-14 Add users in batches

Batch Add

Device

Card Issuer

Read C...

Start No.:

* 2000

Quantity:

* 10

Department:

Default Company

Validity Time:

2023/5/8 0:00:00

Expiration Time:

2023/5/8 23:59:59

Issue Card

ID	Card No.
2000	
2001	
2002	
2003	
2004	
2005	
2006	
2007	
2008	
2009	

OK

Cancel

- Select **Batch Add**.
- Enter the starting user ID and the number of users.
- Select the department.

Users will be generated from the starting user ID.

Step 5 Change department in batches.

Figure 1-15 Change department in batches

The 'Edit' dialog box contains the following fields:

- Department:** A dropdown menu.
- Validity Time:** A checkbox followed by two date/time pickers.
 - to:** 2023-05-08 00:00:00
 - from:** 2023-05-08 23:59:59
- Buttons:** 'OK' (blue) and 'Cancel' (grey).

- Select personnel, and then click **Batch Edit**.
- Select a department.

Department will be changed for the selected personnel.

Step 6 Click **OK**.

1.6 Exporting Personnel Information

Select personnel, and then click **Export** to export personnel information to your local computer.

1.7 Searching for Personnel

Search for personnel according to ID, name or card.

Figure 1-16 Search for personnel

The search bar is a single-line text input with the placeholder text "ID / Name / Card" and a magnifying glass icon on the right side.

1.8 Personnel Display

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



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

Figure 1-17 Card display

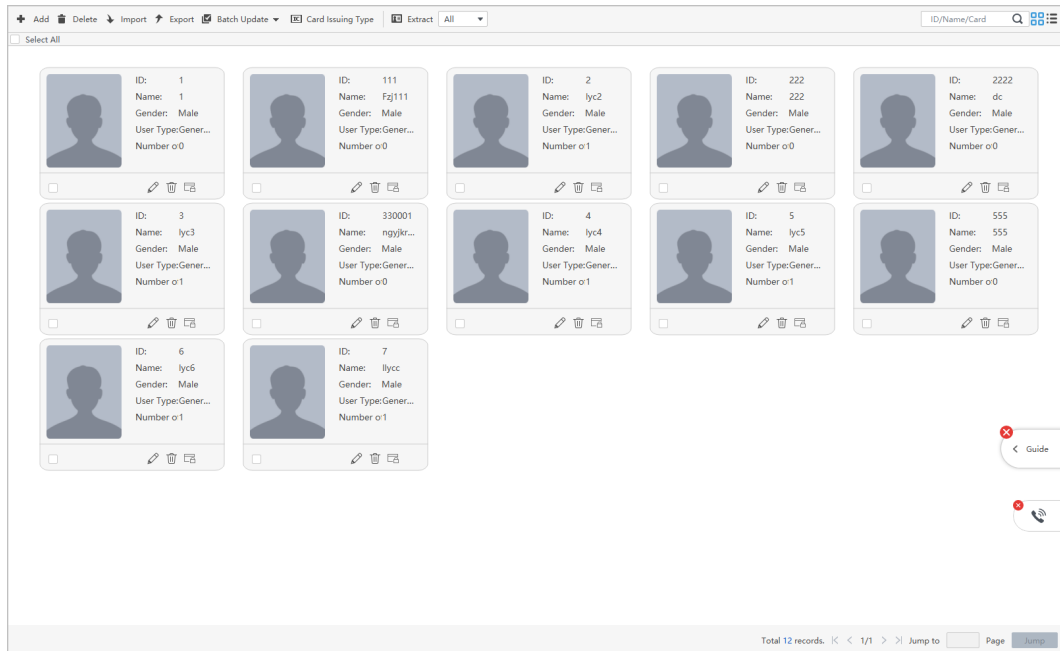


Figure 1-18 List display

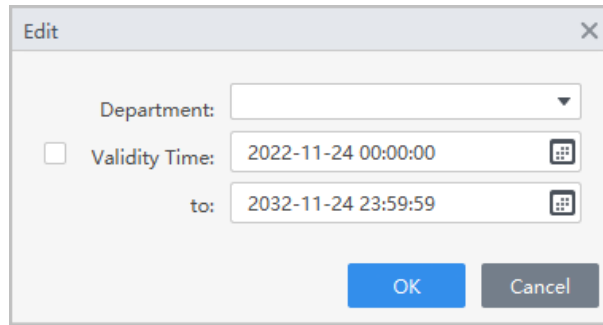
<div> + Add 🗑️ Delete 📁 Import 📤 Export 🔄 Batch Update 📄 Card Issuing Type 📄 Extract All </div> <div>ID/Name/Card 🔍 📄 📄</div>						
<input type="checkbox"/>	Photo	User ID	Name	User Type	Department	Number of Fingerprints
<input type="checkbox"/>		1	1	General User	2	0
<input type="checkbox"/>		111	Fg111	General User	2	0
<input type="checkbox"/>		2	lyc2	General User	01	1
<input type="checkbox"/>		222	222	General User	2	0
<input type="checkbox"/>		2222	dc	General User	2	0
<input type="checkbox"/>		3	lyc3	General User	2	1
<input type="checkbox"/>		330001	ngykrudyt...	General User	2	0
<input type="checkbox"/>		4	lyc4	General User	2	1
<input type="checkbox"/>		5	lyc5	General User	2	1
<input type="checkbox"/>		555	555	General User	2	0
<input type="checkbox"/>		6	lyc6	General User	2	1
<input type="checkbox"/>		7	lycc	General User	2	1

1.9 Editing Personnel in Batches

Select **Personnel** > **Personnel Management** .

Select the needed staff, and then select **Batch Update** > **Batch Edit** to edit department and valid time of users in batches.

Figure 1-19 Edit department



The 'Edit' dialog box contains a 'Department' dropdown menu, a 'Validity Time' section with a checkbox, and two date-time pickers. The 'Validity Time' checkbox is unchecked. The first date-time picker is set to '2022-11-24 00:00:00' and the second is set to '2032-11-24 23:59:59'. At the bottom are 'OK' and 'Cancel' buttons.

1.10 Permission Configuration

1.10.1 Adding Permission Groups

Procedure

Step 1 Select **Personnel** > **Permission Configuration** .

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

Step 3 Set permission parameters.

1. Enter group name and remark.
2. Select the needed time template.



For details on time template setting, see *SmartPSS-Lite_Access Control Solution_User's Manual*.

3. Select the verification method.
4. Select the corresponding device, such as door 1.

Figure 1-20 Add permission group (1)












<div><div><div>+</div><div>🗑️</div></div><div>Search.. 🔍</div></div>		
<input type="checkbox"/>	Permission Group	Operation
<input type="checkbox"/>	Permission Group1	  
<input type="checkbox"/>	Permission Group2	  
<input type="checkbox"/>	Permission Group3	  

Figure 1-21 Add permission group (2)

The screenshot shows the 'Add Permission Group' dialog box. It includes a 'Basic Info' section with input fields for 'Group Name' (filled with 'Permission Group4'), 'Remark', and 'Time Templ...' (set to 'All Day Time Ten'). Below this is a 'Verification Method' section with four checked checkboxes: 'Card', 'Fingerprint', 'Password', and 'Face'. At the bottom left, there is a tree view under the heading 'All Device' with a search bar. The tree shows 'Default Group' expanded, revealing a sub-item and 'Door 1'. To the right of the tree is a 'Selected (0)' area. At the bottom right are 'OK' and 'Cancel' buttons.

Step 4 Click **OK** to save operations.

Related Operations


- Click  to delete group.
- Click  to modify group information.
- Double-click permission group name to view group information.

1.10.2 Configuring Permissions

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

Procedure

Step 1 Select **Personnel** > **Permission Configuration**.

Step 2 Click , and then select the department to be configured permission.

Step 3 Click **OK**.

Figure 1-22 Configure permission

Add Person

Permission Group1

User List

Search..

1(2)

01(1)

1

Selected (2)

ID

Name

2

2

1

1

OK

Cancel





Step 4 (Optional) Click  in the left navigation bar to view the authorization progress.
If authorization failed, click  in the list to view the possible reason.

Figure 1-23 Authorization progress


Permission Group	Device Name	Progress	Status	Result of Issuing	Operation
Permission Group1		<div><div>1/1</div></div>	Error issuing	Successful: 0, Failed: 1	

17

2 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.

2.1 Building Manager

Create a community organization. You can add buildings, units to it.

Prerequisites

The level of the organization was configured. For details, see "4.1 Basic Settings" in the user's manual of SmartPSS Lite. This section uses how to create the organization at the unit level as an example.

Procedure

- Step 1 Open the **Video Intercom** solution.
- Step 2 Click **Intercom Management** > **Building Manager**.
- Step 3 Add buildings under the community level.


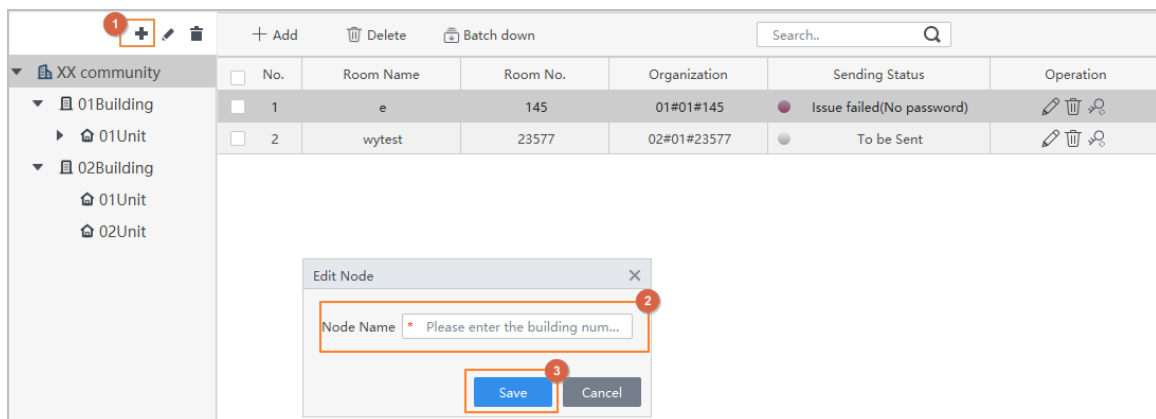
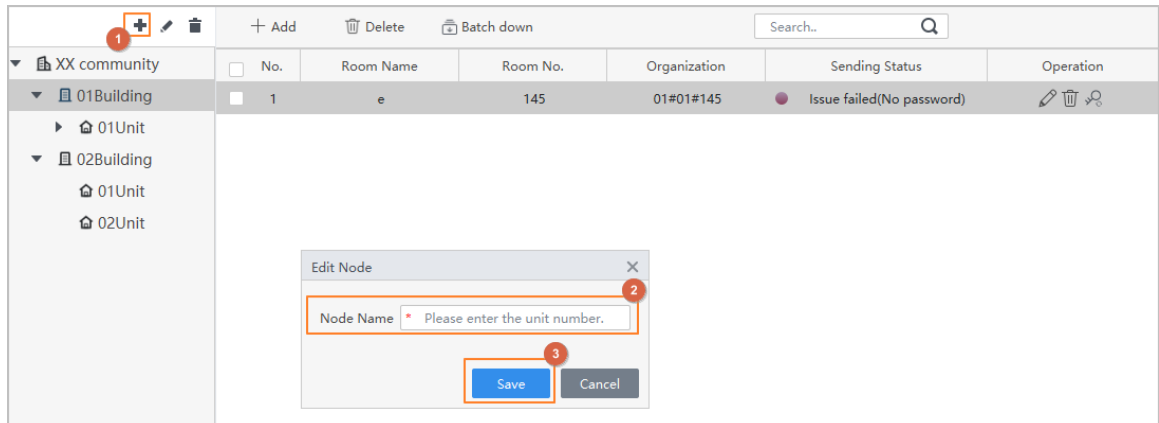
You can click  to edit the name of the community.

Figure 2-1 Add buildings



- Step 4 Add units under the building level.

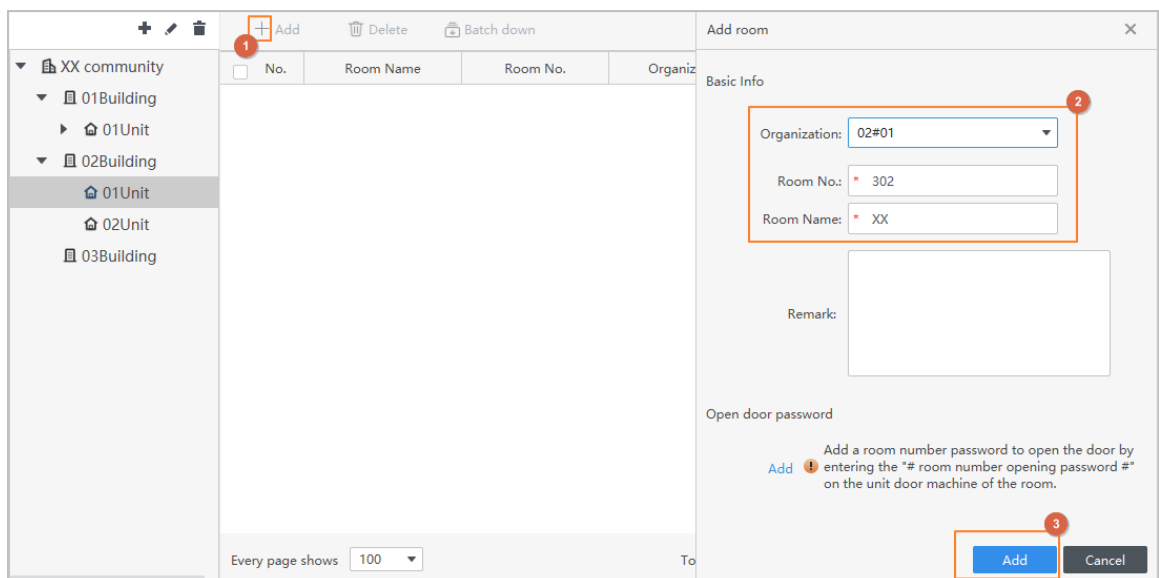
Figure 2-2 Add units



Step 5 Add rooms under the unit level.

- Click **Add**.
- Select a unit from the organization.
- Enter the number of the room and the name of the room.
- If you want to control access by entering the room password in the VTH, you can configure an unlock password. For details, see "2.3 Configuring Unlocking Through Password".
- Click **Add**.

Figure 2-3 Add rooms



Results

The organization is created.


- **Organization:** Displays the exact organization level of the room. For example, 02#01#302 means building 02, 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 2-4 Created organization

<div> <div> <div></div> <div></div> <div></div> </div> <div> <div>+ Add</div> <div>Delete</div> <div>Batch down</div> </div> <div> <div>Search..</div> <div></div> </div> </div>						
<div> <div>XX community</div> <div> <div>01Building</div> <div>01Unit</div> <div>02Building</div> <div>01Unit</div> <div>02Unit</div> <div>03Building</div> </div> </div>	No.	Room Name	Room No.	Organization	Sending Status	Operation
	1	XX	302	02#01#302	To be Sent	<div> <div></div> <div></div> <div></div> </div>

2.2 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 “2.1 Building Manager”.

Procedure

- Step 1 Open the **Video Intercom** solution.
- Step 2 Click **Intercom Config > Dial Management**.
- Step 3 Add registration number for VTH.
 - a. Click **Add**.
 - b. Select a VTH from the drop-down list.
 - c. Select the organization.



If you have added units to the organization, you can only select a unit.

- d. Select a room from the list, and then enter the number of the extension if there are more than one VTH in the room.
- e. 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 2-5 Add registration number for VTH

The 'Add Device' dialog box is shown with the following fields and callouts:

- 1**: '+ Add' button in the top left.
- 2**: 'Device Name' dropdown menu.
- 3**: 'Select Organization' dropdown menu showing a tree structure: '11#01' (selected), 'Default Area', '11Building', and '01Unit'.
- 4**: 'Select room number' input field with a dropdown for '11' and a text input for '5'.
- 5**: 'Add' button at the bottom right.

Other fields in the dialog include: IP (10.81.88.109), Device Type (VTH), SIP Server Port (5080), SIP Registration No. (11#01#11#5), SIP Server IP (10.3...3.88), SIP Registration Password (*****), and Port (37777).

Step 4 Add registration number for VTO.

- Click **Add**.
- Select a VTO from the drop-down list.
- Select the organization.



If you have added units in the organization, you can only select a unit.

- 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.

- Click **Add**.

The registration number is automatically generated. For example, 11#01#8055 means building 11, unit 01 and the number of VTO is 8055.

Figure 2-6 Add registration number for VTO

The 'Add Device' dialog box is shown with the following fields and callouts:

- 1**: '+ Add' button in the top left.
- 2**: 'Device Name' dropdown menu.
- 3**: 'Select Organization' dropdown menu showing a tree structure: '11#01' (selected), 'Default Area', '11Building', and '01Unit'.
- 4**: 'Please enter a 2-digit number, for exam...' input field.
- 5**: 'Add' button at the bottom right.

Other fields in the dialog include: IP (10.81.88.107), Device Type (VTO), SIP Server Port (5080), SIP Registration No. (11#01#8055), SIP Server IP (10.3...3.88), SIP Registration Password (*****), and Port (37777).

Step 5 Add registration number for VTS.

- a. Click **Add**.
- b. Select a VTS from the drop-down list.
- c. 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.

- d. Click **Add**.

The registration number is automatically generated.

Figure 2-7 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.

2.3 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 “2.1 Building Manager”.
- VTH and VTO were registered. For details, see “2.2 Dial Management”.

Procedure

- Step 1 Open the **Video Intercom** solution.
- Step 2 Click **Intercom Management** > **Building Manager**.
- Step 3 Select a room, and then click to add a unlock password.
 - a. Click **Add**.
 - b. Enter and confirm password.

c. Click **OK**.

Figure 2-8 Configure unlock password

Basic Info

Organization: 11#01#11

Room No.: * 11

Room Name: * test

Remark:

Open door password

Add ! Add a room number password to open the door by entering the "# room number opening password #" on the unit door machine of 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 4 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.

2.4 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 2-9 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 2-10 List of Selected Devices


List of Selected Devices	
Selected Dev	Operation
	  
Client	  
<div></div>	

OK

Cancel

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.

2.5 Information Release

Background Information

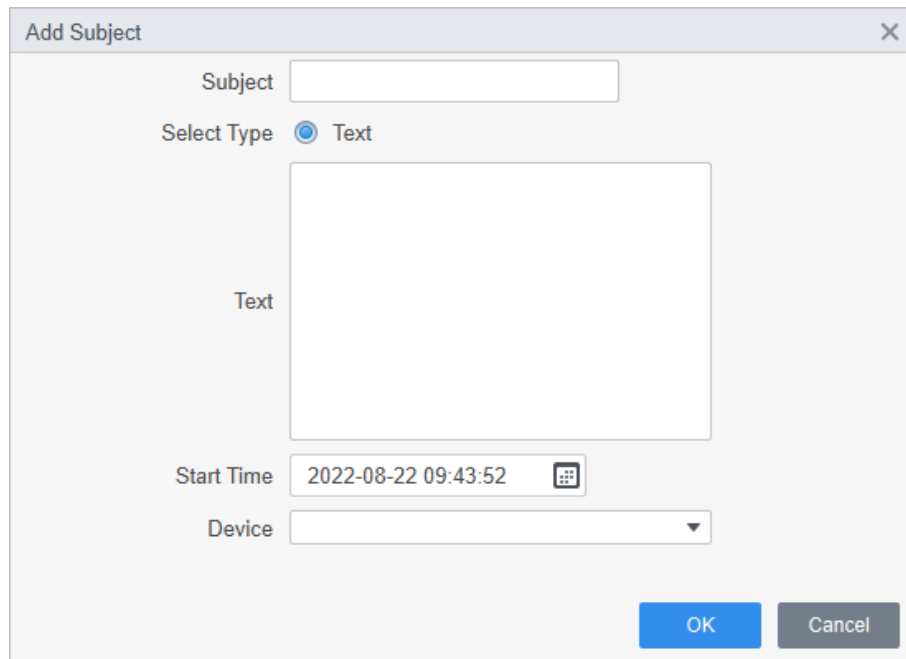


This function is only supported by the devices whose device type is VTO or VTH and whose numbers are bound to the Platform.

Procedure

- Step 1** Open the **Video Intercom** solution.
- Step 2** Select **Intercom Config > Information release**.
- Step 3** Click **Add** to add the subject.
- Step 4** Enter the topic text, and then set the **Start Time**.
- Step 5** Select the device from the drop-down list, and then click **OK**.

Figure 2-11 Add topic



The 'Add Subject' dialog box contains the following fields and controls:

- Subject:** A text input field.
- Select Type:** A radio button labeled 'Text' is selected.
- Text:** A large text area for entering the subject content.
- Start Time:** A date and time picker showing '2022-08-22 09:43:52'.
- Device:** A dropdown menu.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom right.

Step 6 View the added subject.





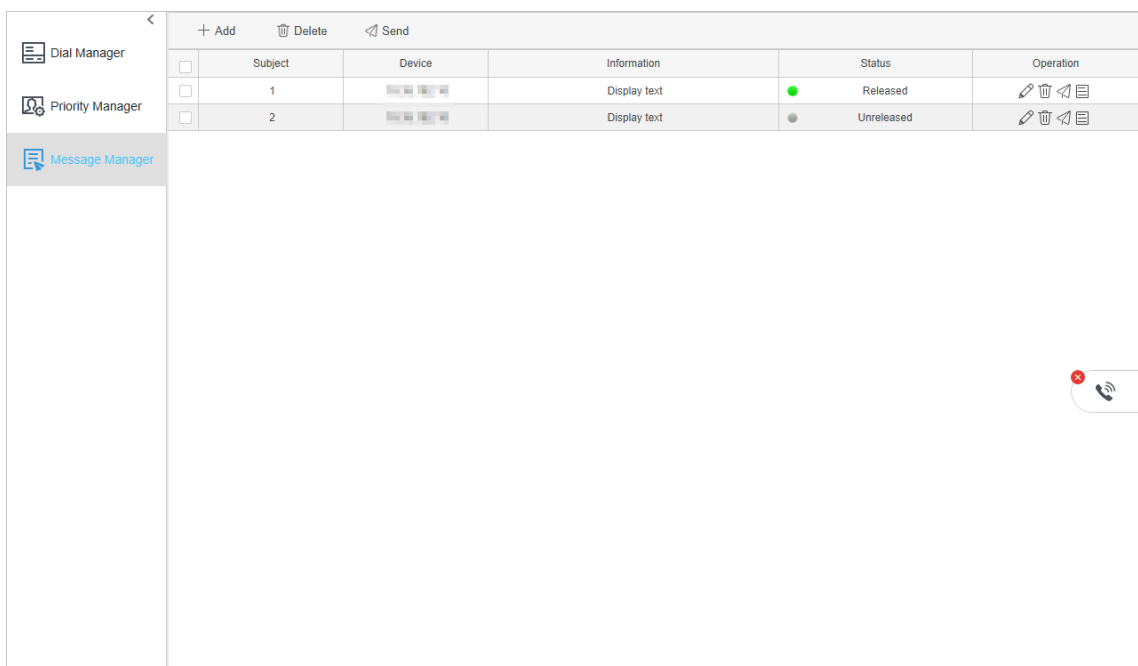










- Click  to modify the added subject.
- Click  corresponding to the theme, or select the subject to be deleted, and then click **Delete** to delete the subject.
- Click  corresponding to the subject, or select the subject to be sent, and then click **Send** to send the subject to the device.
- Click  to view the details of the released topic.

Figure 2-12 View the added subject



The interface shows a sidebar with 'Dial Manager', 'Priority Manager', and 'Message Manager' (selected). The main area displays a table of subjects.

	Subject	Device	Information	Status	Operation
<input type="checkbox"/>	1		Display text	● Released	   
<input type="checkbox"/>	2		Display text	● Unreleased	   

At the bottom right, there is a red 'X' icon and a speaker icon.

3 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 “2.2 Dial Management”.

Procedure

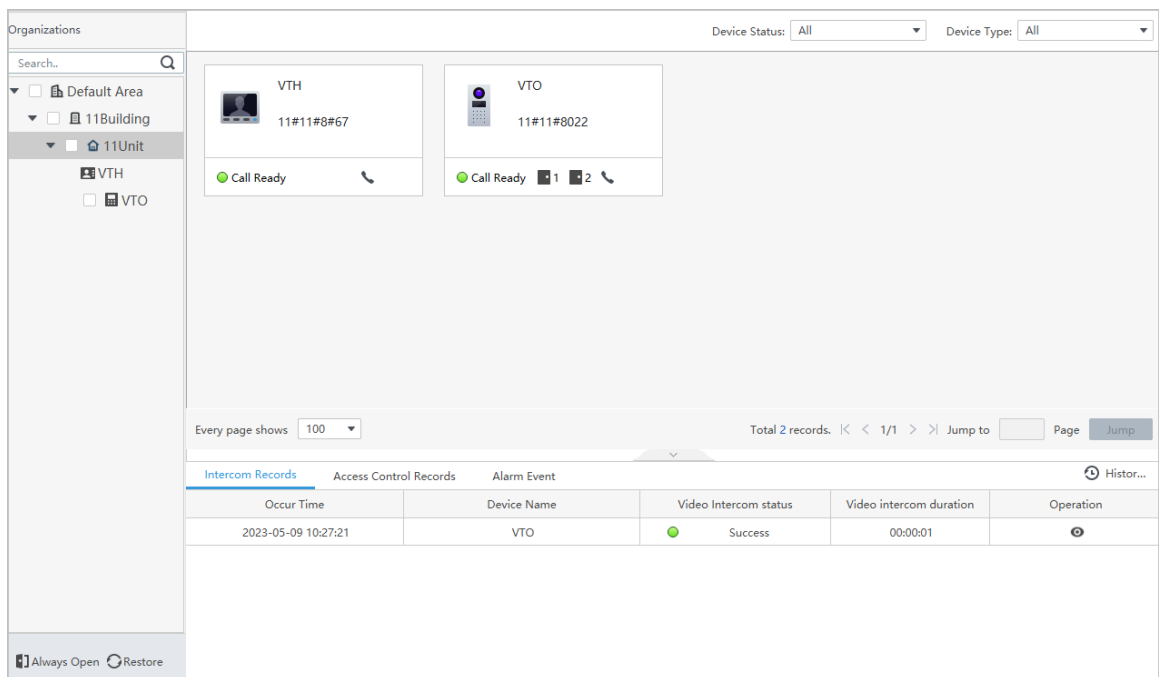
Step 1 Open the **Video Intercom** solution.




Step 2 Click **Intercom Management** on the home page, and then select the intercom device in the organization tree.

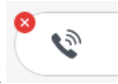


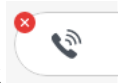
The organization tree is displayed at the unit level by default.

Figure 3-1 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.
- Call Ready: You can make a video call. Click  on the bottom of the device.
- 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.
 - a. Click the floating window to accept the call and enter the video intercom page.
 - b. 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.



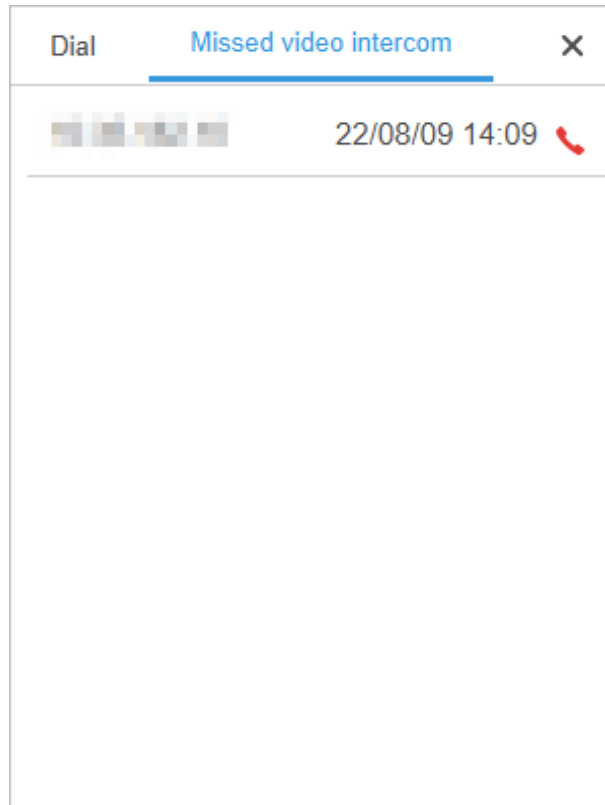
The dial page only supports full number calls, the room number calls are not supported; if you want to call VTH, you need to enter the number and the extension number.

Figure 3-2 Dial page



The screenshot shows a mobile application interface for dialing. At the top, there are two tabs: 'Dial' (active) and 'Missed video intercom'. To the right of the tabs is a close button 'X'. Below the tabs is a text input field containing the number '01018001'. To the right of the input field is a clear button 'X'. Below the input field is a numeric keypad (0-9) and a QWERTY keyboard. At the bottom is a large green button with a white telephone handset icon.

Click **Missed video intercom** to view the missed video intercom call.

Figure 3-3 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 3 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 3-4 Video intercom page

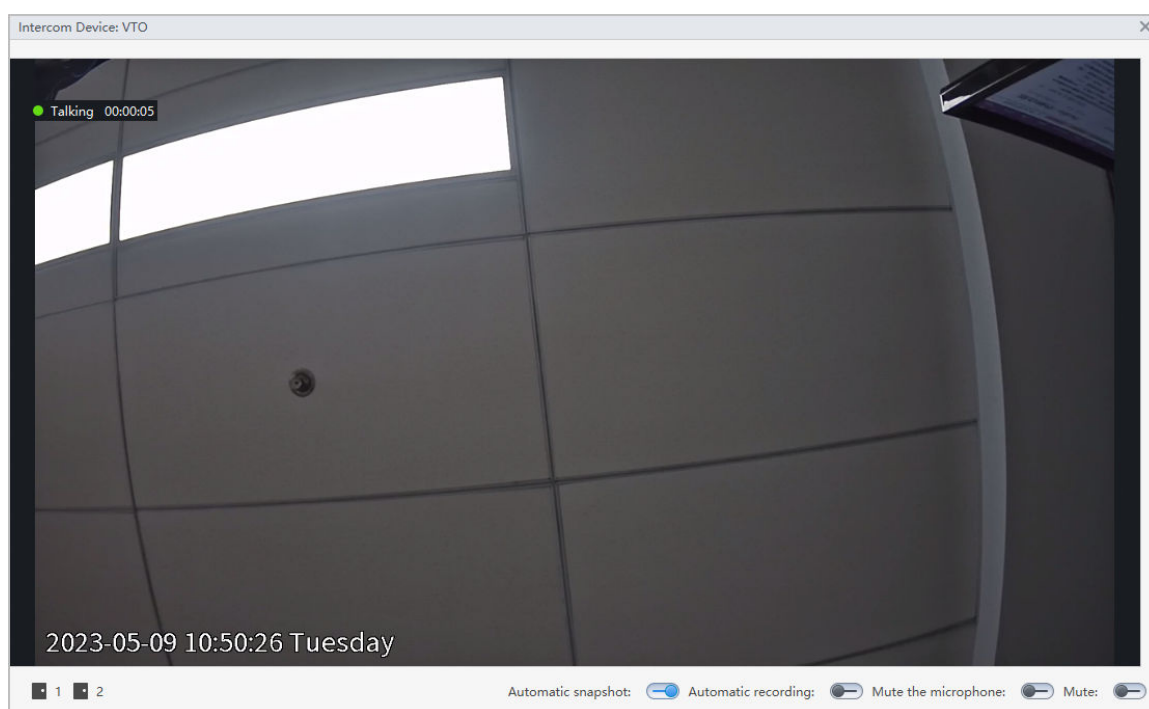






Table 3-1 Description of video intercom page parameters

Parameter	Description
	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	<p>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.</p> <p></p> <p>Only one recording can be retained for per call.</p>
Mute the microphone	After enabling, your microphone will be muted.
Mute	After enabling, the device microphone will be muted.

Step 4 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.

4 Intercom Records

You can filter, export and search for call records, access control records and alarm records.

4.1 Intercom Records Query

You can view and export the call record.

Prerequisites

Make sure that the video intercom device added to the Platform has an intercom event.

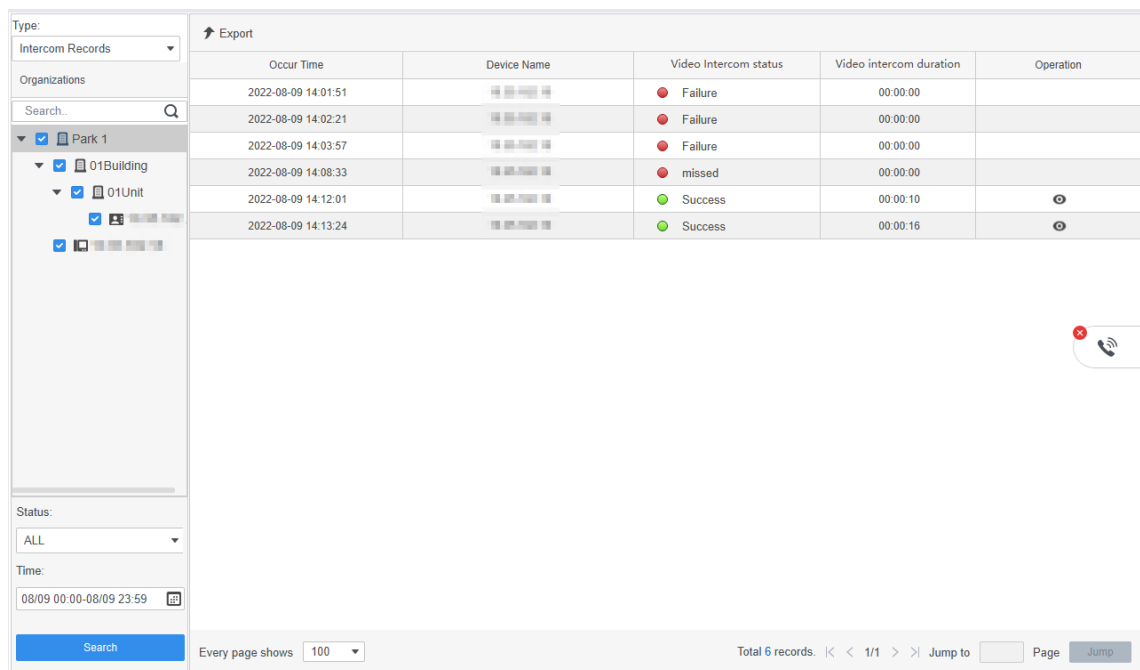
Procedure



- Step 1** Open the **Video Intercom** solution.
- Step 2** Select the **Type** as the **Intercom Records**.
- Step 3** Select the device in the organization tree, and then set the status and time period.
- Step 4** Click **Search**.



Click  to view the pictures and videos saved during the video intercom call.

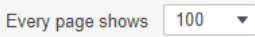




Figure 4-1 View call records



Occur Time	Device Name	Video Intercom status	Video intercom duration	Operation
2022-08-09 14:01:51		Failure	00:00:00	
2022-08-09 14:02:21		Failure	00:00:00	
2022-08-09 14:03:57		Failure	00:00:00	
2022-08-09 14:08:33		missed	00:00:00	
2022-08-09 14:12:01		Success	00:00:10	
2022-08-09 14:13:24		Success	00:00:16	

- Step 5** Click **Export** to export all the call records to the computer.

Related Operations

- Click  to select the number of information showed on every page.
- Click  /  to view the previous page or next page.
- Click  /  to go to the first page or last page.

- Enter the page number in **Jump to** **Page**, and then click **Jump** to jump to the specified page.

4.2 Access Control Records Query

You can view and export records of door opening and closing events.

Prerequisites

Make sure that the video intercom device added to the Platform has an access control event.

Procedure

- Step 1** Open the **Video Intercom** solution.
- Step 2** Select the **Type** as the **Access Control Records**.
- Step 3** Select the device in the organization tree, and then set the time period.
- Step 4** Click **Search**.

Figure 4-2 View access control records

Time	User ID	Name	Card No.	Device	Event	Authentication Method	Access direction
2022-08-09 14:24:55					Close Door		
2022-08-09 14:24:50					Remotely Unl...		
2022-08-09 14:24:50					Open Door		
2022-08-09 14:24:50					Open Door		
2022-08-09 14:24:50					Remotely Unl...		
2022-08-09 14:24:48					Remotely Unl...		
2022-08-09 14:24:48					Open Door		
2022-08-09 14:24:38					Close Door		
2022-08-09 14:24:33					Open Door		
2022-08-09 14:24:33					Remotely Unl...		

- Step 5** Click **Export** to export all the access control records to the computer.

Related Operations

- Click **Every page shows** to select the number of information showed on every page.
- Click / to view the previous page or next page.
- Click / to go to the first page or last page.
- Enter the page number in **Jump to** **Page**, and then click **Jump** to jump to the specified page.

4.3 Alarm Record Query

You can view and export the alarm event records.

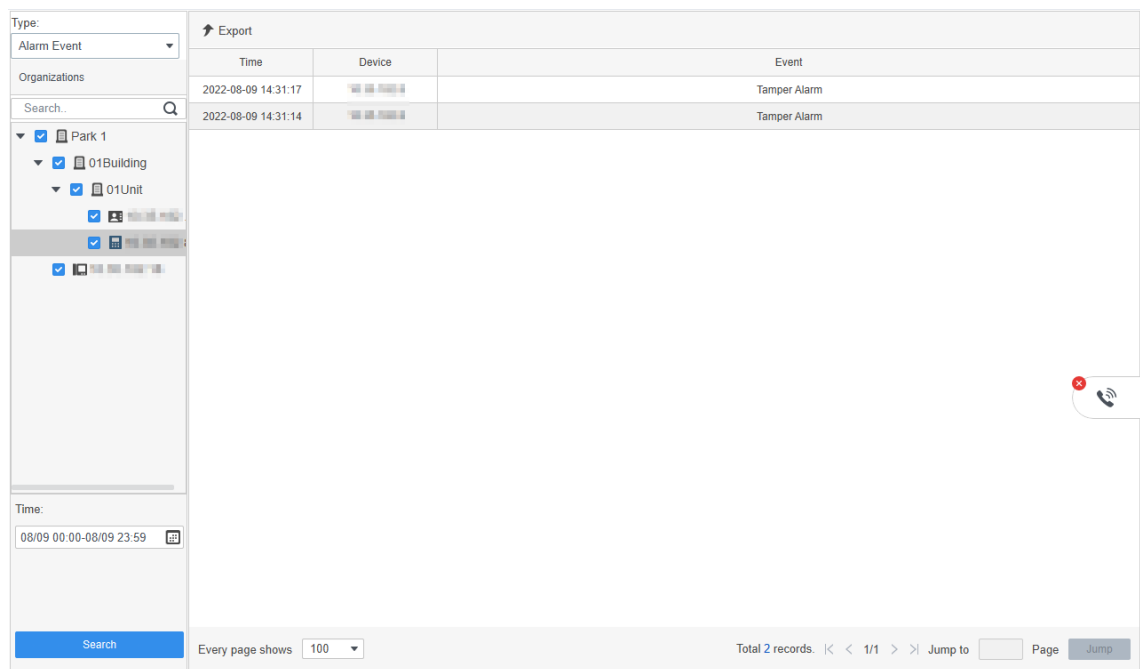
Prerequisites

Make sure that the video intercom device added to the Platform has an alarm event.

Procedure





- Step 1 Open the **Video Intercom** solution.
- Step 2 Select the **Type** as the **Alarm Event**.
- Step 3 Select the device in the organization tree, and then set the time period.
- Step 4 Click **Search**.

Figure 4-3 View alarm records



- Step 5 Click **Export** to export all the alarm records to the computer.

Related Operations

- Click **Every page shows** to select the number of information showed on every page.
- Click  /  to view the previous page or next page.
- Click  /  to go to the first page or last page.
- Enter the page number in **Jump to** **Page**, and then click **Jump** to jump to the specified page.

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.