

SmartPSS Lite Access Control Solution

User's Manual








Foreword

General

This manual introduces the functions and operations of the access control solution of the SmartPSS Lite platform (hereinafter referred to as "the Platform"). Read carefully before using the platform, and keep the manual safe for future reference.

Safety Instructions

The following signal words might appear in the manual.

Signal Words	Meaning
 DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
 WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
 CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, reductions in performance, or unpredictable results.
 TIPS	Provides methods to help you solve a problem or save time.
 NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.1.0	<ul style="list-style-type: none">Updated person management function.Updated access controller configuration function.	December 2022
V1.0.1	Updated staff display image.	August 2022
V1.0.0	First release.	April 2022

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, 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 Overview	1
2 Access Guide	2
3 Personnel Management	3
3.1 Adding Company	3
3.2 Department Management	3
3.3 Staff Management	4
3.3.1 Setting Card Type	4
3.3.2 Adding Staff	5
3.3.2.1 Adding Staff One by One Manually	5
3.3.2.2 Adding Staff in Batches	8
3.3.2.3 Extracting Staff Information from Other Devices	10
3.3.2.4 Importing Staff Information from Local Storage	11
3.3.3 Issuing Cards in Batches	11
3.3.4 Exporting Staff Information	13
3.3.5 Searching for Staff	13
3.3.6 Staff Display	13
3.3.7 Editing Staff in Batch	14
3.4 Permission Configuration	14
3.4.1 Adding Permission Group	14
3.4.2 Configuring Permission	16
4 Time Template Setting	17
5 Advanced Functions Configuration	20
5.1 First Card Unlock	20
5.2 Multi Card Unlock	21
5.3 Anti-passback	24
5.4 Inter-door Lock	25
6 Access Controller Configuration	27
7 Viewing Historical Event	29
8 Access Manager	31
8.1 Remotely Opening and Closing Door	31
8.2 Setting Always Open and Always Close	32
8.3 Resetting Door Status	32
8.4 Setting Access Point	33
8.5 Viewing Access Control Video	33

8.5.1 Viewing Single Access Control Video	34
8.5.2 Viewing Multiple Access Control Videos	34
8.6 Starting Real-time Event Monitoring	35
8.7 Rebooting Access Controller	35
8.8 Viewing Access Control Details	36

1 Overview

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

2 Access Guide

You can quickly use the common functions of access control here.

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

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

Step 3 Configure functions in the order from top to bottom and from left to right. For details about how to use these functions, see the corresponding chapters.

Figure 2-1 Access guide

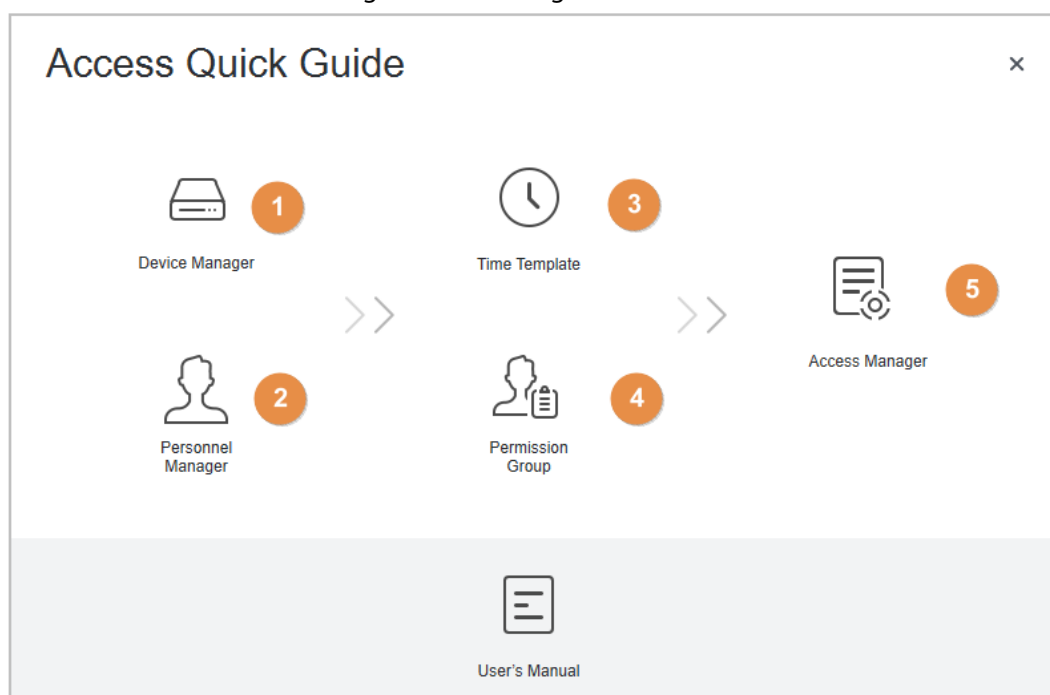


Table 2-1 Functions of access guide

Functions	Description
Device Manager	For details, see <i>SmartPSS Lite_General_User's Manual</i> .
Personnel Manager	For details, see "3 Personnel Management".
Time Template	You can set time template, configure parameters of anti-pass back, configure access controller and view historical event.
Permission Group	For details, see "3.4 Permission Configuration".
Access Manger	You can control door remotely. For details, see "8 Access Manager".

3 Personnel Management

You can manage department information and staff information.

3.1 Adding Company

- 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 3-1 Add company

Company: * 1

Fax:

Email:

Tel:

Website:

Postal Code:

Address 1:

Address 2:

LOGO

Image Size: 0-100 KB

OK Cancel

3.2 Department Management

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

Procedure

- Step 1 Select **Personnel > User 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 3-2 Add department

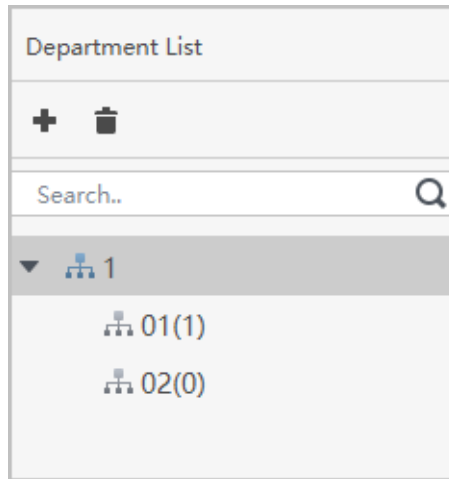
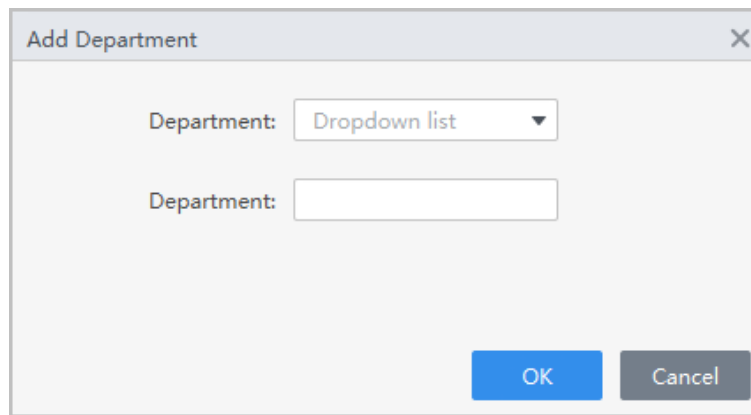




Figure 3-3 Add department information



Related Operations

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

3.3 Staff Management

You can add personnel information, issue cards, export personnel information to local, and freeze cards.

3.3.1 Setting Card Type

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

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




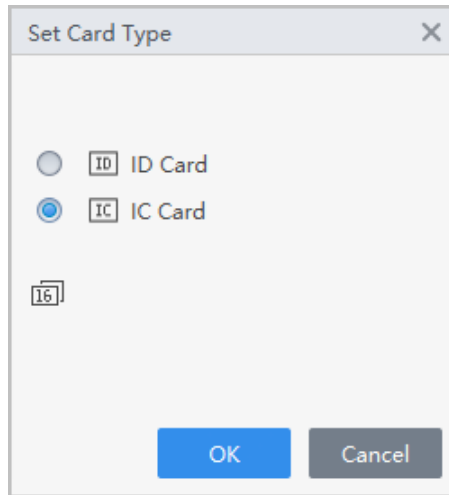
- The system uses hexadecimal card number by default. Click  to change to decimal card number.
- When the card number type is changed, the card number in the **Access Manger**, user's card, and **History Event** will also be changed.

Figure 3-4 Set card type



3.3.2 Adding Staff

Select one of the methods to add staff.

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

3.3.2.1 Adding Staff One by One Manually


Procedure


Step 1 Select **Personnel > User Management > Add**.

Step 2 Enter basic information of staff.

- 1) Select **Basic Info**.
- 2) Add basic information of staff.
- 3) Take snapshot or upload picture, and then click **Finish**.



- The card number can be read automatically or filled in manually. To automatically read card number, select the card reader next to **Card No.**, and then place the card on the card reader. The card number will be read automatically.
- You can select multiple USB cameras to snap pictures.
- 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
 1. Click  to select **Device** or **Card issuer** as card reader.
 2. Add card. The card number must be added if the non-second generation access controller is used.
 3. 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.

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

Figure 3-5 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 Select **Personnel > User Management > Add > Certification** to add extended information of the staff, and then click **Finish** to save.

Figure 3-6 Add extended information

The screenshot shows a software window titled 'Add User' with a close button (X) in the top right corner. It contains three tabs: 'Basic Info', 'Extended information' (which is selected), and 'Permission'. Below the tabs is a 'Details' section. The 'Extended information' tab contains the following fields and controls:

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

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

Step 4 Configure permissions.

Permission group is a combination of all devices supported by various solutions. After selecting the permission group, the personnel info will be sent to corresponding device and used for related functions of access control and attendance check.

Figure 3-7 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 5 Click **Finish**.



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

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.
- Click  to display the **Permission Configuration** page.

3.3.2.2 Adding Staff in Batches

Step 1 Select **Personnel > User 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 3-8 Add staff in batches

Batch Add

Device

Card Issuer

Read C...

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.
----	----------

OK

Cancel

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

3.3.2.3 Extracting Staff Information from Other Devices

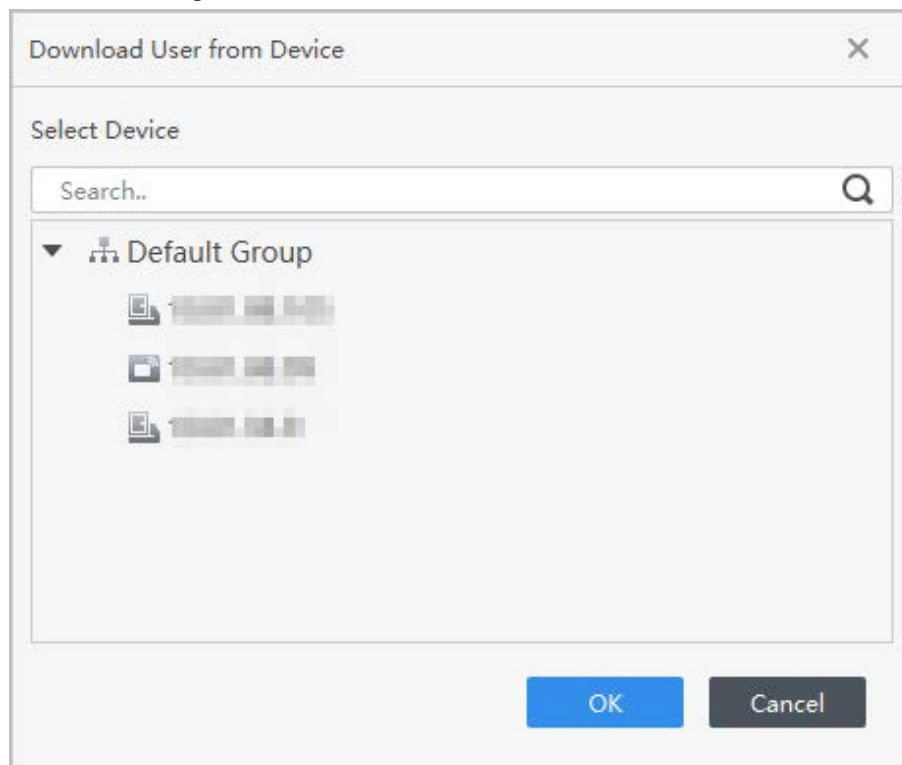
Step 1 Select **Personnel > User Management > Extract**.

Step 2 Select the needed 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 3-9 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 3-10 Extract users

The screenshot shows a window titled "Download User from Device" with a close button (X) in the top right corner. Below the title bar, there is a "Device Name:" label followed by a text input field containing "ID/Name/Card" and a search icon (magnifying glass). Below this is a table with the following columns: No., User ID, Name, Card No., User Type, Department, and Fingerprint Count. The table contains four rows of data. Below the table is a large empty rectangular area. At the bottom right of the window are three buttons: "Extract" (blue), "Export" (blue), and "Cancel" (grey).

<input type="checkbox"/>	No.	User ID	Name	Card No.	User Type	Department	Fingerprint Count
<input type="checkbox"/>	1	356356	356356		VIP User		1
<input type="checkbox"/>	2	13	a		General User		0
<input type="checkbox"/>	3	14	b		General User		0
<input type="checkbox"/>	4	1223231	13123123		General User		0

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

3.3.2.4 Importing Staff Information from Local Storage

Step 1 Click **Personnel > User > Import**.

Step 2 Import staff information according to instructions.

Figure 3-11 Import staff information

The screenshot shows a dialog box titled "Please select" with a close button (X) in the top right corner. Inside the dialog box, there are two blue buttons stacked vertically: "Create List Template" and "Import Person List".

3.3.3 Issuing Cards in Batches

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

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

Step 2 Select the needed staff, and then select **Batch Update > Batch Issue Card**.

Step 3 Issue card in batches. Card No. can be read automatically by card reader or entered

manually.

- Read automatically
 1. Select card reading device, and then click **Read Card No.**
 2. According to the order list, put the cards of the corresponding staff on card reader in sequence, and then the SmartPSS Lite will automatically read the card No..
 3. Modify staff information, such as start time and end time for card validation.
- Enter manually
 1. Select the staff in card list, and then enter the corresponding card No..
 2. Modify staff information, such as start time and end time for card validation.

Figure 3-12 Issue card in batches

Batch Issue Card

Device:
Card Issuer

Read C...

ID:
1

Name:
1

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

Department:
2

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	lyc2		
3	lyc3		
330001	ngyjkrudu...		
4	lyc4		
5	lyc5		
6	lyc6		

OK

Cancel

Step 4 Click **OK**.

3.3.4 Exporting Staff Information

Select the staff information which needs to be exported, and then click **Export** to export all staff information to local.

3.3.5 Searching for Staff

Search for staff who meet the conditions, according to ID, name or card.

Figure 3-13 Search for staff

ID / Name / Card

3.3.6 Staff Display

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

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

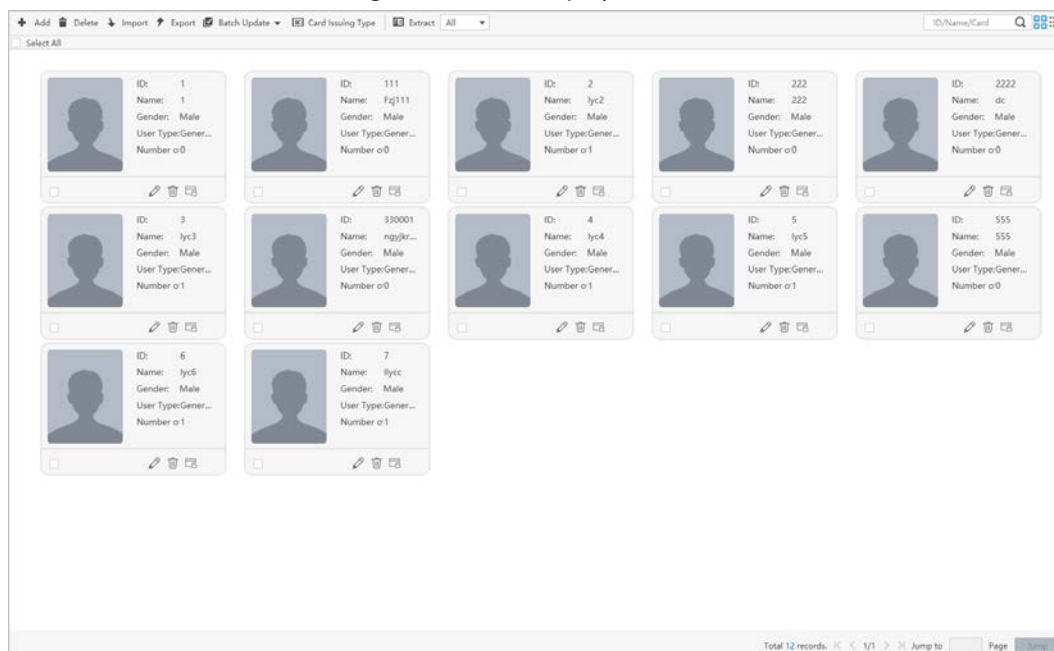
Figure 3-14 Card display

<div><div><div> Add</div><div> Delete</div><div> Import</div><div> Export</div><div> Batch Update</div><div> Card Issuing Type</div><div> Extract</div><div>All</div></div></div> <div>ID/Name/Card</div> <div></div> <div></div> <div></div>

Every page shows: 20

Total 12 records. < 1/1 > Jump to Page

Figure 3-15 List display



3.3.7 Editing Staff in Batch

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

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

Figure 3-16 Edit department

3.4 Permission Configuration

3.4.1 Adding Permission Group

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.

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

Step 5 (Optional) Click  to delete group.

Step 6 (Optional) Click  to modify group information.

Step 7 (Optional) Double-click permission group name to view group information.

Figure 3-17 Add permission group (1)













<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 3-18 Add permission group (2)

Add Permission Group

Basic Info

Group Name
Permission Group4

Remark:

Time Templ... All Day Time Ten


Verification Method: ☒ Card ☒ Fingerprint ☒ Password ☒ Face


All Device


Selected (2)

Search..

Default Group

☐  Door 1

☐  Door 2

☒  Door 1

10.81.88.99

10.81.94.9-Door 1

OK

Cancel

3.4.2 Configuring Permission

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


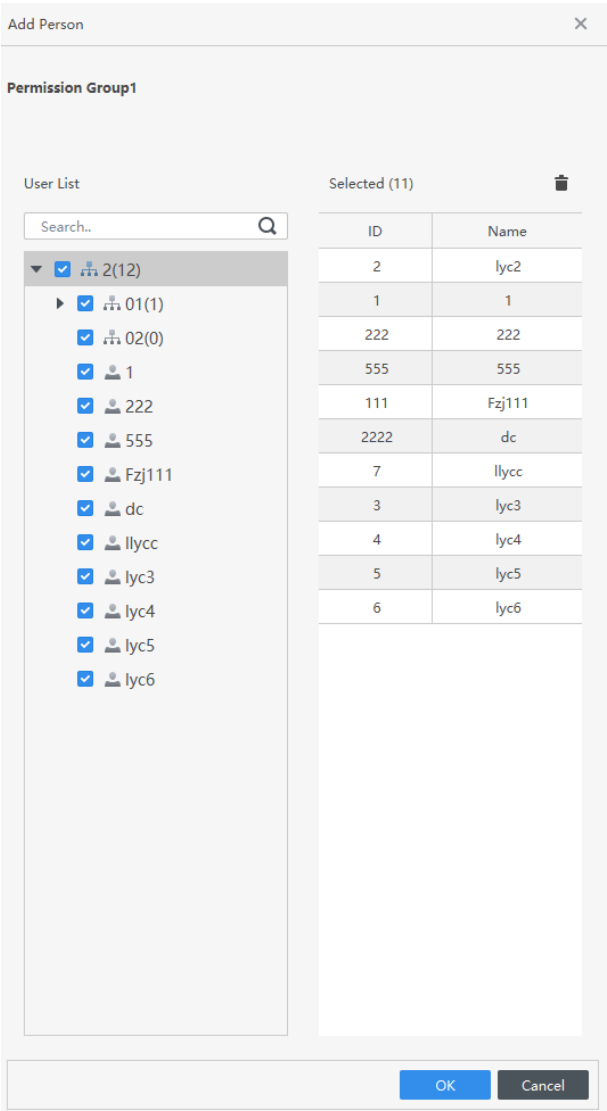
- Step 1 Select **Personnel** > **Permission Configuration**.
- Step 2 Click , and then select the department to be configured permission.
- Step 3 Click **OK**.

Figure 3-19 Configure permission







- 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 3-20 Authorization progress


Permission Group	Device Name	Progress	Status	Result of Issuing	Operation
Permission Group3		<div><div></div></div> 1/1	Finished Issuing	Successful: 1, Failed: 0	

4 Time Template Setting

Time template is to configure the working hours of access controllers, such as when to open and when to close. SmartPSS Lite provides 4 time templates by default. You can set new time templates as needed.



The default templates cannot be modified.

Step 1 Click **Access Configuration** on the home page. (You can also select **Access Guide** >  on the home page.)

Step 2 Click **Add**.

Step 3 Set time template.



- When the week plan and the holiday plan are in conflict, the holiday plan has higher priority.
 - After the time template is configured, assign the permission in **Personnel Manager** > **Permission Configuration** when selecting time template.
- 1) Enter **Template Name** and description note.
 - 2) Click **Week Plan** to set week plan to allow personnel to pass through during specified periods from Monday to Sunday. You can add up to 4 needed time periods for each day.

There are two methods.



- Method 1: Move the cursor to the period area. When cursor is , click the periods that are not needed, and the periods become gray. During these periods, personnel are not allowed to pass through. When cursor is , click the needed periods, and the periods become green. Personnel are allowed to pass through during these periods. Click **Save**.

Figure 4-1 Set week plan (method 1)


- Method 2: Click  to the right of the time bar, and set time period. You can apply the set time period to other days. Click **OK**, and then **Save**.

Figure 4-2 Set week plan (method 2)


- 3) (Optional) Click  to recycle the week plan.
- 4) Click **Holiday Plan** to set holiday plan. Set the time periods; click **Add**, enter the holiday information on the right side of the page, and then click **OK**.
- 5) Select the needed holiday in the **Holiday List**, and then click **OK**.

Figure 4-3 Set holiday plan (1)

Time Template Detail

Template Name: * Time Template 2

description:

Week Plan: **Holiday Plan** 1

00:00 02:00 04:00 06:00 08:00 10:00 12:00 14:00 16:00 18:00 20:00 22:00 24:00 2

Holiday List

+ Add 3

Name

Operation

Select Holiday List

Selected (0)

Name

Add Holiday

Name: * Holiday 1

Holiday Time: 2020-05-21

Holiday Length: * 1 4

5 OK Cancel

Figure 4-4 Set holiday plan (2)

Time Template Detail

Template Name: * Time Template 2

description:

Week Plan: **Holiday Plan**

00:00 02:00 04:00 06:00 08:00 10:00 12:00 14:00 16:00 18:00 20:00 22:00 24:00

Holiday List

+ Add

Name

Operation

6

Holiday 1

Select Holiday List

Selected (1)

Name

Holiday 1

7 Done Cancel

5 Advanced Functions Configuration

5.1 First Card Unlock

You can set multiple first cards. Only after any one of the users swipes the first card can other users without first cards unlock the door with their cards.



- The person to be granted with the first card unlock permission should be the **General** user type and have permission of the certain door. Set the type when adding. For details, see "3.3.2 Adding Staff".
- For details on permission assignment, see "3.4 Permission Configuration".

Step 1 Select **Access Configuration > Advanced Config**.

Step 2 Click the **First Card Unlock** tab.

Step 3 Click **Add**.

Step 4 Configure the parameters, and then click **Save**.

Figure 5-1 First card unlock configuration

First Card Unlock configuration

Door: Door 1 Timezone: All Day Time Template

Status: Normal

Select Personnel

Dropdown list Search..

ID	Name
1	1
2	2
3	3

Selected(2) Clear



ID	Name	Operation
1	1	
2	2	

Save Cancel

Table 5-1 Parameters of first card unlock

Parameter	Description
Door	Select the target access control channel to configure the first card unlock.

Parameter	Description
Timezone	First Card Unlock is valid in the time period of the selected time template.
Status	After First Card Unlock is enabled, the door is in either Normal mode or Always Open mode .
User	Select one or more users to hold first cards. Any one of them swiping the first card means first card unlock is done.

Step 5 (Optional) Click , and then the icon changes to , indicating that **First Card Unlock** is enabled.

The newly added **First Card Unlock** is enabled by default.

5.2 Multi Card Unlock

In this mode, one or multiple groups of users have to swipe cards for an access control channel in an established sequence to unlock the door. One group can have up to 50 users, and one person can belong to multiple groups.

With **Multi-Card Unlock** enabled for an access control channel, there can be up to 4 groups of users being on site at the same time for verification. The total number of users can be 200 at most, with up to 5 valid users.



- The priority of **First Card Unlock** is higher than **Multi Card Unlock**. When enabled at the same time, the platform performs **First Card Unlock** first.
- We do not recommend **First Card Unlock** user join **Multi Card Unlock** user group.
- The user type in the **User Group** cannot be **VIP User** and **Patrol User**. You can set the user type when adding staff. For details, see "3.3.2 Adding Staff".

Step 1 Select **Access Configuration > Advanced Config**.

Step 2 Click **Multi Card Unlock** tab.

Step 3 Add user group.

1) Click **User Group**

Figure 5-2 User group manager

User Group Manager

+ Add Delete

Search..

	GroupName	Total	Operation
<input type="checkbox"/>			

2) Click **Add**.

Figure 5-3 User group configuration

User Group Manager

User Group List > User Group Configuration

User Group Name: * Group1

Select Personnel


Dropdown list Search..

	ID	Name
<input checked="" type="checkbox"/>	1	1
<input checked="" type="checkbox"/>	2	2
<input type="checkbox"/>	3	3

Selected(2) Clear

ID	Name	Operation
1	1	<input type="checkbox"/>
2	2	<input type="checkbox"/>

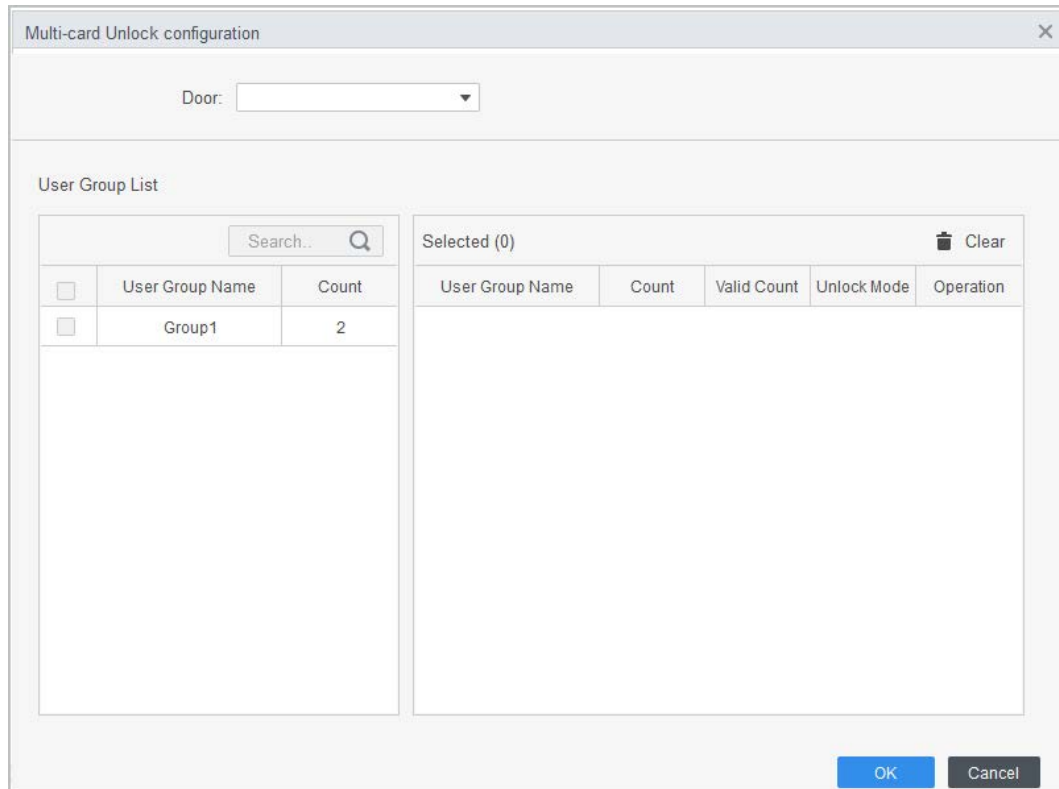
OK Cancel

- 3) Set up **User Group Name**. Select users from **User List**, and then click **OK**. You can select up to 50 users.
- 4) Click  at the upper-right corner of the **User Group Manager** page.

Step 4 Configure parameter of multi card unlock.

- 1) Click **Add**.

Figure 5-4 Multi card unlock configuration (1)

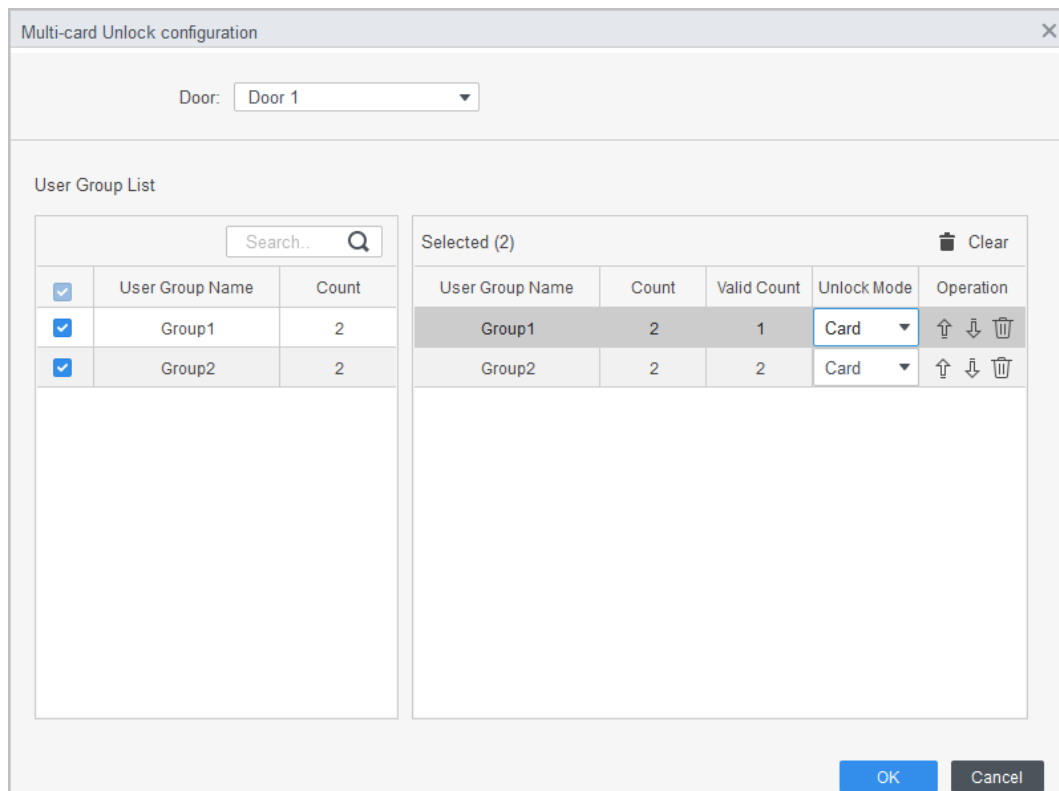


The dialog box titled "Multi-card Unlock configuration" has a "Door:" dropdown menu at the top. Below it is the "User Group List" section. On the left, there is a table with columns "User Group Name" and "Count". It contains one row: "Group1" with a count of "2". Above this table is a search bar. On the right, there is a "Selected (0)" section with a "Clear" button. Below it is a table with columns: "User Group Name", "Count", "Valid Count", "Unlock Mode", and "Operation". At the bottom right are "OK" and "Cancel" buttons.


- 2) Select the door.


- 3) Select the user group. You can select up to four groups.

Figure 5-5 Multi card unlock configuration (2)



The dialog box titled "Multi-card Unlock configuration" shows the "Door:" dropdown set to "Door 1". In the "User Group List" section, the table on the left now has two rows: "Group1" and "Group2", both with a count of "2". Both rows have a checked checkbox in the first column. The "Selected (2)" section on the right now contains two rows. The first row is "Group1" with a count of "2", a "Valid Count" of "1", and an "Unlock Mode" of "Card". The second row is "Group2" with a count of "2", a "Valid Count" of "2", and an "Unlock Mode" of "Card". Each row in the "Selected" table has "Operation" icons (up, down, and delete). At the bottom right are "OK" and "Cancel" buttons.

- 4) Fill in the **Valid Count** for each group to be on site and the **Unlock Mode**. Click  or



 to adjust the group sequence to unlock the door.

- 5) The valid count refers to the number of users in each group that must be on site to swipe their cards. Use Figure 5-5 as an example. The door can be unlocked only if it swiped by any person of group 1 and 2 persons of group 2.



Up to five valid users are allowed.

- 6) Click **OK**.

Step 5 (Optional) Click , and then the icon changes to , indicating that **Multi Card Unlock** is enabled.

The newly added **Multi Card Unlock** is enabled by default.

5.3 Anti-passback

The anti-passback feature requires a person to enter/exit through defined entry/exit door group. You cannot leave without matched entry record, nor can you enter without a complete entry/exit record (for example, only entry record).



Step 1 Select **Access Configuration > Advanced Config**.

Step 2 Click **Add**.

Step 3 Configure parameters.

- 1) Select device and enter device name.
- 2) Select time template.
- 3) Set rest time and the unit is minute. For example, set the reset time as 30 minutes. If one staff has swiped in but not swiped out, the anti-pass back alarm will be triggered when this staff tends to swipe in again within the 30 minutes. The second swipe-in of this staff is only valid after 30 minutes later.
- 4) Click **In Group**, and then select the corresponding reader.
- 5) Click **Out Group** and then select the corresponding reader.
- 6) Click **OK**, and then the configuration will issue to device and take effect.

Figure 5-6 Anti-pass back configuration

Step 4 (Optional) Click , and then the icon changes to , indicating that **Anti-passback** is enabled.

The newly added **Anti-passback** is enabled by default.

5.4 Inter-door Lock

Inter-door lock allows only one access open in a door group at a time. When opening one access, other accesses must be closed. Otherwise, you cannot unlock any access.

One access controller supports two groups of inter-door unlock, and each door group can add up to 4 doors.

Step 1 Select **Access Configuration > Advanced Config.**

Step 2 Click the **Inter-Lock** tab.

Step 3 Click **Add**.

Step 4 Configure parameters, and then click **OK**.

1) Select device and enter device name.

2) Enter remark.

3) Click **Add** twice to add two door groups.

4) Add doors of the access controller to the needed door group. Click one door group, and then click doors to add.

5) Click **OK**.

Figure 5-7 Inter-door lock configuration

inter-lock info

Device: Name: * Room 1

Remark:

Inter-door Lock List

☒

- ☒ Door 1
- ☒ Door 2
- ☒ Door 3
- ☒ Door 4

+ Add



Group 1

- Door 1
- Door 2

Group 2 X

- Door 3
- Door 4

OK Cancel

Step 5 (Optional) Click , and then the icon changes to , indicating that **Inter-door Lock** is enabled.

The newly added **Inter-door Lock** is enabled by default.

6 Access Controller Configuration

You can configure access door, such as reader direction, door status and unlock mode.



The configuration might vary depending on different devices.

Step 1 Select **Access Configuration > Access Config**.

Step 2 Click the door needs to be configured.

Step 3 Configure parameters.

Figure 6-1 Configure access door


The screenshot shows the 'Access Door Config' window with the following settings:

- Door: * Door 1
- Reader Direction Config: IN Reader1 ⇌ OUT
- Status: ☒ Normal ☐ Always Open ☐ Always Close
- Keep OpenTimezone: Unopened
- Keep Close Timezone: Unopened
- Holiday Keep Open Timezone: Unknown
- Holiday Keep Close Timezone: Unknown
- Alarm: ☒ Intrusion ☒ Overtime ☒ Duress
- Door Sensor: ☐
- Administrator Password: ☐
- Remote Verification: ☐
- Binding Channel: No bound.
- Unlock Hold Interval: 6.0 Second
- Close Timeout: 1 Second
- Unlock Mode: or
- ☒ Card ☒ Fingerprint ☐ Face ☒ Password

Buttons: Save, Cancel

Table 6-1 Parameters of access door

Parameter	Description
Door	Enter door name.
Reader Direction	Click ⇌ to set reader direction according to actual situations.

Parameter	Description
Status	<p>Set door status, including Normal, Always Open and Always Close.</p>  <p>It is not the actual door status because SmartPSS Lite can only send commands to the device. If you want to know the actual door status, enable door sensor.</p>
Keep Open Timezone	Select time template when door is always opened.
Keep Close Timezone	Select time template when door is always closed.
Holiday Keep Open Timezone	Select holiday time template when door is always opened.
Holiday Keep Close Timezone	Select holiday time template when door is always closed.
Alarm	Enable alarm function and set alarm type, including intrusion, overtime and duress. When alarm enabled, the SmartPSS Lite will receive uploaded message when the alarm is triggered.
Door Sensor	Enable door sensor so that you can know the actual door status. You are recommended to enable the function.
Administrator Password	Enable and set the administrator password. You can access by entering the password.
Remote Verification	Enable the function and set the time template, and then the access of personnel have to be verified remotely through the SmartPSS Lite during the template periods.
Binding Channel	Set the video channel of the access control linkage. After setting, when live viewing the access control videos, the real-time video of the linked video channel will be displayed.
Unlock Hold Interval	Set the unlock holding interval. The door will automatically close when time is over.
Close Timeout	Set the timeout for alarm. For example, set close timeout as 60 seconds. If the door is not closed for more than 60 seconds, the alarm message will be uploaded.
Unlock Mode	<ul style="list-style-type: none"> • Select And, and then select unlock methods. You need to satisfy all the configured methods at the same time to open the door. • Select Or, and then select unlock methods. You can open the door in any way you configured.. • Select Unlock by time period, and then select unlock mode for each time period. The door can only be opened when you satisfy the unlock methods during the period.

Step 4 Click **Save**, and then the configuration will issue to device and take effect.

7 Viewing Historical Event

Historical door events include those happened on the SmartPSS Lite client and door devices. Before viewing, extract historical events on the door devices to ensure that all events are searched.

Prerequisites

Make sure the personnel you search has been added to the platform.

Procedure

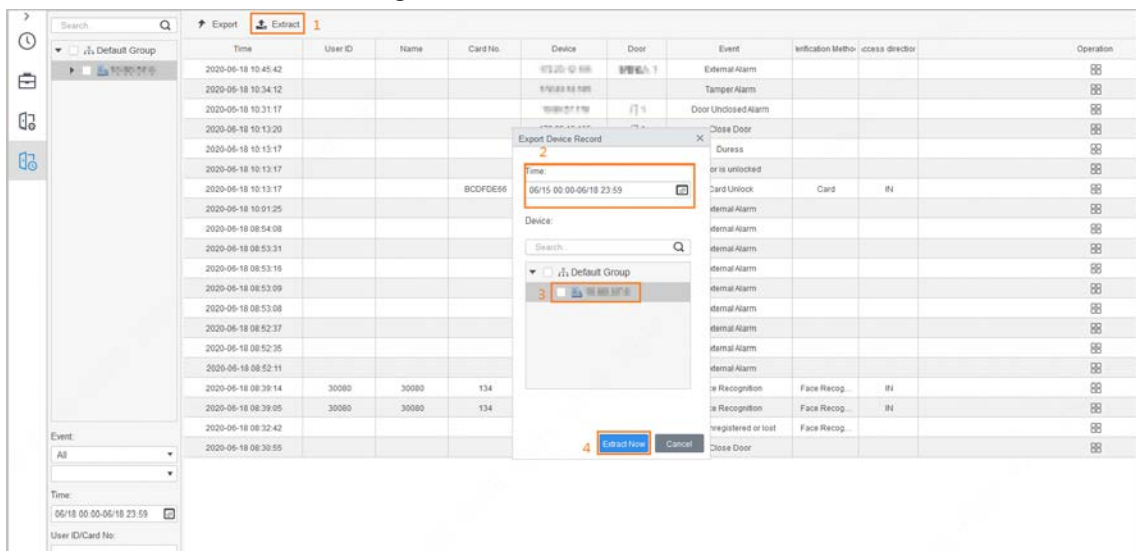
Step 1 Click **Access Configuration > History Event** on the home page.

Step 2 Extract events from door device to the local. Click **Extract**, set the time, select the door device, and then click **Extract Now**.



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

Figure 7-1 Extract events



Step 3 Set filtering conditions, and then click **Search**.

Figure 7-2 Search for events by filtering conditions

Search..

▼

Default Group

▼

Door 1

Event:

Abnormal

All

Time:

05/07 00:00-05/07 23:59

User ID/C...

1

Name:

1

Departme...

Company\DepartmentA

Search


Step 4 (Optional) Click **Export**, and then save the searched door events to the local.

8 Access Manager

After completing access controller configuration, you can remotely monitor access controller status and operate access controller through the platform.

8.1 Remotely Opening and Closing Door

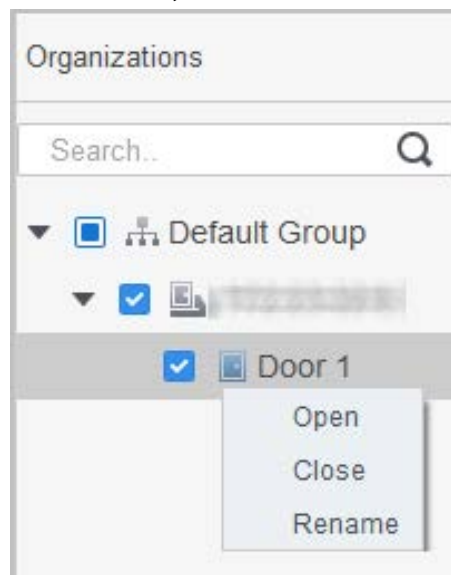
Procedure

Step 1 Click **Access Manager** on the home page. (You can also click **Access Guide** > ).

Step 2 Remotely control the door. There are two methods.

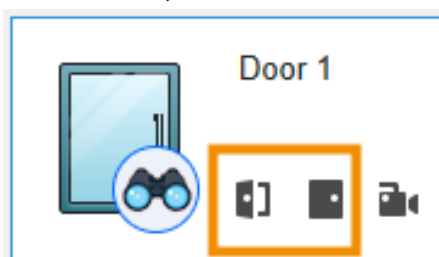
- Method 1: Right-click the door, and then select **Open** or **Close**.

Figure 8-1 Remotely control (method 1)



- Method 2: Click  or  to open or close the door.

Figure 8-2 Remotely control (method 2)



Step 3 View door status on **Event Info** list. For details, see "7 Viewing Historical Event".

Related Operations


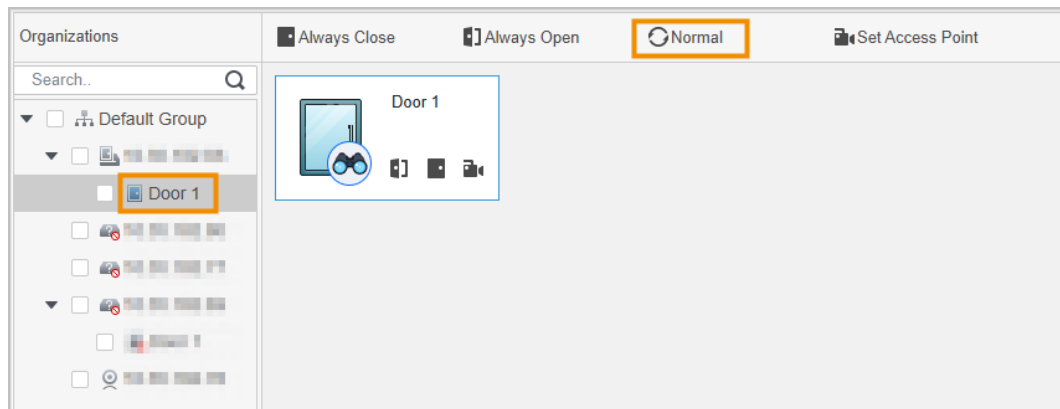
Click  to open the **Event Info** list.

Figure 8-5 Reset door status

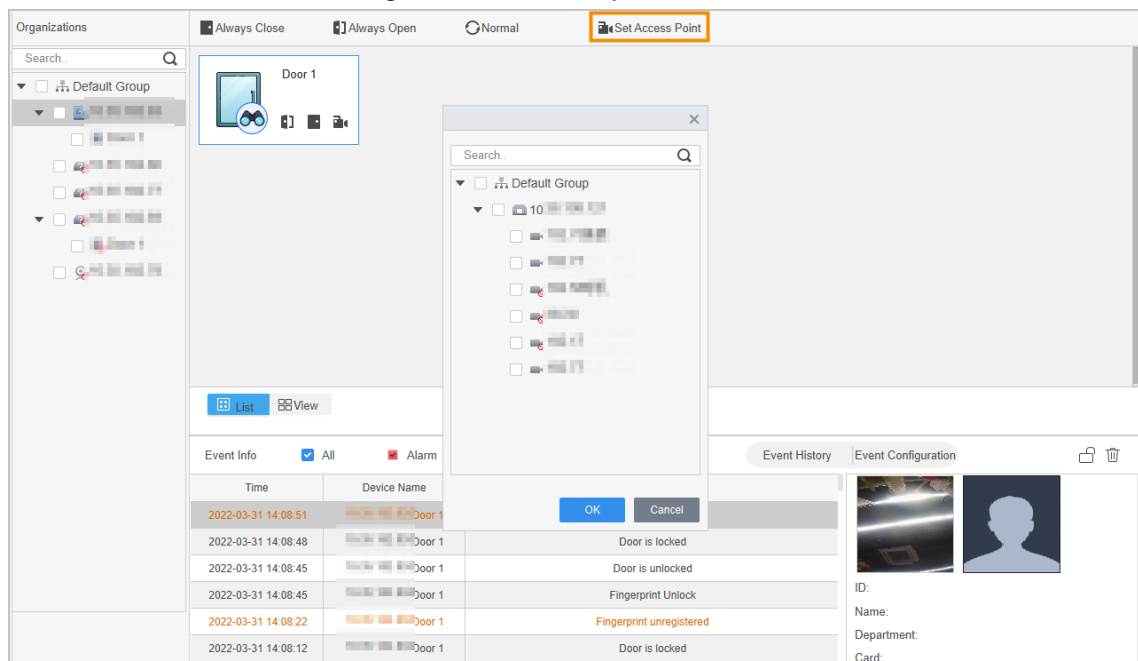


8.4 Setting Access Point

Set the linked smart devices (NVR, IPC, IVSS and more) that support target recognition as the access control point. After setting, the door opening record of target recognition will be uploaded to the platform.

- Step 1** Click **Access Manager** on the home page. (You can also click **Access Guide** >).
- Step 2** Click **Set Access Point**.
- Step 3** Select the device that needs to be set as the access point.

Figure 8-6 Set access point



- Step 4** Click **OK**.
- You can view the event information of the added access points in the **Event Info** below.

8.5 Viewing Access Control Video


View the video captured by the camera of the access controller or the linked external camera.

- If the access controller is equipped with a camera and linked with an external camera at the same

time, the video you viewed is the video of the linked camera.

- If the access controller is equipped with a camera but does not link with an external camera, the video you viewed is the video of the access control camera.
- If you cannot view access control video, it means that the access controller has no camera and is not linked to an external camera. Please configure an external camera for access controller. For details, see "6 Access Controller Configuration".

8.5.1 Viewing Single Access Control Video

Step 1 Click **Access Manager** on the home page. (You can also click **Access Guide** > ).


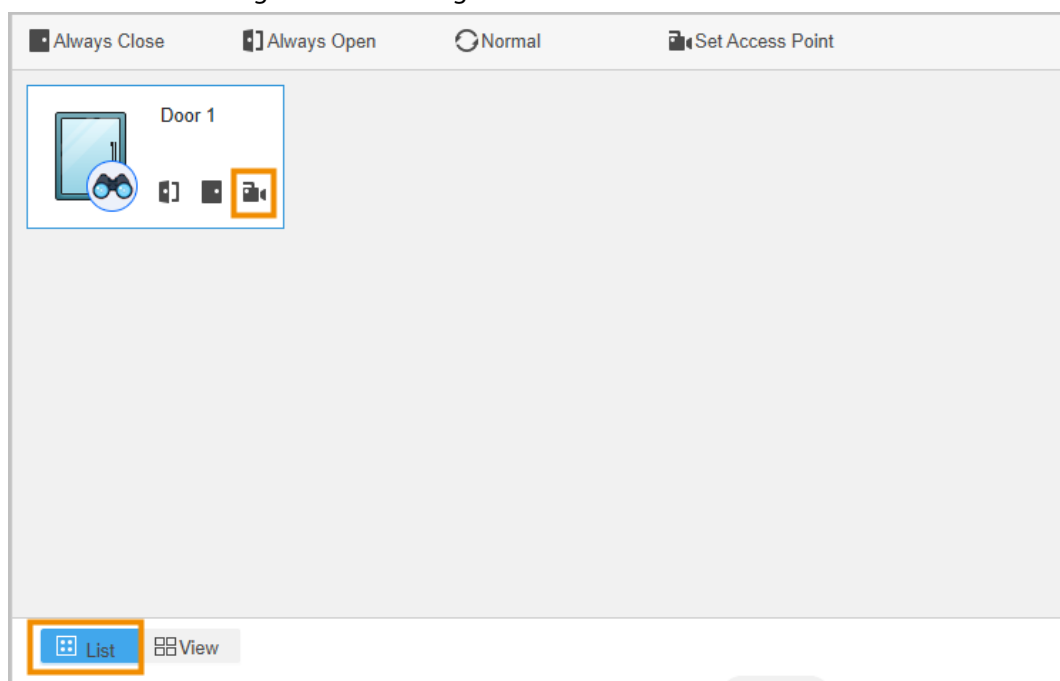

Step 2 Click **List** on the **Access Manager** page, and then click  on the lower-right corner of the device.

Figure 8-7 View single access control video



8.5.2 Viewing Multiple Access Control Videos

Step 1 Click **Access Manager** on the home page. (You can also click **Access Guide** > ).

Step 2 Click **View** on the **Access Manager** page.

Step 3 View access control videos.





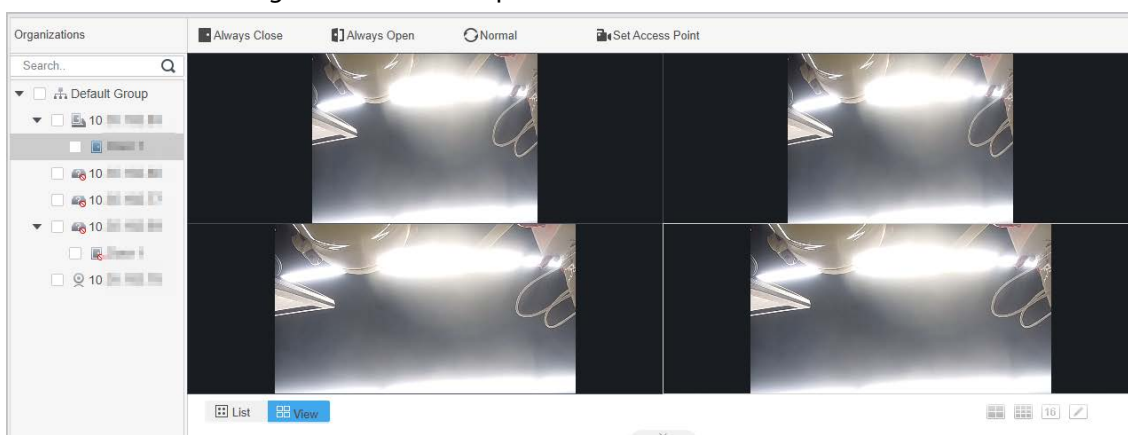
- 1) (Optional) Click     to set the number of windows.
- 2) Drag the access controller in the organization tree to the corresponding window, or click the window, and then double-click the access controller in the organization tree.

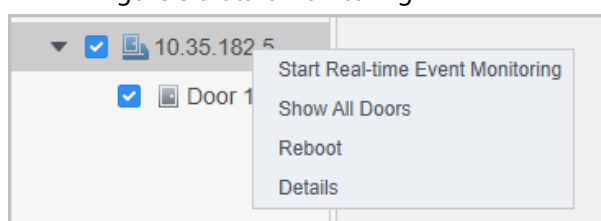
Figure 8-8 View multiple access control videos



8.6 Starting Real-time Event Monitoring

- Step 1** Click **Access Manager** on the home page. (You can also click **Access Guide** >).
- Step 2** Click the access controller that you want to monitor in the left organization tree, right-click the device, and then click **Starting Real-time Event Monitoring** to start real-time event monitoring.

Figure 8-9 Start monitoring

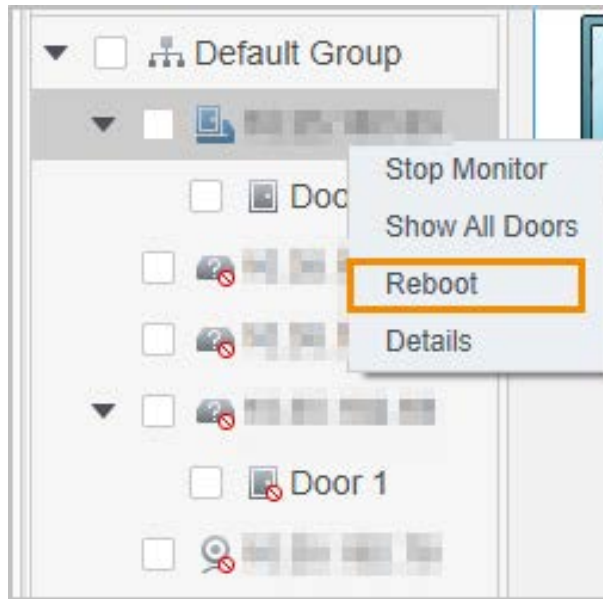


8.7 Rebooting Access Controller

Support remotely rebooting access controllers through the platform.

- Step 1** Click **Access Manager** on the home page. (You can also click **Access Guide** >).
- Step 2** Click the access controller that you want to reboot in the left organization tree, right-click the device, and then click **Reboot** to reboot the device.

Figure 8-10 Reboot device



8.8 Viewing Access Control Details

View the IP address, model, status, serial number, firmware version and other information of the access controllers.

Step 1 Click **Access Manager** on the home page. (You can also click **Access Guide** >).

Step 2 Click the access controller that you want to view in the left organization tree, right-click the device, and then click **Details** to view the detailed information of the device.

Figure 8-11 View details

