SmartPSS-AC_Access Control Solution

User’s Manual

V1.0.1

Foreword

General

This manual introduces the access control solution of SmartPSS-AC (hereinafter referred to as "the SmartPSS-AC").

Safety Instructions

The following categorized signal words with defined meaning 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, lower performance, or unpredictable result.
TIPS	Provides methods to help you solve a problem or save you time.
NOTE	Provides additional information as the emphasis and supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.1	● Add first card unlock function, multi card unlock function, inter-door lock function. ● Add video viewing function.	June 2020
V1.0.0	First release.	May 2020

Privacy Protection Notice

As the device user or data controller, you might collect personal data of others such as face, fingerprints, car plate number, email address, phone number, GPS and so on. You need to be in compliance with the local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures include but not limited to: providing clear and visible identification to inform data subject the existence of surveillance area and providing related contact.

About the Manual

- The manual is for reference only. If there is inconsistency between the manual and the actual product, the actual product shall prevail.

- We are not liable for any loss caused by the operations that do not comply with the manual.
- The manual would be updated according to the latest laws and regulations of related regions. For detailed information, see the paper manual, CD-ROM, QR code or our official website. If there is inconsistency between paper manual and the electronic version, the electronic version shall prevail.
- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the manual. Please contact the customer service for the latest program and supplementary documentation.
- There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, please refer to our 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 the company names in the manual are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurred when using the device.
- If there is any uncertainty or controversy, please refer to our final explanation.

Table of Contents

1 Overview

The access control solution is used with the access control devices through SmartPSS-AC 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 homepage.

The guide bar is displayed at any functions.

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

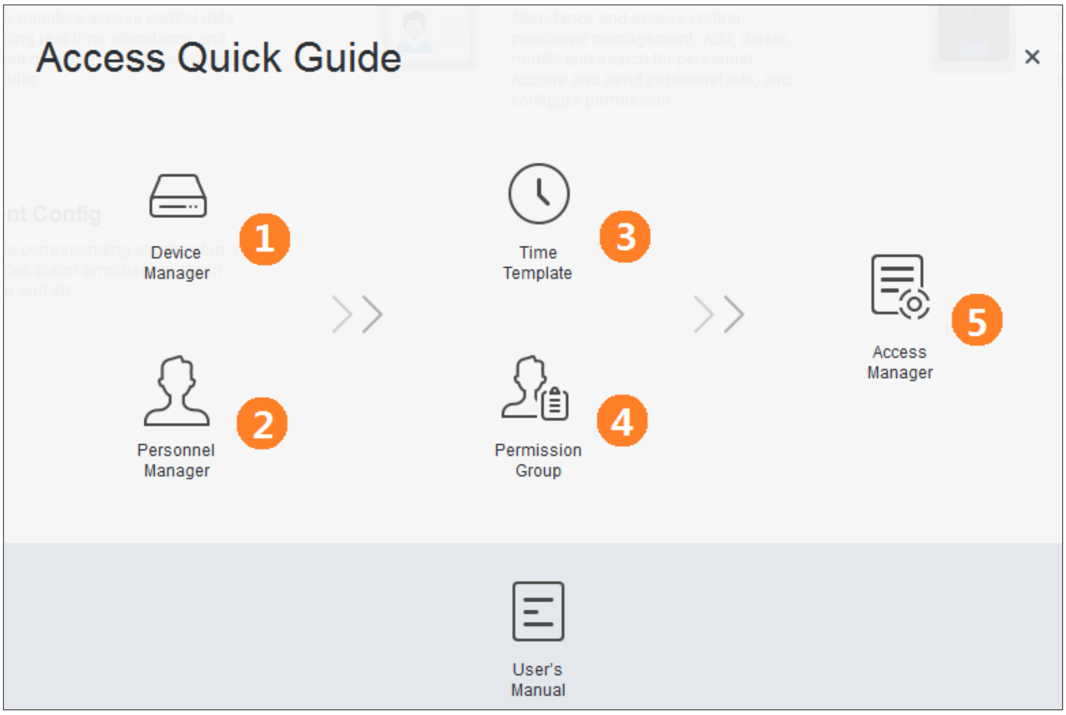


Table 2-1 Functions of access guide

Functions	Description
Device Manager	For details, see *SmartPSS-AC_General_User's Manual*.
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 "3.3 Permission Configuration."
Access Manger	You can control door remotely. For details, see "8 Access Management."
In addition to the above functions, you can also configure events. For details, see "9 Event Configuration."	

3 Personnel Management

You can manage department information and staff information.

3.1 Department Management

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

Step 1 Select **Personnel Manager** on the homepage.

Step 2 (Optional) Select the company and click ✎ to modify campby info, such as region, email and websete.

Step 3 Click ✚ in the **Department List** to add.

Step 4 Select a superior department, and then add a new sub-department. Click **OK** to confirm.

Figure 3-1 Add department

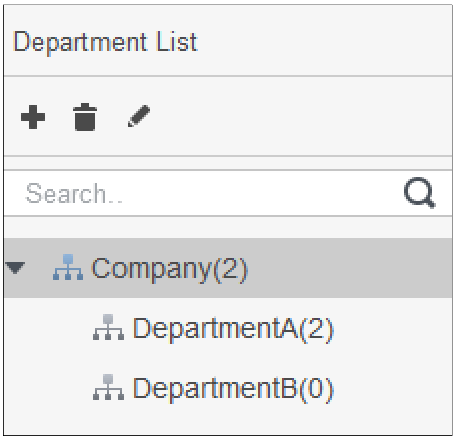
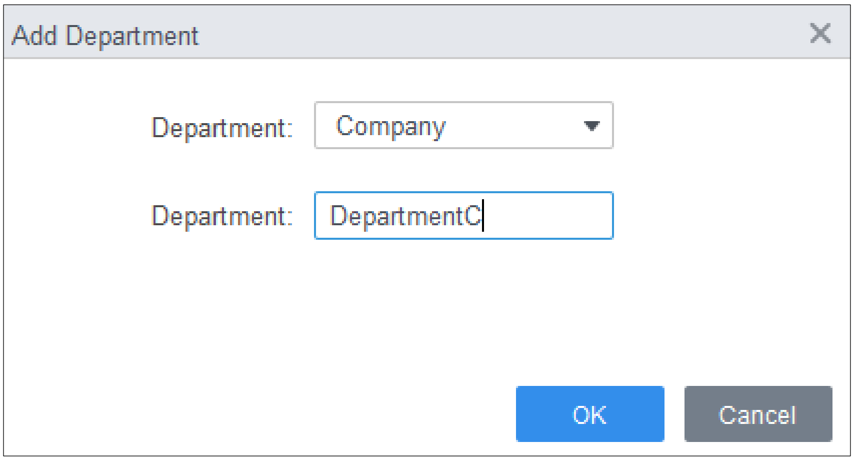


Figure 3-2 Add department information


Add Department

Department: Company

Department: DepartmentC

Step 5 (Optional) Click 🗑 in the **Department List** to delete.

Step 6 (Optional) Select the department and click ✎ in the **Department List** to modify.

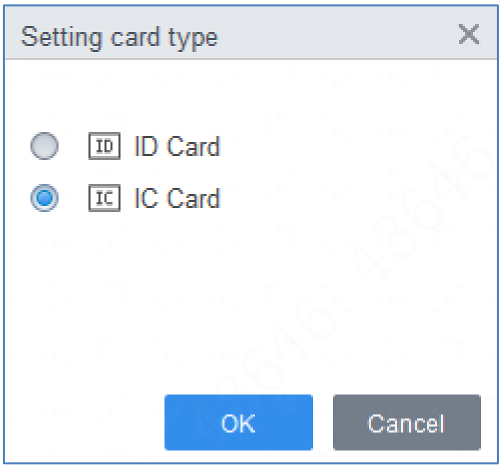
3.2 Staff Management

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

3.2.1 Card Type Setting

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

Figure 3-3 Set card type



Setting card type

○ ID Card

● IC Card

3.2.2 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.

Add Staff One by One Manually

Step 1 Click **Personnel Manger > User > Add**.

Step 2 Add basic information of staff.

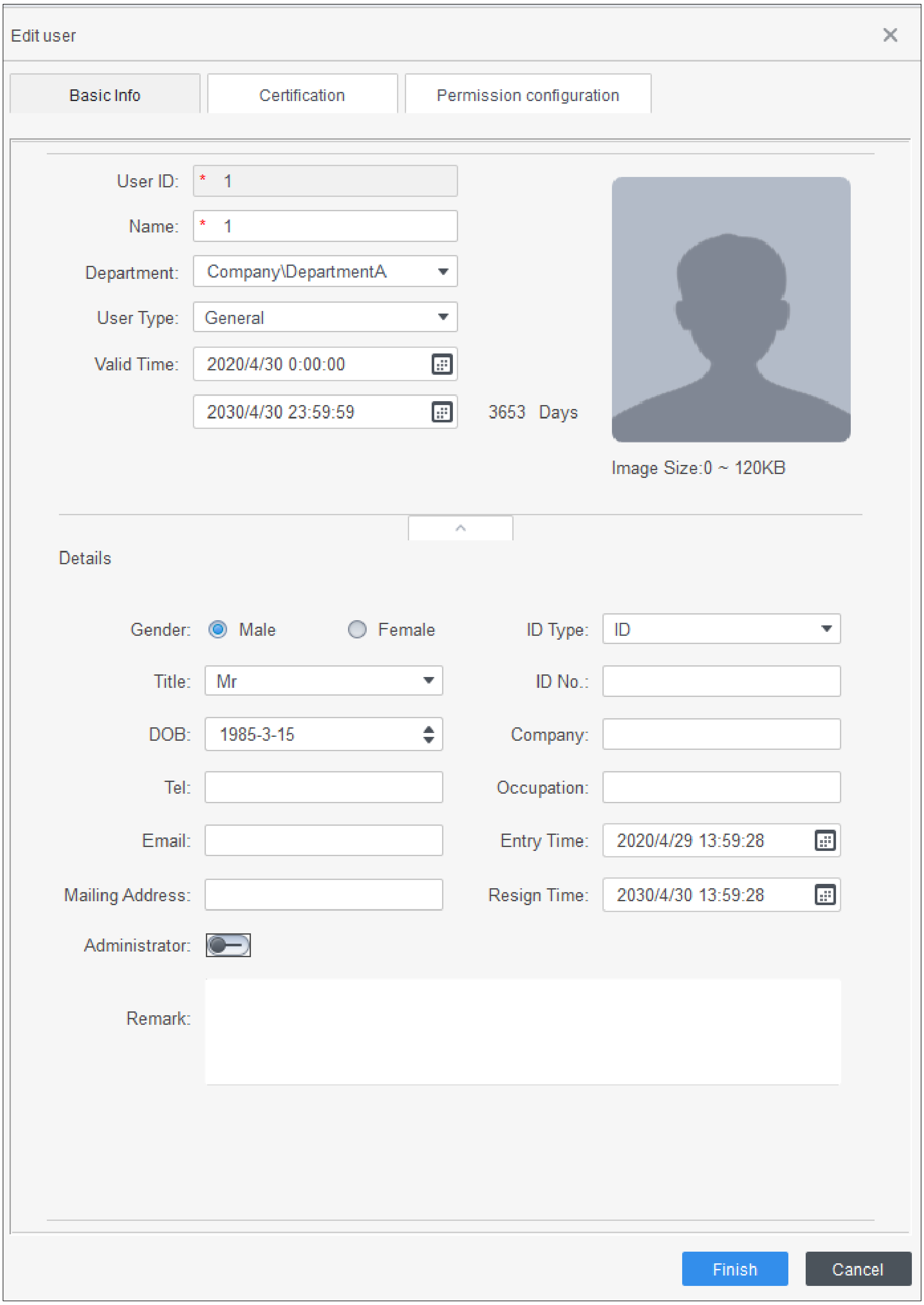
1) Select Basic Info.

2) Add basic information of staff, and upload picture. Then click **Finish** to save.

🕮

The card number can be read automatically or filled in manually. For automatically read, select card reader next to the **Card No.**, and then place the card on the card reader. The card number is read automatically after that.

Figure 3-4 Add basic information



Edit user

Basic Info | Certification | Permission configuration

User ID: * 1

Name: * 1

Department: Company\DepartmentA

User Type: General

Valid Time: 2020/4/30 0:00:00

2030/4/30 23:59:59 3653 Days

Image Size:0 ~ 120KB

Details

Gender: ● Male ○ Female

ID Type: ID

Title: Mr

ID No.:

DOB: 1985-3-15

Company:

Tel:

Occupation:

Email:

Entry Time: 2020/4/29 13:59:28

Mailing Address:

Resign Time: 2030/4/30 13:59:28

Administrator:

Remark:

Step 3 Click **Personnel Manger > User > Add > Certification** to add certification information of staff.

- Configure password.

1) Set password. For the second generation access controllers, set the personnel password; for other devices, set the card password. The new password 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.

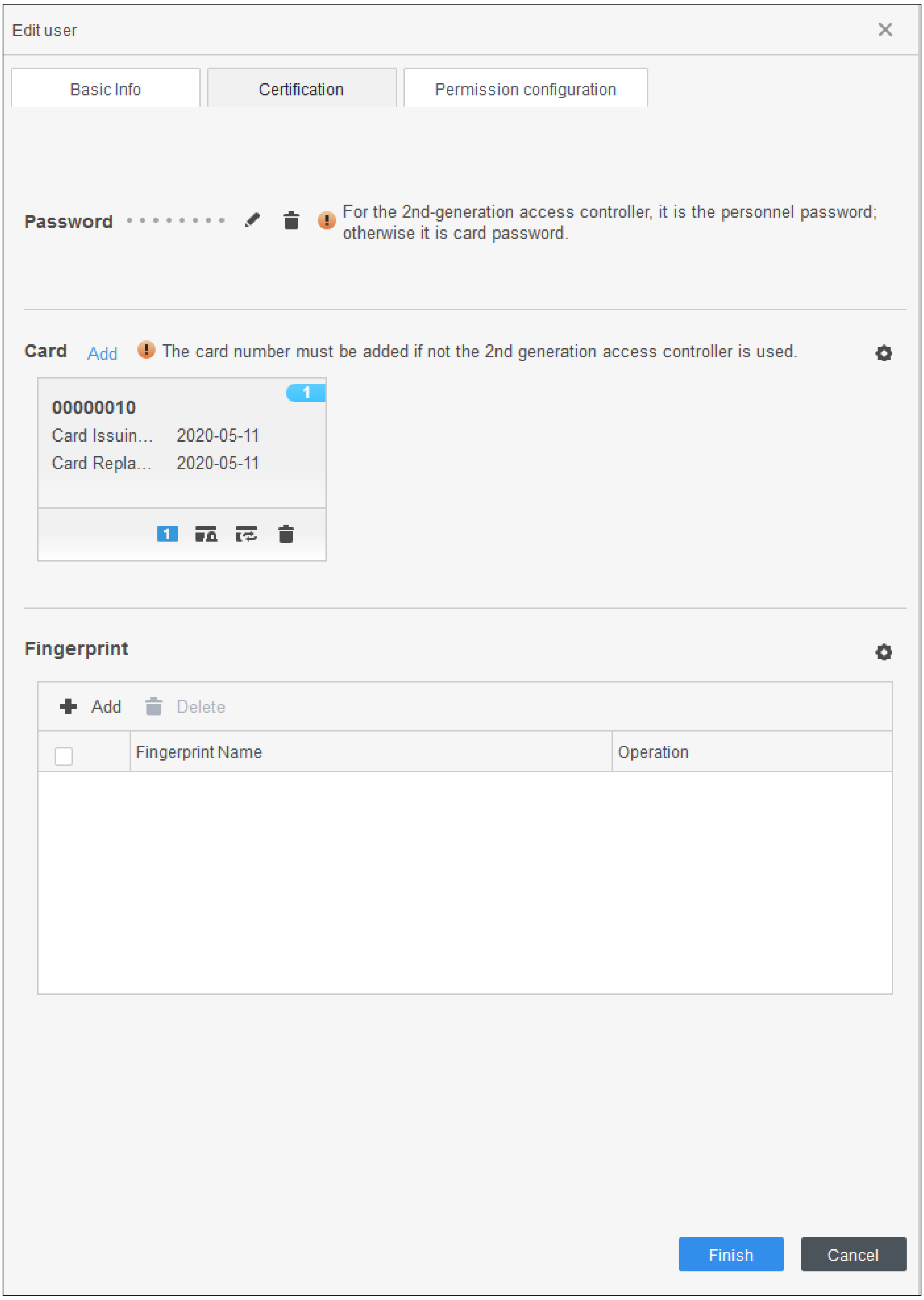
3) After adding, you can select the card as main card or duress card, or replace the card with new one, or delete the card.

- Configure fingerprint.

1) Click ⚙ to select **Device** or **Fingerprint Scanner** as fingerprint collector.

2) Add fingerprint. Click **Add Fingerprint** and press finger on the scanner three times continuously.

Figure 3-5 Configure certification



Edit user ×

Basic Info | Certification | Permission configuration

Password ••••••••• For the 2nd-generation access controller, it is the personnel password; otherwise it is card password.

Card Add The card number must be added if not the 2nd generation access controller is used.

00000010 1

Card Issuin...	2020-05-11
Card Repla...	2020-05-11

Fingerprint

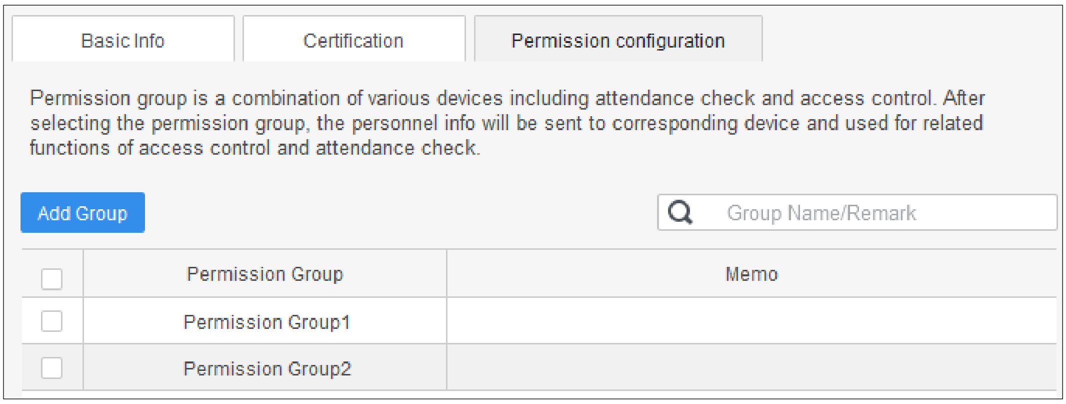
Add Delete

□	Fingerprint Name	Operation

Finish Cancel

Step 4 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. For details, see "3.3 Permission Configuration."

Figure 3-6 Permission configuration

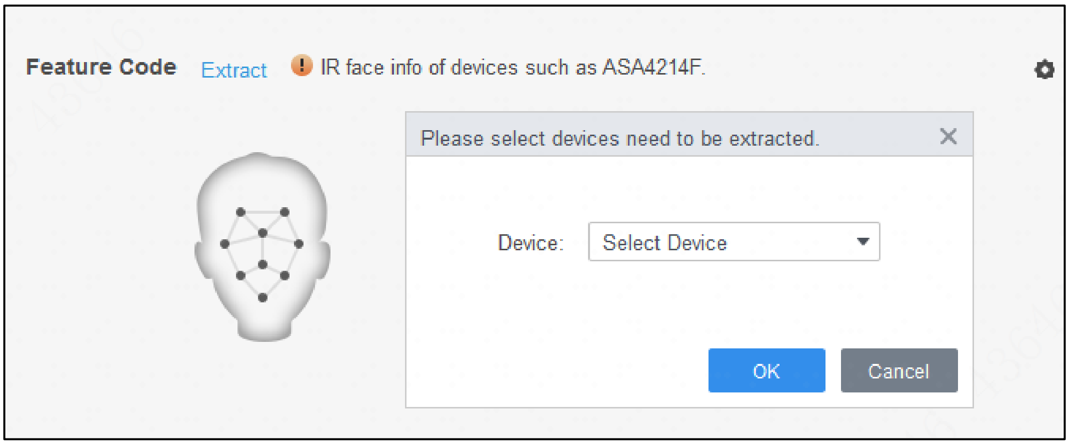


Permission group is a combination of various devices including attendance check and access control. After selecting the permission group, the personnel info will be sent to corresponding device and used for related functions of access control and attendance check.

	Permission Group	Memo
□	Permission Group1	
□	Permission Group2	

Step 5 Click **Finish**.

Figure 3-7 Feature code


Feature Code
Extract
IR face info of devices such as ASA4214F.
Please select devices need to be extracted.
Device:
Select Device
OK
Cancel

Step 6 (Optional) If the user you added has face unlock permission of a device (device model is ASA4214F for example) with IR face feature function, and if you want to grant the user face unlock permission of other devices with IR face feature function, do the following operations.

1) Click ✎ on the right of the user.
2) Click the authentication tag on the pop-up interface.
3) Click ⚙.
4) Select devices that are with face features of the user.
5) Click **OK** and then click **Extract**.

The user can unlock with faces on the selected devices that are with IR face feature function.

Add Staff in Batches

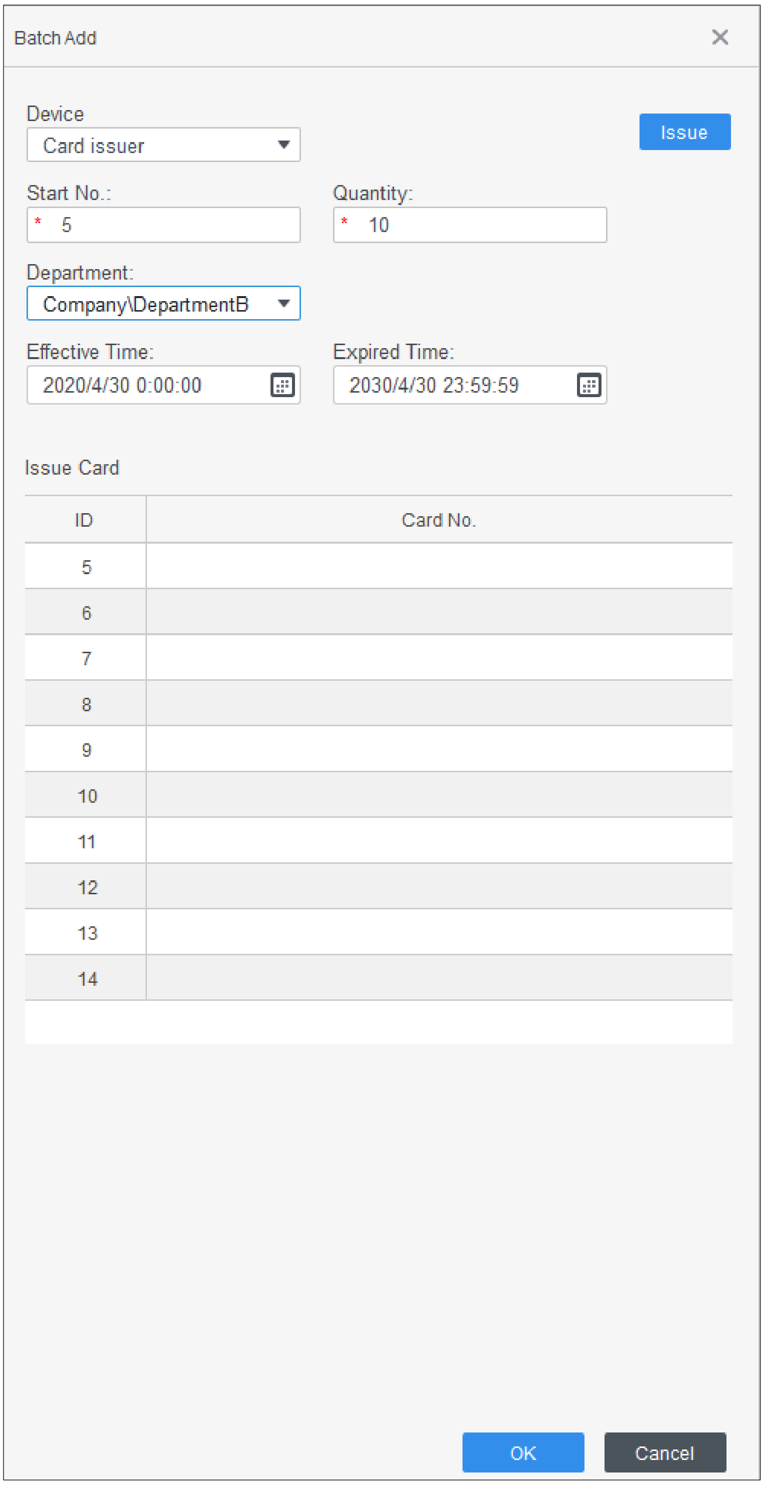
Step 1 Click **Personnel Manger > User > Batch Add**.

Step 2 Select card reader and the department of staff. Set the start number, end number of card, effective time and expired time of card.

Step 3 Click **Issue** and the card number will be read automatically.

Step 4 Click **OK**.

Figure 3-8 Add staff in batches



Device: Card issuer

Start No.: * 5

Quantity: * 10

Department: Company\DepartmentB

Effective Time: 2020/4/30 0:00:00

Expired Time: 2030/4/30 23:59:59

Issue Card

ID	Card No.
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	

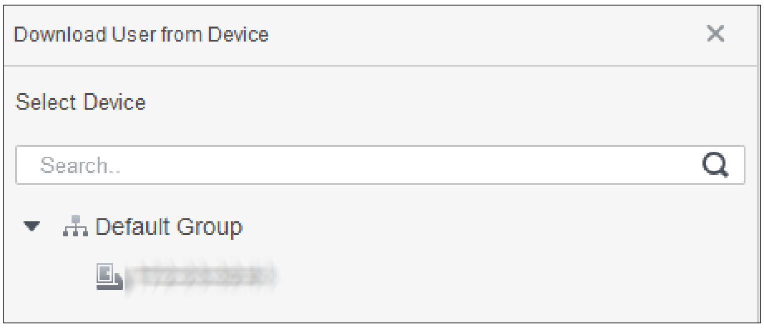
Step 5 In the list of staff, click ✎ to modify information or add details of staff.

Extract Staff Information from Other Devices

Step 1 Click **Personnel Manger > User > Extract**.

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

Figure 3-9 Devices with staff information



Download User from Device

Select Device

Search..

Default Group

[redacted]

<u>Step 3</u> Select the needed staff information, and click **Extract**.

<u>Step 4</u> In the list of staff, click ✎ to modify information or add details of staff.

Import Staff Information from the Local

<u>Step 1</u> Click **Personnel Manger > User > Import**.

<u>Step 2</u> Import staff information according to instructions.

3.2.3 Issuing Card in Batches

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

<u>Step 1</u> Select **Personnel Manager > User**.

<u>Step 2</u> Select the needed staff and then click **Batch Issue Card**.

<u>Step 3</u> Issue card in batches. Card No. can be auto read by card reader or entered manually.

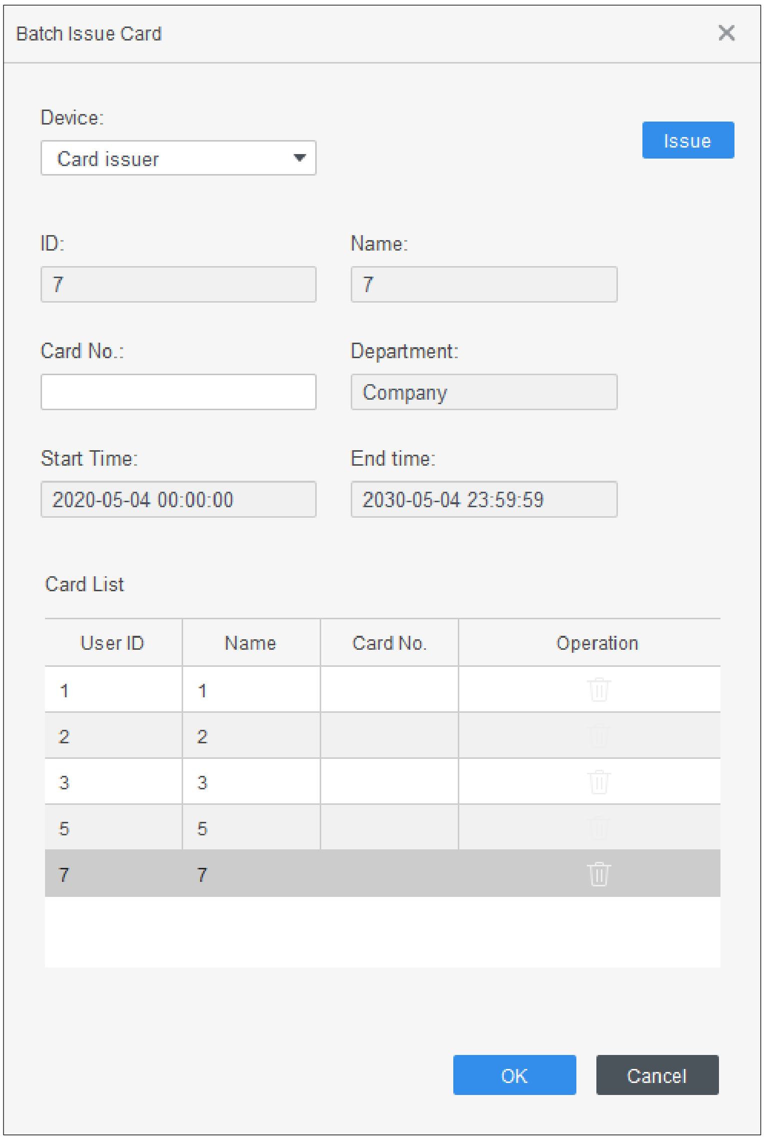
- Auto read

1) Select card reading device, and then click **Issue.**
2) According to the order list, put the cards of the corresponding staff on card reader in sequence, and then the SmartPSS-AC will auto read the card No..
3) Modify staff info, such as start time and end time for card validation.

- Enter manually

1) Select staff in card list and enter the corresponding card No..
2) Modify staff info, such as start time and end time for card validation.

Figure 3-10 Issue card in batches



Device: Card issuer

ID: 7

Name: 7

Card No.:

Department: Company

Start Time: 2020-05-04 00:00:00

End time: 2030-05-04 23:59:59

Card List

User ID	Name	Card No.	Operation
1	1		🗑
2	2		🗑
3	3		🗑
5	5		🗑
7	7		🗑

Step 4 Click **OK**.

3.2.4 Exporting Staff Information

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

3.2.5 Searching for Staff

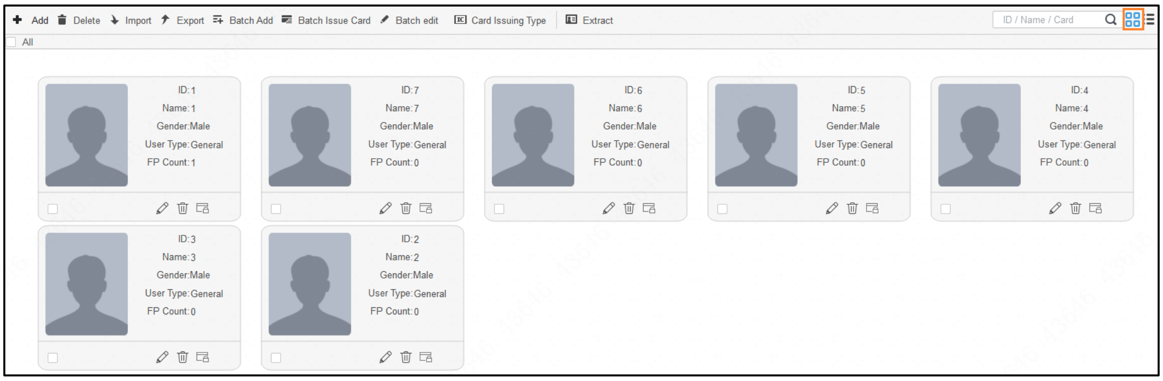
Search for staff who meet the conditions, according to ID, name or card.

Figure 3-11 Search for staff

3.2.6 Staff Displaying

You can select display modes: card display and list display; and you can also edit department and valid time of users in batches.

Figure 3-12 Card display



ID:1
Name:1
Gender:Male
User Type:General
FP Count:1

ID:7
Name:7
Gender:Male
User Type:General
FP Count:0

ID:6
Name:6
Gender:Male
User Type:General
FP Count:0

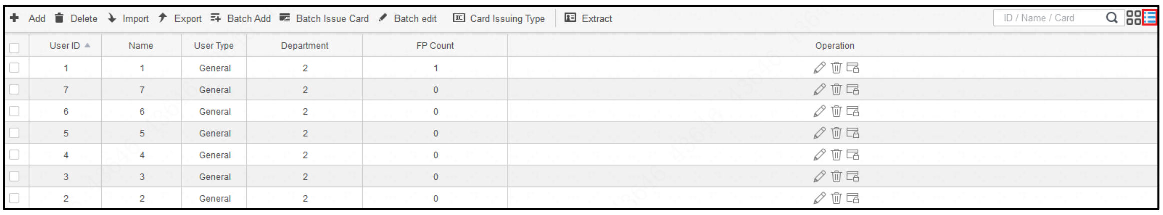
ID:5
Name:5
Gender:Male
User Type:General
FP Count:0

ID:4
Name:4
Gender:Male
User Type:General
FP Count:0

ID:3
Name:3
Gender:Male
User Type:General
FP Count:0

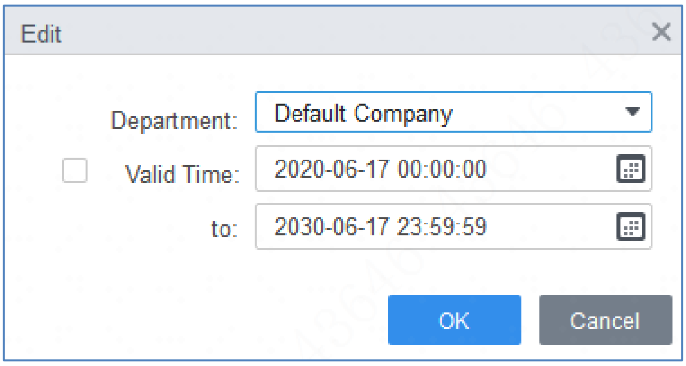
ID:2
Name:2
Gender:Male
User Type:General
FP Count:0

Figure 3-13 List display



□	User ID	Name	User Type	Department	FP Count	Operation
□	1	1	General	2	1	
□	7	7	General	2	0	
□	6	6	General	2	0	
□	5	5	General	2	0	
□	4	4	General	2	0	
□	3	3	General	2	0	
□	2	2	General	2	0	

Figure 3-14 Edit department



Department: Default Company

□ Valid Time: 2020-06-17 00:00:00

to: 2030-06-17 23:59:59

3.3 Permission Configuration

3.3.1 Adding Permission Group

Step 1 Click **Personnel Manger > 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 of time template setting, see SmartPSS-AC_Access Control Solution_User's Manual.

3) Select the corresponding device, such as door 1.

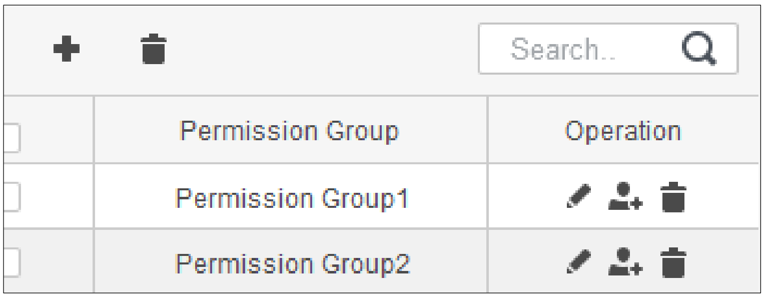
Step 4 Click **OK** to save operations.

Step 5 (Optional) Click 🗑 to delete group.

Step 6 (Optional) Click ✎ to modify group info.

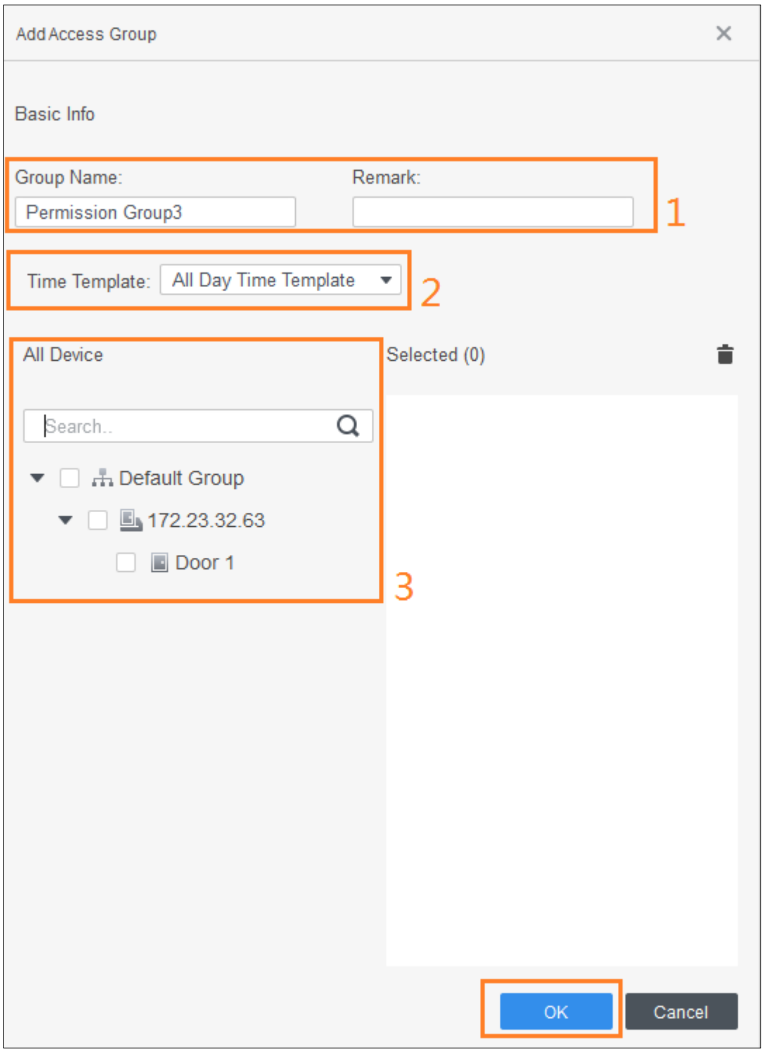
Step 7 (Optional) Double-click permission group name to view group info.

Figure 3-15 Add permission group (1)



□	Permission Group	Operation
□	Permission Group1	✎ 👤+ 🗑
□	Permission Group2	✎ 👤+ 🗑

Figure 3-16 Add permission group (2)



Group Name: Permission Group3

Remark:

Time Template: All Day Time Template

- □ Default Group
  - □ 172.23.32.63
    - □ Door 1

3.3.2 Configuring Permission

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

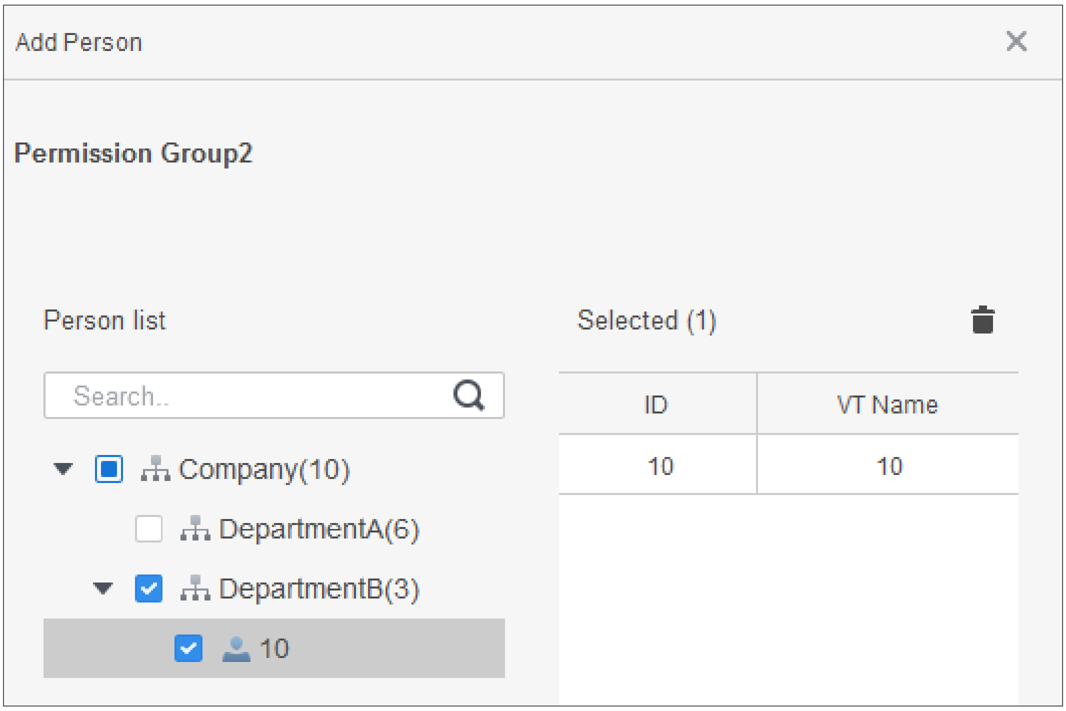
Step 1 Click **Personnel Manger > Permission Configuration**.

Step 2 Click .

Step 3 Select the department need to be configured permission.

Step 4 Click **OK**.

Figure 3-17



- ■ Company(10)
  - □ DepartmentA(6)
  - ☑ DepartmentB(3)
    - ☑ 10

ID	VT Name
10	10

Step 5 (Optional) Click in the left navigation bar to view the authorization progress. Click to view the details.

4 Time Template Setting

Time template is to configure the working hours of access controllers, such as when to open and when to open. The SmartPSS-AC 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 homepage. (Or select **Access Guide >** 🕒 on the homepage.)

Step 2 Click **Add**.

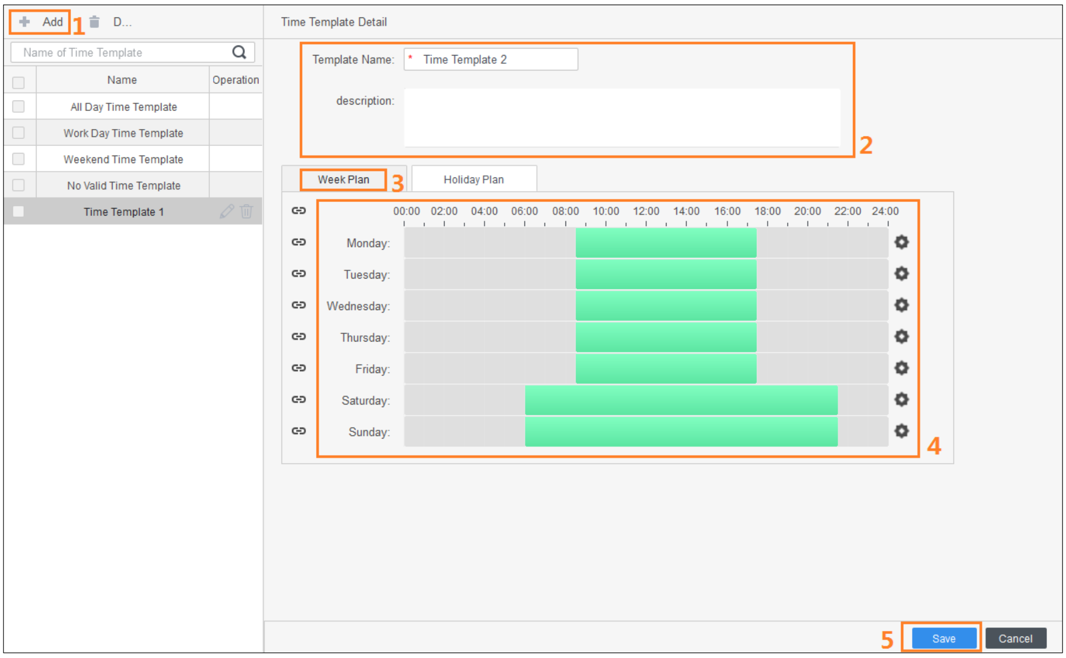
Step 3 Set time template.

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. 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 and not allow personnel to pass through. When cursor is ✏, click the needed periods, and the periods become green and allow personnel to pass through. Click **Save**.

Figure 4-1 Set week plan (method 1)



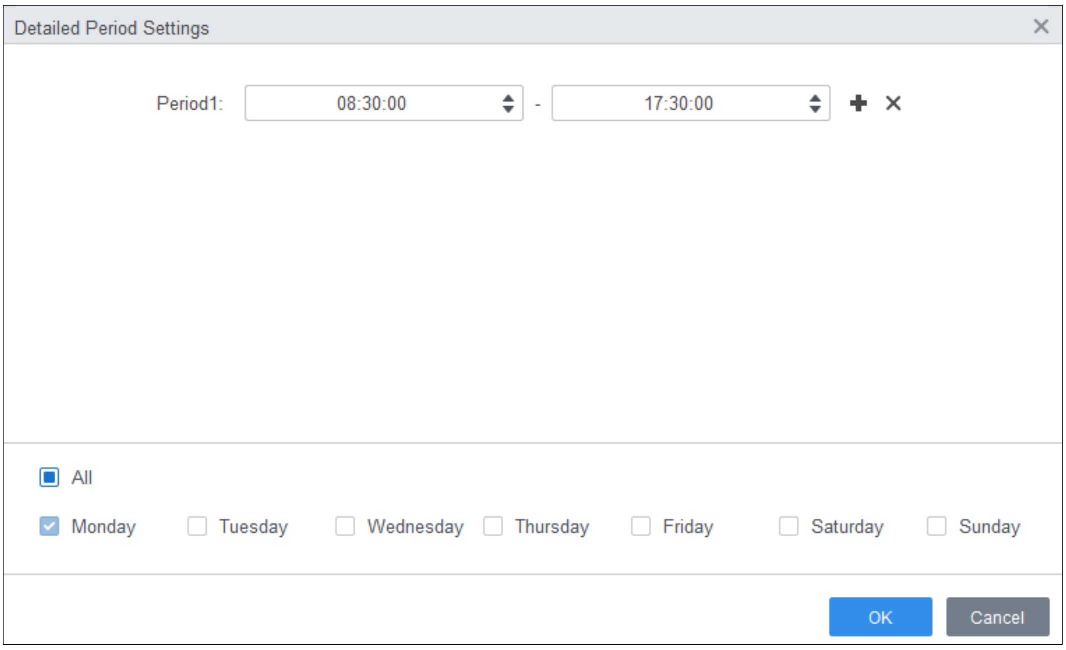
□	Name	Operation
□	All Day Time Template	
□	Work Day Time Template	
□	Weekend Time Template	
□	No Valid Time Template	
□	Time Template 1	

Template Name: * Time Template 2

description:

   ◇ 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 **Save**.

Figure 4-2 Set week plan (method 2)



Detailed Period Settings

Period1: 08:30:00 - 17:30:00

☑ All

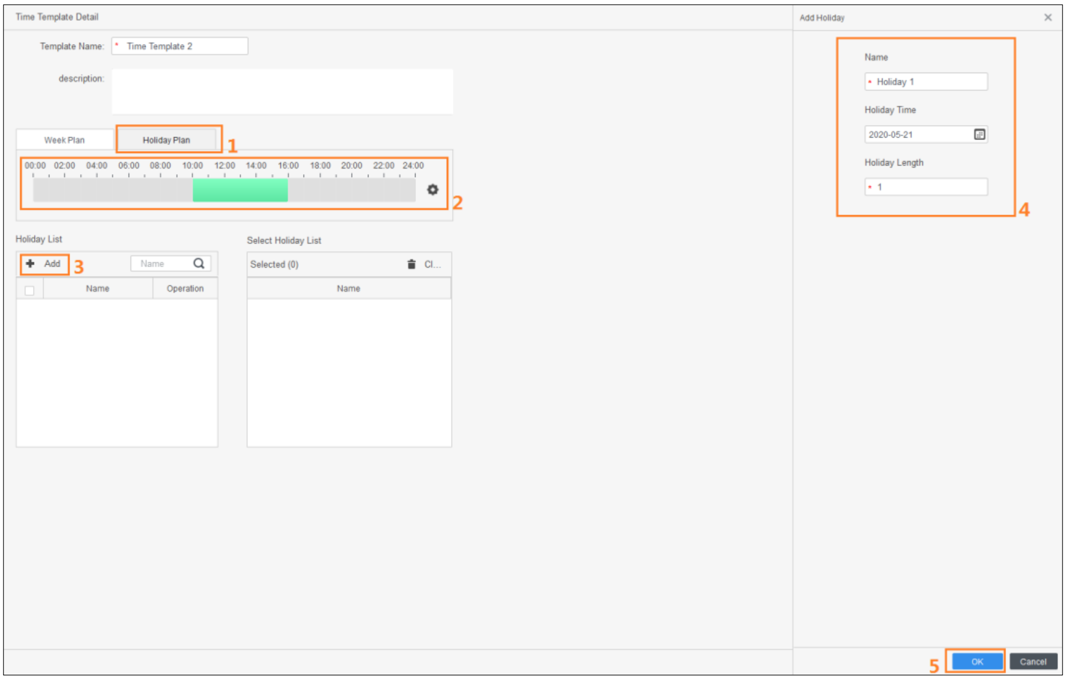
☑ Monday □ Tuesday □ Wednesday □ Thursday □ Friday □ Saturday □ Sunday

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 interface, and then click **OK.** Select the needed holiday in the **Holiday List** and click **OK**.

- When the week plan and the holiday plan are in conflict, the holiday plan has higher priority. For example, if the week plan is set to allow access but the holiday plan is not, the access controller is accessible.
- After the time template is configured, assign the permission in **Personnel Manager > Permission Configuration** when selecting time template.

Figure 4-3 Set holiday plan (1)



Time Template Detail

Template Name: * Time Template 2

description:

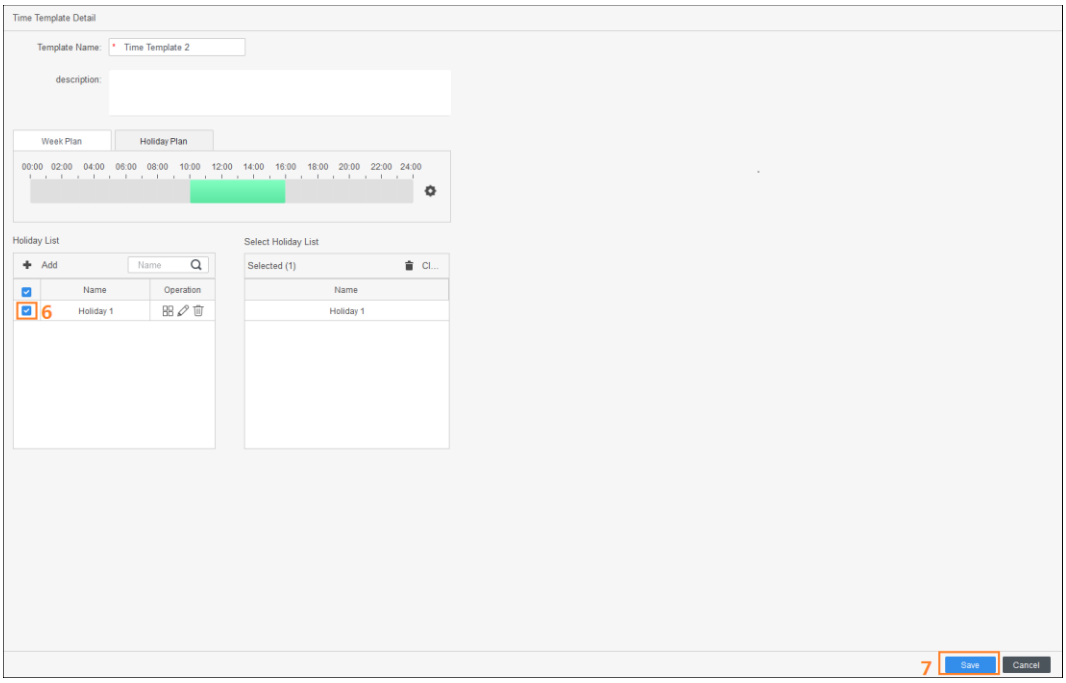
Add Holiday

Name: * Holiday 1

Holiday Time: 2020-05-21

Holiday Length: * 1

Figure 4-4 Set holiday plan (2)



Time Template Detail

Template Name: * Time Template 2

description:

5 Advanced Functions Configuration

5.1 First Card Unlock

Only after the specified first-card user swipes the card every day can other users unlock the door with their cards. 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 "3.2.2 Adding Staff."
- For details of permission assignment, see "3.3 Permission Configuration."

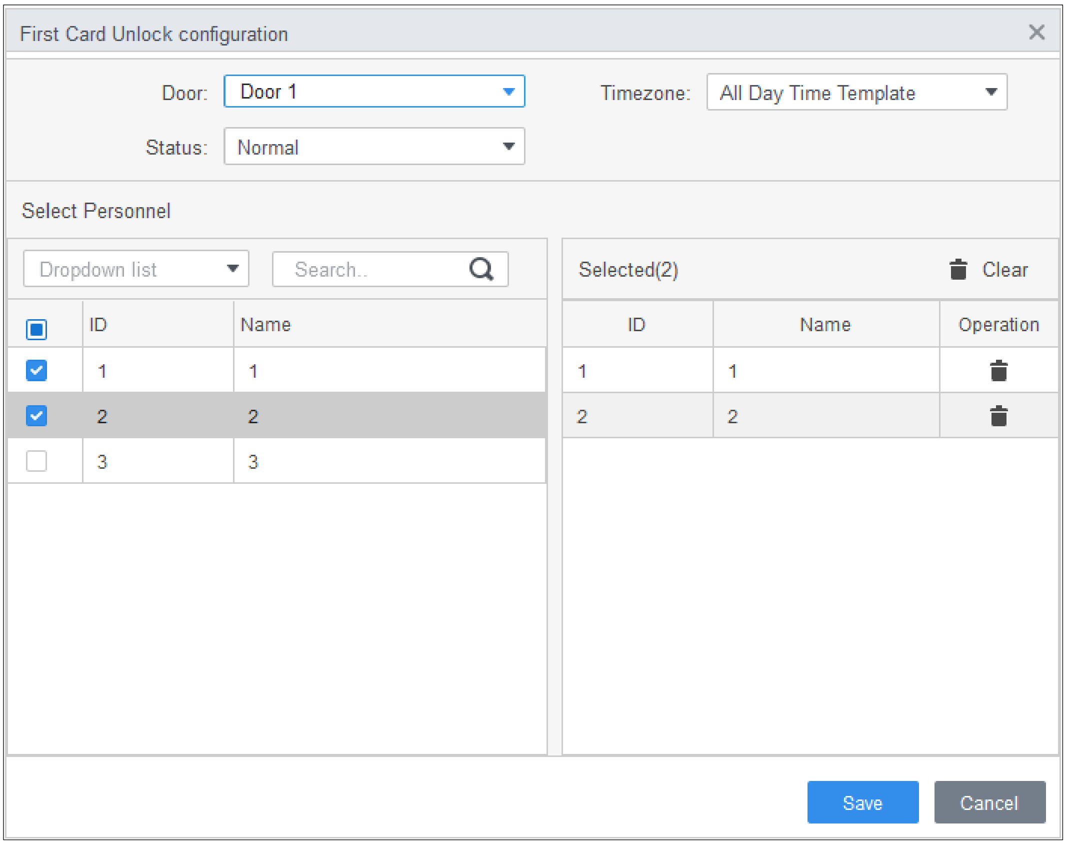
Step 1 Select **Access Configuration > Advanced Config**.

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

Step 3 Click **Add**.

Step 4 Configure the **First Card Unlock** parameters and 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

☑	ID	Name
☑	1	1
☑	2	2
□	3	3

Selected(2)

ID	Name	Operation
1	1	🗑
2	2	🗑

Table 5-1 Parameters of first card unlock

Parameter	Description
Door	Select the target access control channel to configure the first card unlock.
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 the **Normal mode** or **Always Open mode**.

Parameter	Description
User	Select the user to hold the first card. Supports selecting a number of users to hold first cards. Any one of them swiping the first card means first card unlock is done.

Step 5 (Optional) Click . The icon changing into indicates **First Card Unlock** is enabled.

6) 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 four 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.

🕮

- First card unlock has higher priority than multi-card unlock, which means if the two rules are both enabled, the system performs first card unlock first.
- You are recommended to add people with first card unlock permission to the multi-card Unlock group.
- Do not set the **VIP** or **Patrol** type for people in the user group. For details, see "3.2.2 Adding Staff."
- For details of permission assignment, see "3.3 Permission Configuration."

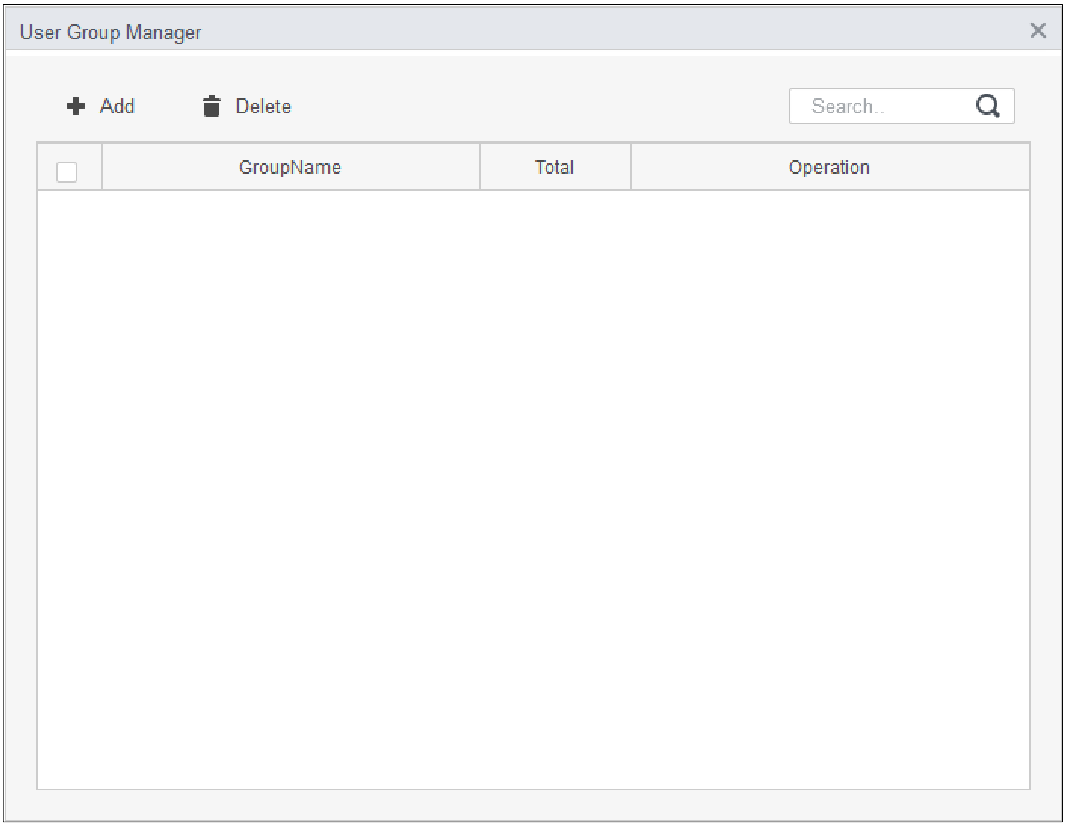
Step 1 Select **Access Configuration > Advanced Config**.

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

Step 3 Add user group.

1) Click User Group.

Figure 5-2 User group manager



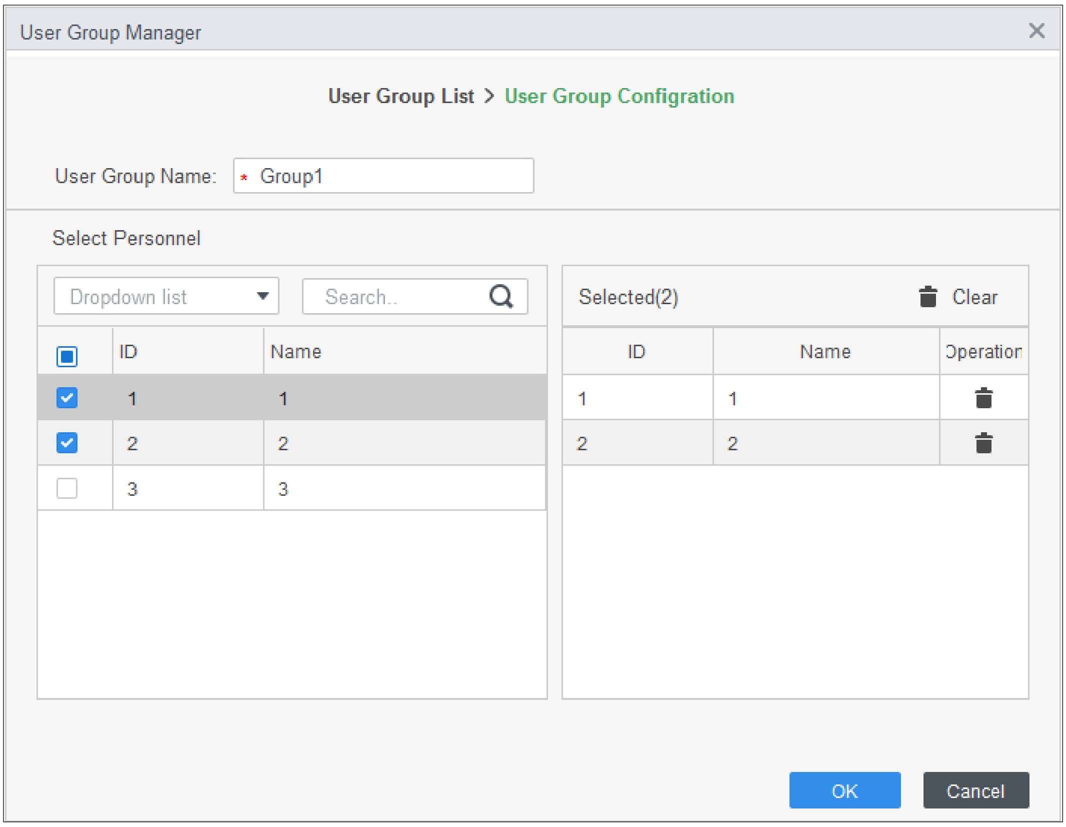
User Group Manager ✕

✚ Add   Delete   Search..

□	GroupName	Total	Operation

2) Click **Add**.

Figure 5-3 User group configuration



User Group Manager ✕

User Group List > User Group Configration

User Group Name: * Group1

Select Personnel

Dropdown list ▾   Search..

■	ID	Name
☑	1	1
☑	2	2
□	3	3

Selected(2)   Clear

ID	Name	Operation
1	1	🗑
2	2	🗑

OK   Cancel

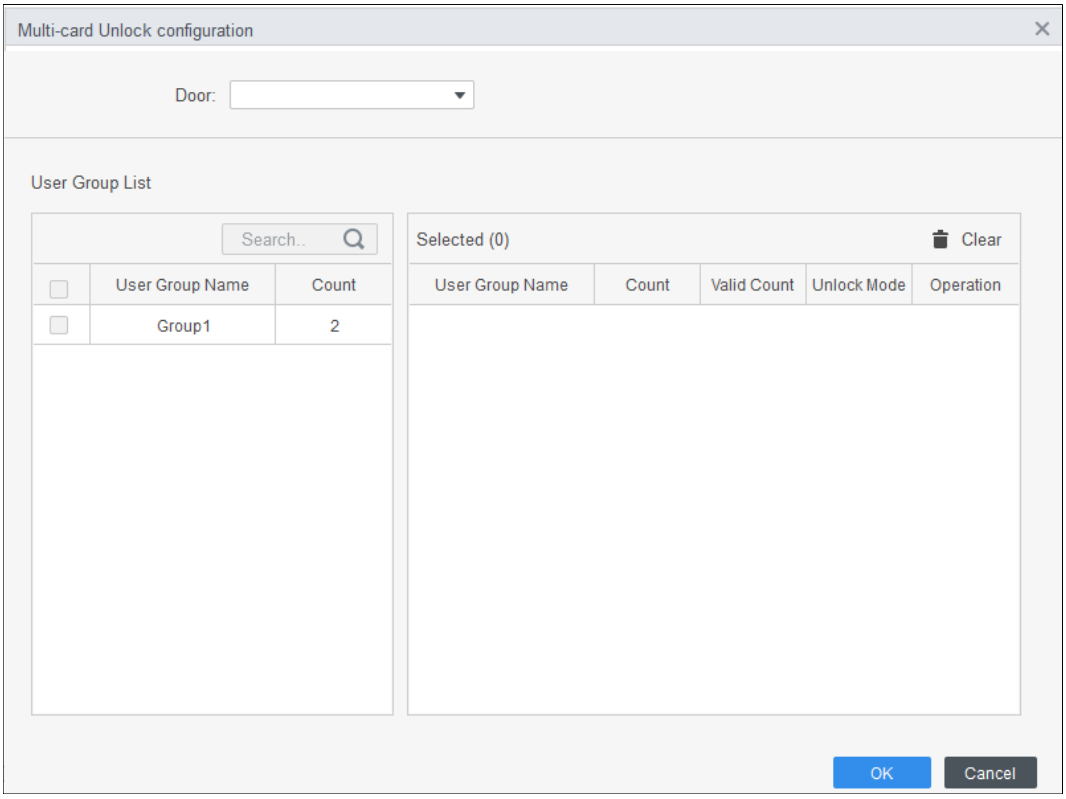
3) Set up **User Group Name**. Select users from **User List** and click **OK**. You can select up to 50 users.

4) Click ☒ at the upper-right corner of the **User Group Manager** interface.

Step 4 Configure parameter of multi card unlock.

1) Click **Add**.

Figure 5-4 Multi card unlock configuration (1)



Multi-card Unlock configuration

Door:

User Group List

Search..

□	User Group Name	Count
□	Group1	2

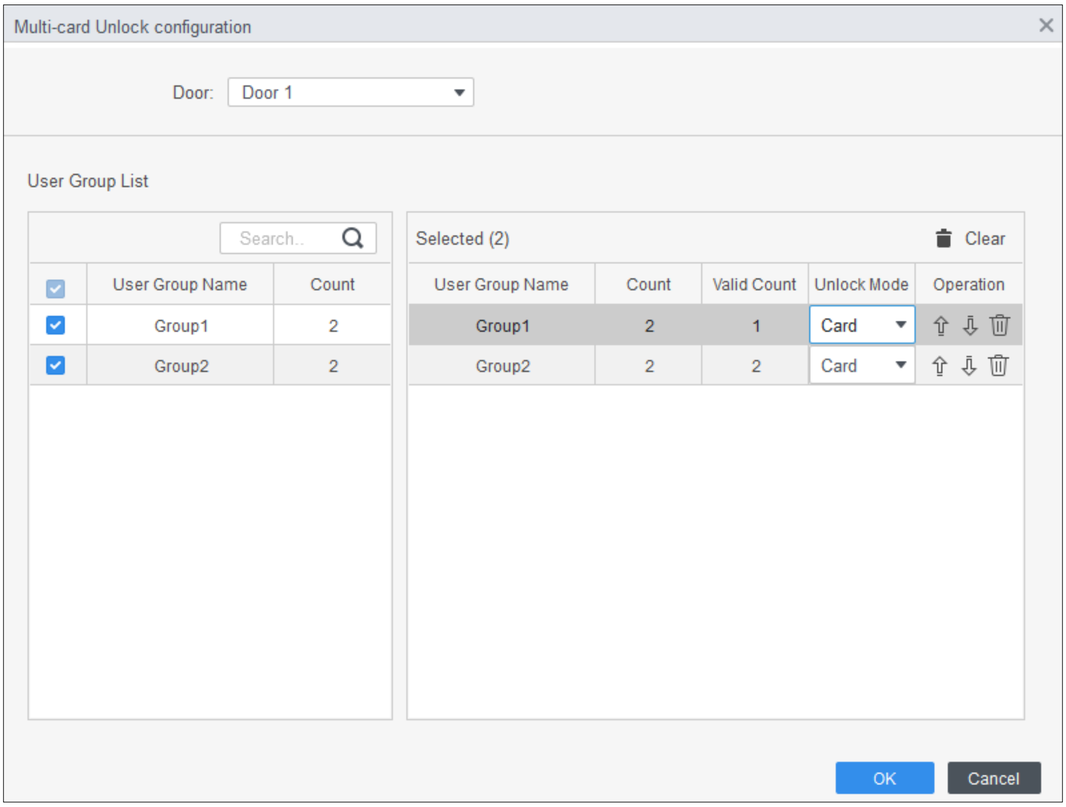
Selected (0) Clear

User Group Name	Count	Valid Count	Unlock Mode	Operation

2) Select the door.

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

Figure 5-5 Multi card unlock configuration (2)



Multi-card Unlock configuration

Door: Door 1

User Group List

Search..

☑	User Group Name	Count
☑	Group1	2
☑	Group2	2

Selected (2) Clear

User Group Name	Count	Valid Count	Unlock Mode	Operation
Group1	2	1	Card	⇧ ⇩ 🗑
Group2	2	2	Card	⇧ ⇩ 🗑

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.

The valid count refers to the number of users in each group that must be on site to swipe their cards. Take 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.

5) Click **OK**.

Step 5 (Optional) Click . The icon changing into indicates **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 exit from the specific doors. For the same person, an entry record must pair with an exit record. If someone has entered by tailing someone else, which means there is no entry record, this person cannot unlock the door for exit.

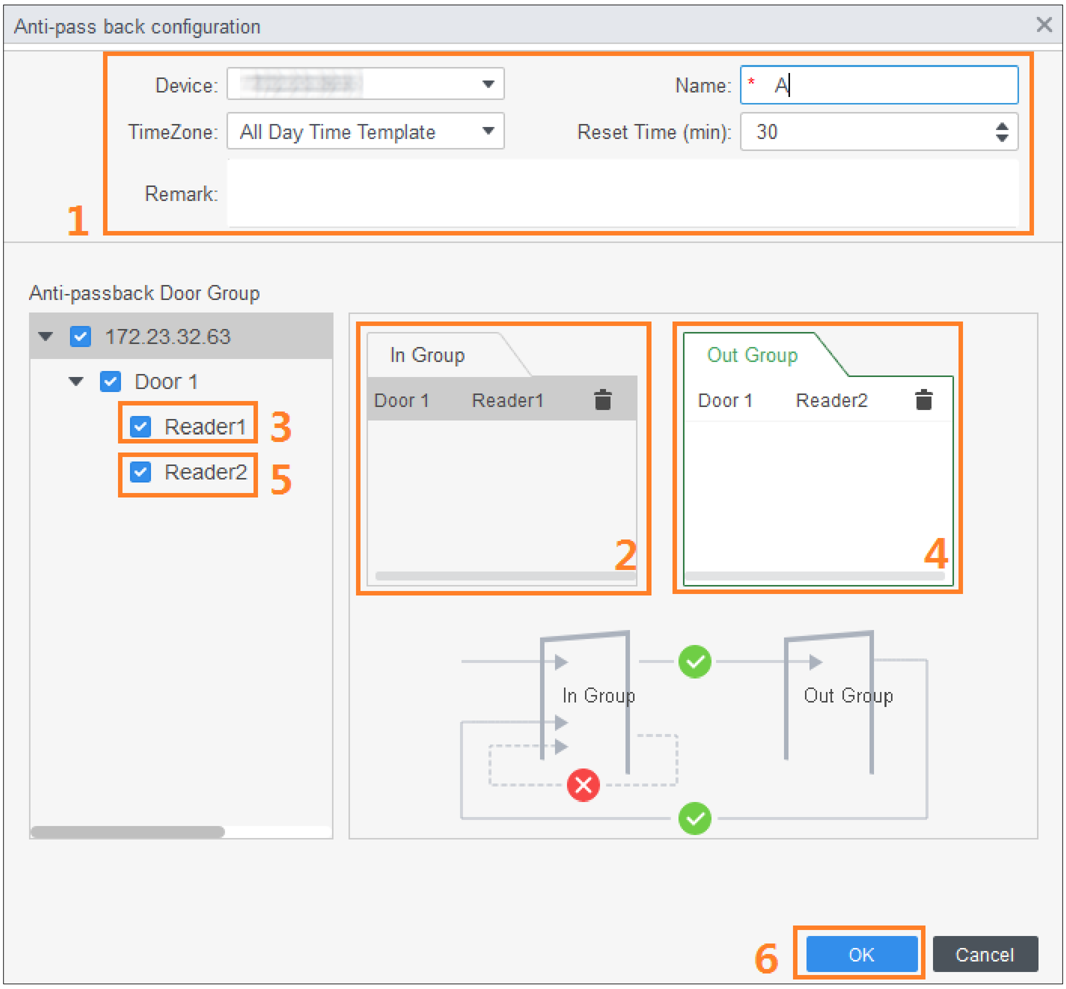
Step 1 Select **Access Configuration > Advanced Config**.

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 select the corresponding reader. And then click **Out Group** and select the corresponding reader.
5) Click **OK**. And then the configuration will issue to device and take effect.

Figure 5-6 Anti-pass back configuration



Anti-pass back configuration

Device: [redacted]

Name: * A

TimeZone: All Day Time Template

Reset Time (min): 30

Remark:

Anti-passback Door Group

- ☑ 172.23.32.63
  - ☑ Door 1
    - ☑ Reader1
    - ☑ Reader2

In Group	
Door 1	Reader1

Out Group	
Door 1	Reader2

Step 4 (Optional) Click ○. The icon changing into ● indicates **Anti-passback** is enabled.

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

5.4 Inter-door Lock

One A&C central 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**.

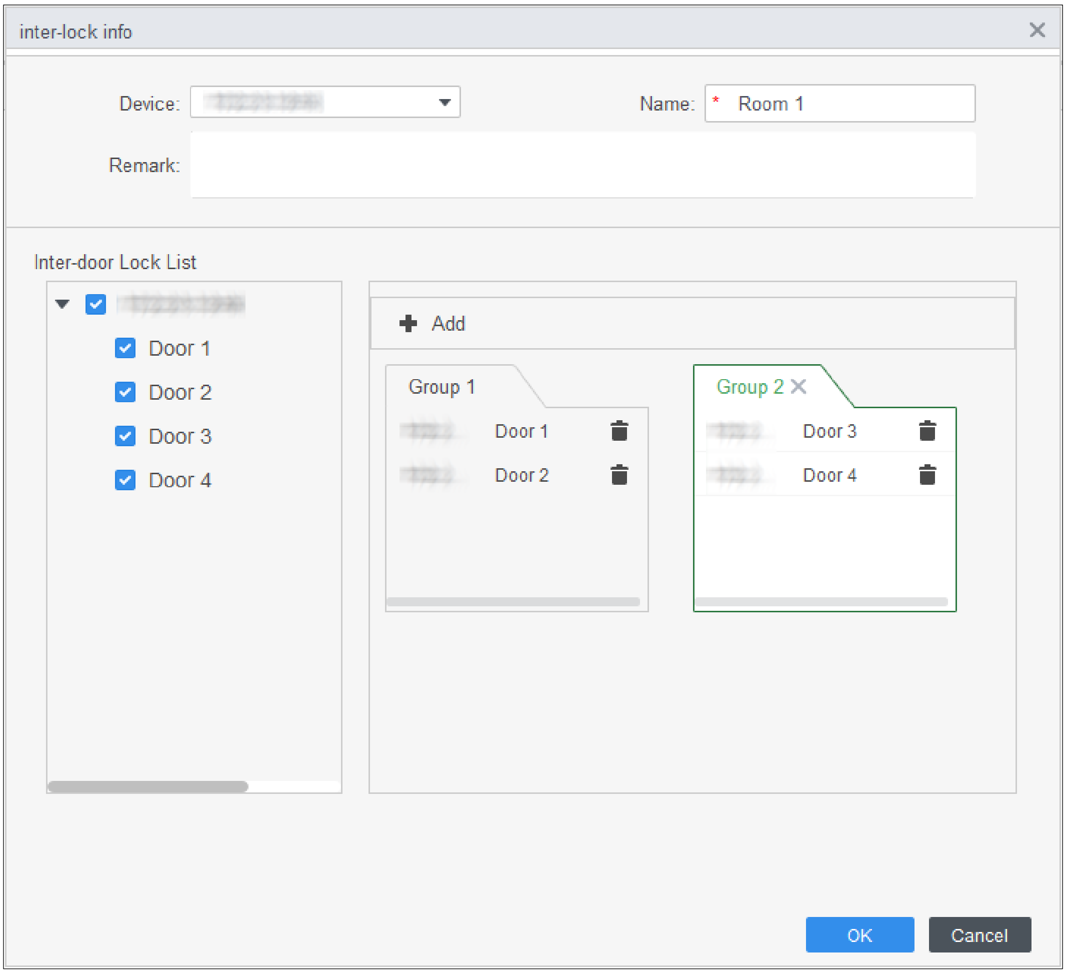
Step 2 Click the **Inter-Lock** tab.

Step 3 Click **Add**.

Step 4 Configure parameters and 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 ✕
Door 3
Door 4

OK Cancel

Step 5 (Optional) Click ⬛. The icon changing into ⬛ indicates **Inter-door Lock** is enabled.

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

6 Access Controller Configuration

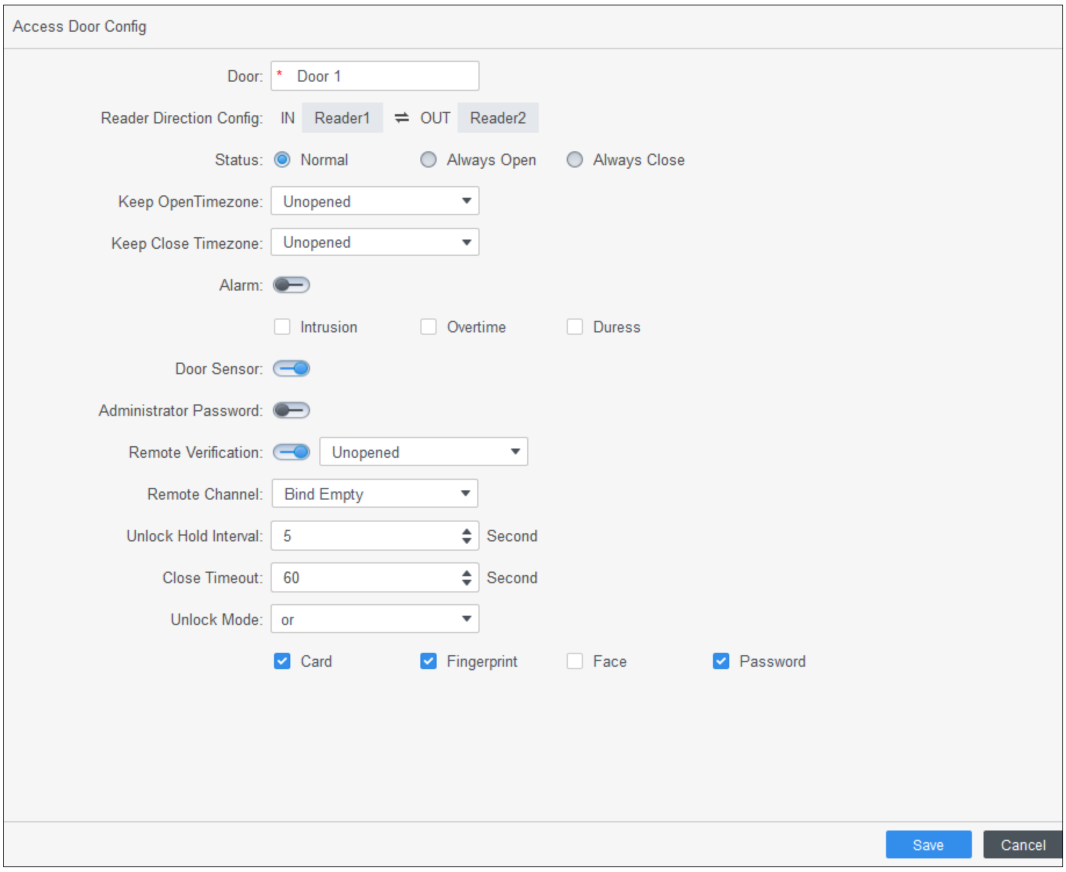
You can configure access door, such as reader direction, door status and unlock mode.

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



Access Door Config

Door: * Door 1

Reader Direction Config: IN Reader1 ⇌ OUT Reader2

Status: ● Normal ○ Always Open ○ Always Close

Keep OpenTimezone: Unopened

Keep Close Timezone: Unopened

Alarm: off

□ Intrusion □ Overtime □ Duress

Door Sensor: on

Administrator Password: off

Remote Verification: on Unopened

Remote Channel: Bind Empty

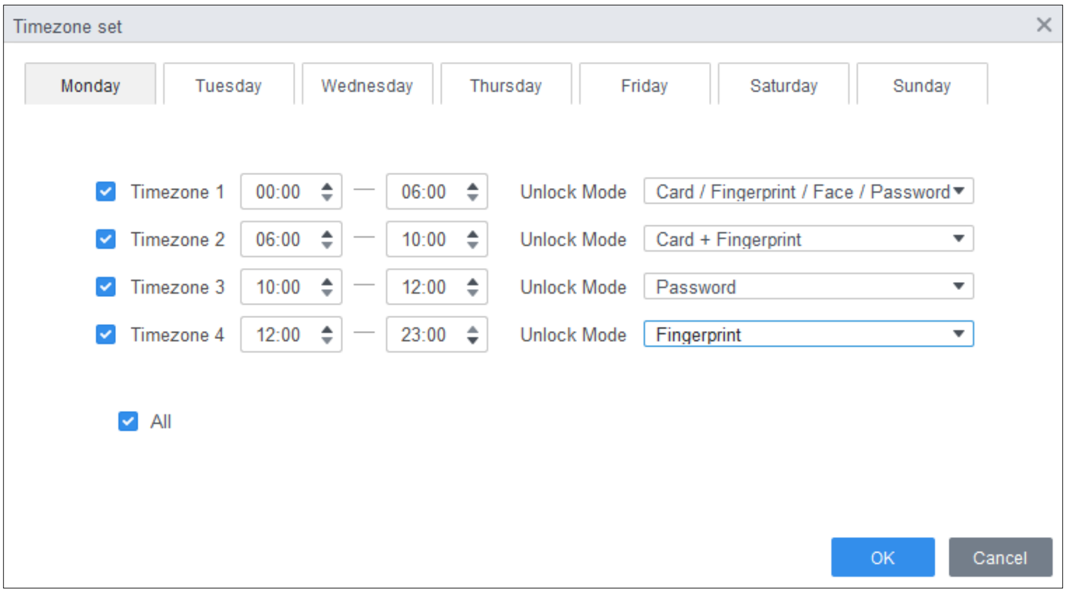
Unlock Hold Interval: 5 Second

Close Timeout: 60 Second

Unlock Mode: or

☑ Card ☑ Fingerprint □ Face ☑ Password

Figure 6-2 Unlock by time period



Timezone set

☑	Timezone 1	00:00	06:00	Unlock Mode	Card / Fingerprint / Face / Password
☑	Timezone 2	06:00	10:00	Unlock Mode	Card + Fingerprint
☑	Timezone 3	10:00	12:00	Unlock Mode	Password
☑	Timezone 4	12:00	23:00	Unlock Mode	Fingerprint

☑ All

Table 6-1 Parameters of access door

Parameter	Description
Door	Enter door name.
Reader Direction	Click ⇌ to set reader direction according to actual situations.
Status	Set door status, including **Normal**, **Always Open** and **Always Close**. 📖 It is not the actual door status because the SmartPSS-AC can only send commands to the device. If you want to know the actual door status, enable door sensor.
Keep Open Timezone	Select time template when door is always opened.
Keep Close Timezone	Select 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-AC 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-AC during the template periods.
Remote Channel	Set the linked video channel of access controllers. After setting, when viewing the video of access controller, the real-time video of the pre-defined video channel will be displayed.
Unlock Hold Interval	Set the unlock holding interval. The door will auto 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	Select unlock mode as needed. ● Select **And** and select unlock methods. You need to satisfy all the configured methods at the same time to open the door. ● Select **Or** and select unlock methods. You can open the door in any way you configured.. ● Select **Unlock by time period** and 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-AC and door devices. Before viewing, extract historical events on the door devices to ensure that all events are searched.

Step 1 Add the needed personnel to the SmartPSS-AC.

Step 2 Click **Access Configuration** > **History Event** on the homepage.

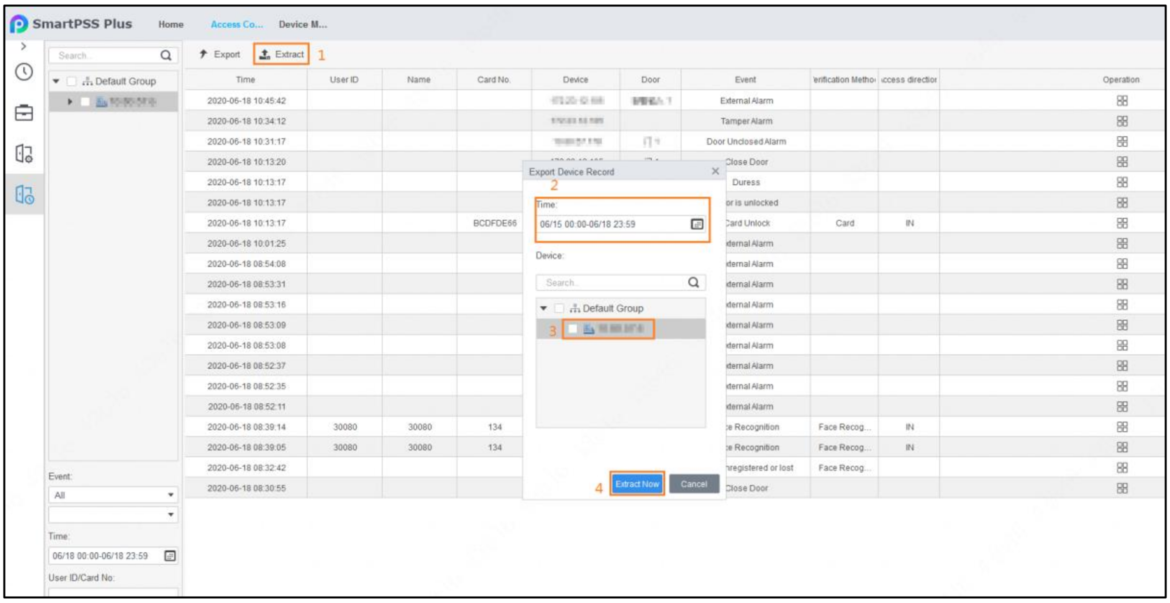
Step 3 Click on the **Access Manager** interface.

Step 4 Extract events from door device to the local. Click **Extract**, set the time, select the door device, and then click **Extract Now**.

7) 📖

You can select multiple devices at one time to extract events.

Figure 7-1 Extract events



Event: All

Time: 06/18 00:00-06/18 23:59

User ID/Card No:

Time	User ID	Name	Card No.	Device	Door	Event	erification Metho	ccess directio	Operation
2020-06-18 10:45:42				[redacted]	[redacted]	External Alarm			⊞
2020-06-18 10:34:12				[redacted]		Tamper Alarm			⊞
2020-06-18 10:31:17				[redacted]	[redacted]	Door Unclosed Alarm			⊞
2020-06-18 10:13:20						Close Door			⊞
2020-06-18 10:13:17						Duress			⊞
2020-06-18 10:13:17						or is unlocked			⊞
2020-06-18 10:13:17			BCDFDE66			Card Unlock	Card	IN	⊞
2020-06-18 10:01:25						xternal Alarm			⊞
2020-06-18 08:54:08						xternal Alarm			⊞
2020-06-18 08:53:31						xternal Alarm			⊞
2020-06-18 08:53:16						xternal Alarm			⊞
2020-06-18 08:53:09						xternal Alarm			⊞
2020-06-18 08:53:08						xternal Alarm			⊞
2020-06-18 08:52:37						xternal Alarm			⊞
2020-06-18 08:52:35						xternal Alarm			⊞
2020-06-18 08:52:11						xternal Alarm			⊞
2020-06-18 08:39:14	30080	30080	134			e Recognition	Face Recog...	IN	⊞
2020-06-18 08:39:05	30080	30080	134			e Recognition	Face Recog...	IN	⊞
2020-06-18 08:32:42						nregistered or lost	Face Recog...		⊞
2020-06-18 08:30:55						Close Door			⊞

Export Device Record

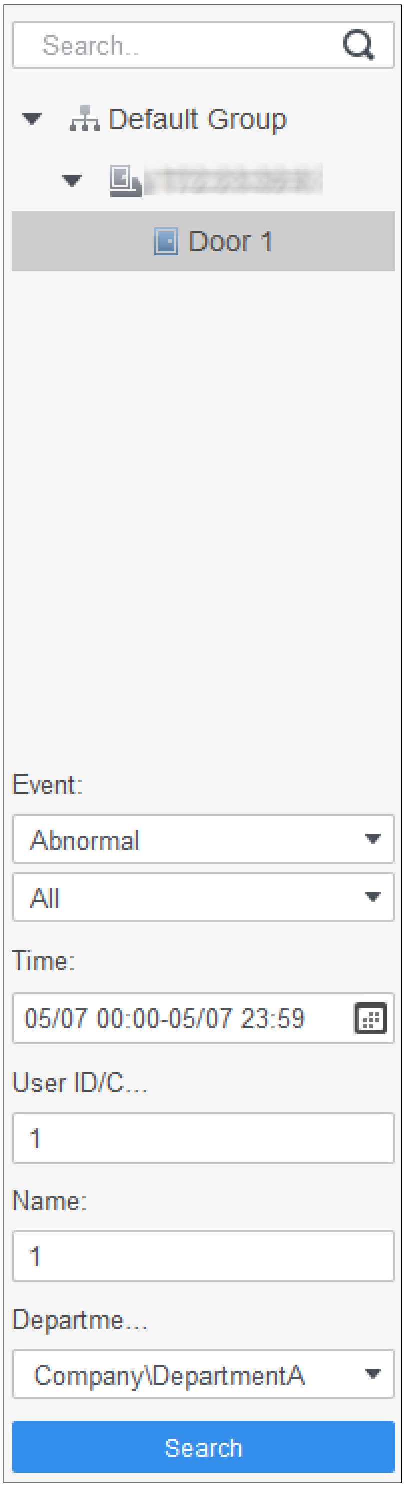
Time: 06/15 00:00-06/18 23:59

Device:

Default Group

Step 5 Set filtering conditions, and then click **Search**.

Figure 7-2 Search for events by filtering conditions



[redacted]

Event:

Abnormal

All

Time:

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

User ID/C...

1

Name:

1

Departme...

Company\DepartmentA

Step 6 (Optional) Click **Export**, and then operate according to instructions to save the searched door events to the local.

8 Access Management

8.1 Remotely Opening and Closing Door

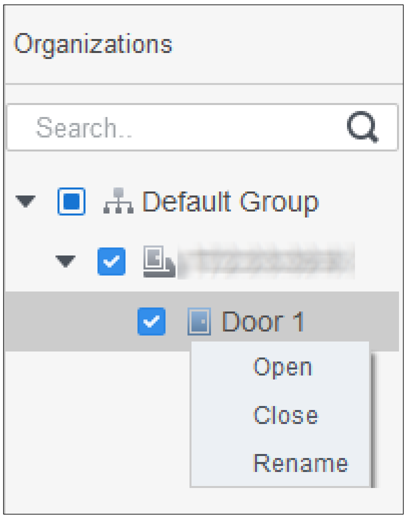
After access configuration, you can remotely control door through SmartPSS-AC.

Step 1 Click **Access Manager** on the homepage. (Or click **Access Guide >** 📋).

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

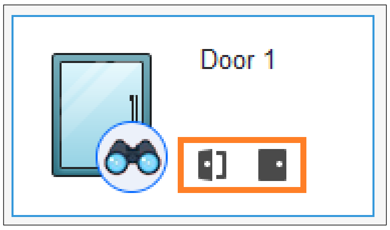
- Method 1: Select the door, right click and select **Open**.

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 by **Event Info** list. For details, see "7 Viewing Historical Event."

📖

- Event filtering: Select the event type in the **Event Info**, and the event list displays events of the selected types. For example, select **Alarm**, and the event list only displays alarm events.
- Event refresh locking: Click 🔓 to the right of **Event Info** to lock or unlock the event list, and then the real-time events cannot be viewed.
- Event deleting: Click 🗑 to the right of **Event Info** to clear all events in the event list.

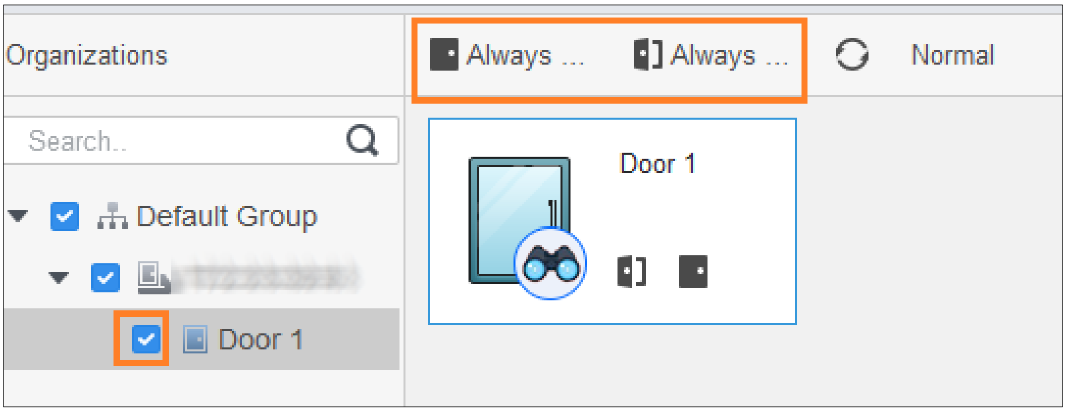
8.2 Setting Always Open and Always Close

After setting always open or always close, the door is open or closed all the time and cannot be controlled manually. If you want to manually control the door again, click **Normal** to reset the door status.

Step 1 Click **Access Manager** on the homepage. (Or click **Access Guide >** 🗒).

Step 2 Select the needed door, and then click **Always Open** or **Always Close**.

Figure 8-3 Set always open or always close



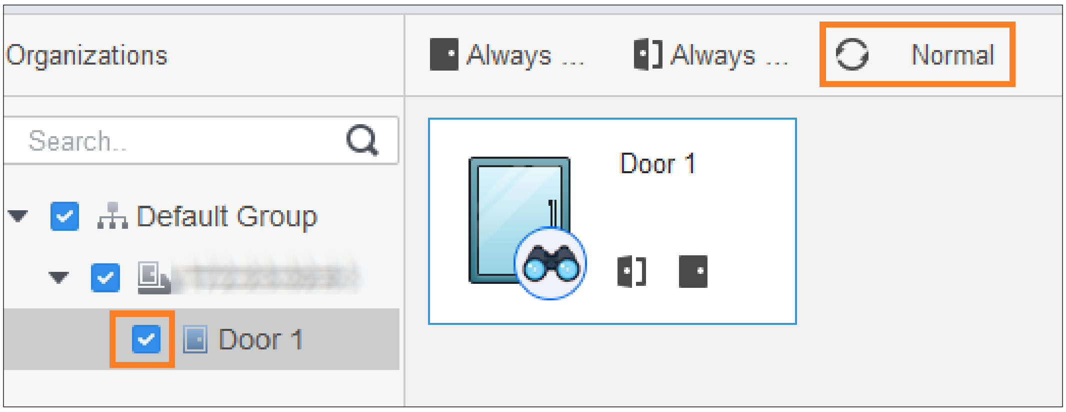
8.3 Resetting Door Status

Click **Normal** to reset the door status, if you want to manually control the door again when you have clicked **Always Open** or **Always Close**.

Step 1 Click **Access Manager** on the homepage. (Or click **Access Guide >** 🗒).

Step 2 Select the needed door, and then click **Normal**. And then follow the on-screen instructions to operate.

Figure 8-4 Reset door status



9 Event Configuration

By event configuration, you can make software linkages, such as alarm sound, mail sending and alarm linkages.

- Configure external alarm linkages connected to the access controller, such as smoke alarm.
- Configure linkages of access controller events.
  - ◇ Alarm event
  - ◇ Abnormal event
  - ◇ Normal event

For anti-pass back function, set the anti-pass back mode in **Abnormal** of **Event Config**, and then configure the parameters in **Advanced Config**. For details, see "5 Advanced Functions Configuration."

Step 1 Click **Event Config** on the homepage.

Step 2 Select the needed door and select **Alarm Event > Intrusion Event**.

Step 3 Click ○ to the right of **Intrusion Alarm** to enable the function.

Step 4 Configure intrusion alarm linage actions as needed.

- Enable alarm sound.

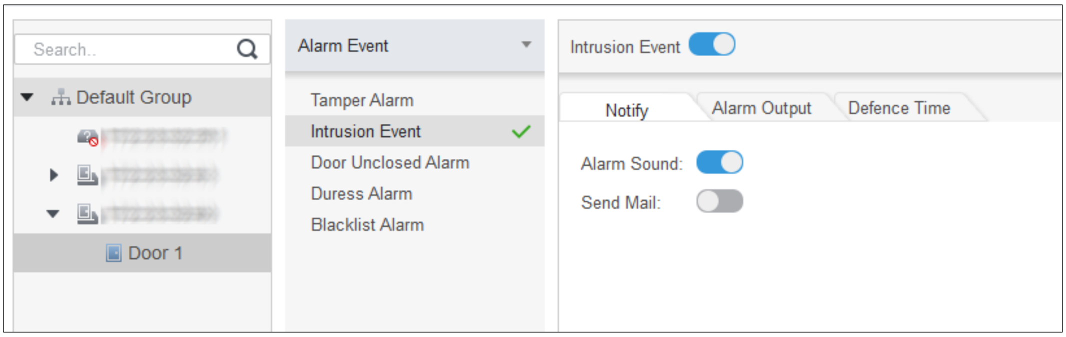
  Click the **Notify** tab, and click ○ to the right of **Alarm Sound**. When intrusion event happens, the access controller warns by alarm sound.

- Send alarm mail.

1) Enable **Send Mail** and confirm to set SMTP, you will automatically go to the **System Settings** interface.
2) Configure SMTP parameters, such as server address, port number, and encrypt mode.

   When intrusion event happens, the system automatically sends alarm mails to the specified receiver.

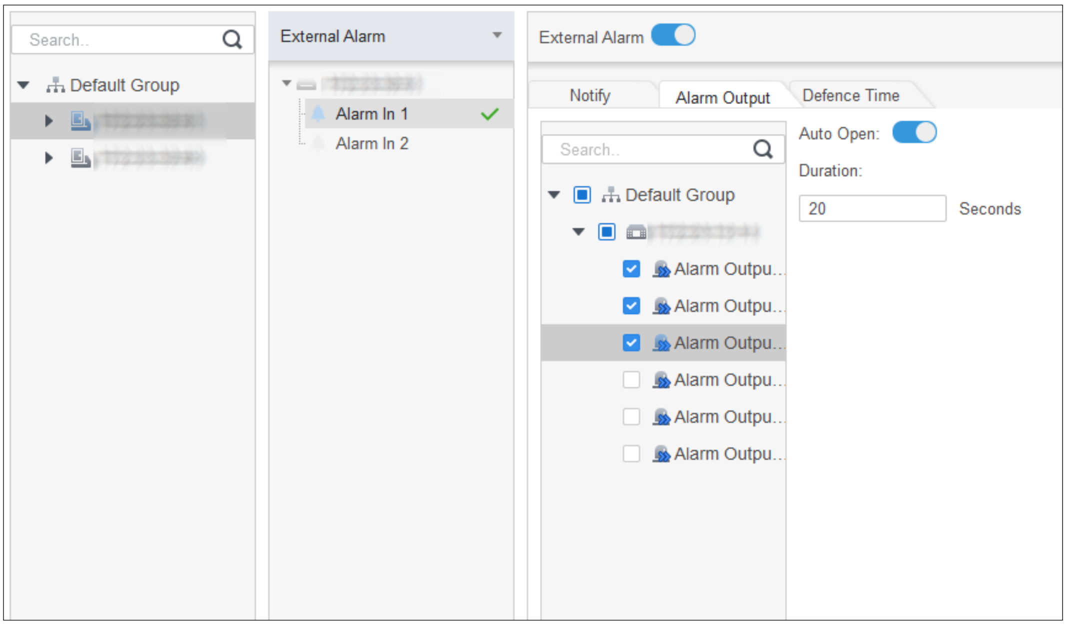
Figure 9-1 Configure intrusion alarm



- Configure alarm I/O.

1) Click Alarm Output tab.
2) Select the device which supports alarm in, then select alarm-in interface, and then enable **External Alarm**.
3) Select the device which supports alarm out, then select alarm-out interface.
4) Enable **Auto Open** for the alarm linkage.
5) Set the duration.

Figure 9-2 Configure alarm linkage



Search..

▾ Default Group
- ▸ [redacted]
- ▸ [redacted]

External Alarm ▾

▾ [redacted]
- Alarm In 1 ✓
- Alarm In 2

External Alarm ●

Notify | Alarm Output | Defence Time

Search..

▾ ■ Default Group
- ▾ ■ [redacted]
  - ☑ Alarm Outpu...
  - ☑ Alarm Outpu...
  - ☑ Alarm Outpu...
  - □ Alarm Outpu...
  - □ Alarm Outpu...
  - □ Alarm Outpu...

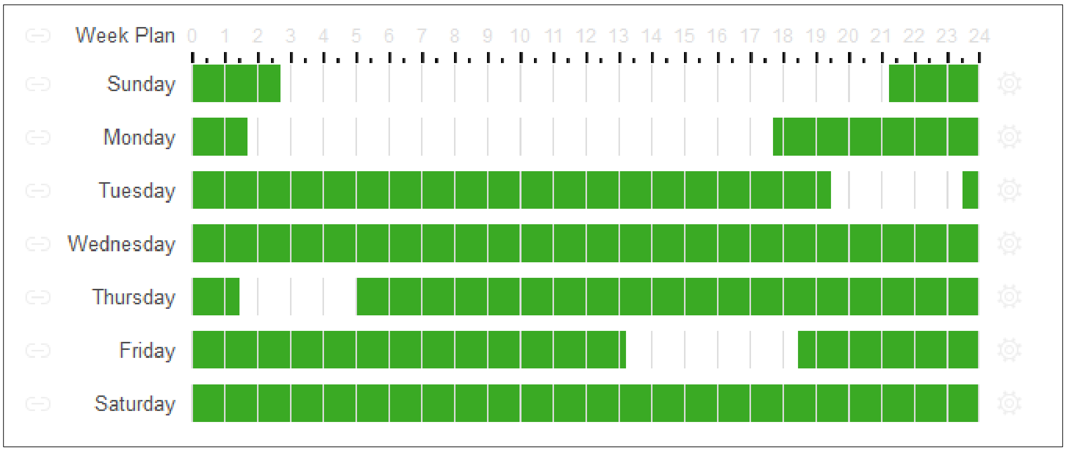
Auto Open: ●

Duration:

20 Seconds

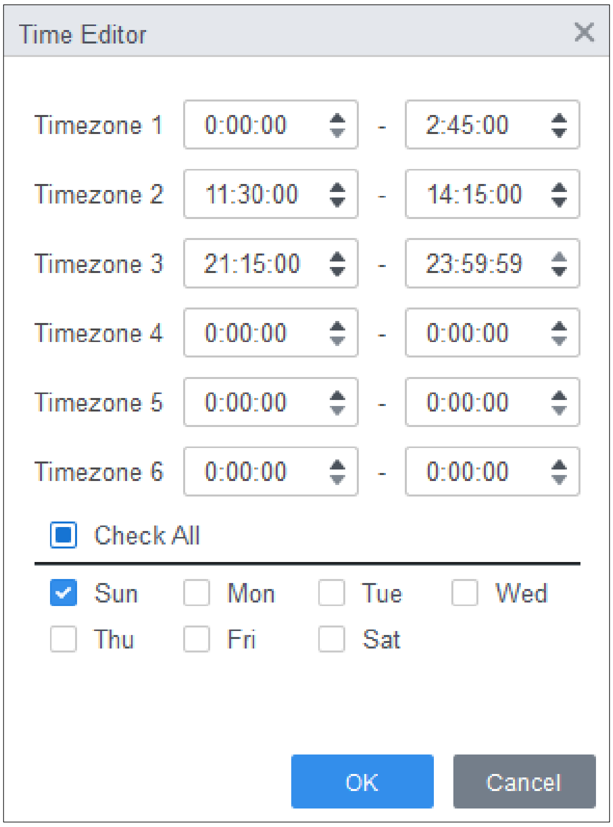
- Set defence time. There are two methods.
  - ◇ Method 1: Move the cursor to set time periods. When the cursor is pencil, click to add periods; when the cursor is eraser, click to minus periods. The green area is the periods with defence.

Figure 9-3 Set defence time (method 1)



- ◇ Method 2: Click ⚙ to set periods, and then click **OK**.

Figure 9-4 Set defence time (method 2)



Timezone 1	0:00:00	-	2:45:00
Timezone 2	11:30:00	-	14:15:00
Timezone 3	21:15:00	-	23:59:59
Timezone 4	0:00:00	-	0:00:00
Timezone 5	0:00:00	-	0:00:00
Timezone 6	0:00:00	-	0:00:00

■ Check All

☑ Sun ☐ Mon ☐ Tue ☐ Wed

☐ Thu ☐ Fri ☐ Sat

Step 5 (Optional) Click **Copy To**, select the access controller to be applied on, and then click **OK**.

Step 6 Click **Save**.

Appendix 1 Cybersecurity Recommendations

Cybersecurity is more than just a buzzword: it’s something that pertains to every device that is connected to the internet. IP video surveillance is not immune to cyber risks, but taking basic steps toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations on how to create a more secured security system.

Mandatory actions to be taken for basic equipment network security:

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. **Update Firmware and Client Software in Time**

   - According to the standard procedure in Tech-industry, we recommend to keep your equipment (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the equipment is connected to the public network, it is recommended to enable the “auto-check for updates” function to obtain timely information of firmware updates released by the manufacturer.
   - We suggest that you download and use the latest version of client software.

"Nice to have" recommendations to improve your equipment network security:

1. **Physical Protection**

   We suggest that you perform physical protection to equipment, especially storage devices. For example, place the equipment 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, unauthorized connection of removable equipment (such as USB flash disk, serial port), etc.

2. **Change Passwords Regularly**

   We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

3. **Set and Update Passwords Reset Information Timely**

   The equipment supports password reset function. Please set up related information for password reset in time, including the end user’s mailbox and password protection questions. 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.

4. **Enable Account Lock**

   The account lock feature is enabled by default, and we recommend you 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.

5. **Change Default HTTP and Other Service Ports**

We suggest you to change default HTTP and other service ports into any set of numbers between 1024~65535, reducing the risk of outsiders being able to guess which ports you are using.

6. **Enable HTTPS**

   We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

7. **Enable Whitelist**

   We suggest you to enable whitelist 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 whitelist.

8. **MAC Address Binding**

   We recommend you to bind the IP and MAC address of the gateway to the equipment, thus reducing the risk of ARP spoofing.

9. **Assign Accounts and Privileges Reasonably**

   According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

10. **Disable Unnecessary Services and Choose Secure Modes**

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

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

    - SNMP: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
    - SMTP: Choose TLS to access mailbox server.
    - FTP: Choose SFTP, and set up strong passwords.
    - AP hotspot: Choose WPA2-PSK encryption mode, and set up strong passwords.

11. **Audio and Video Encrypted Transmission**

    If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

    Reminder: encrypted transmission will cause some loss in transmission efficiency.

12. **Secure Auditing**

    - Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
    - Check equipment log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

13. **Network Log**

    Due to the limited storage capacity of the equipment, the stored log is limited. If you need to save the log for a long time, it is recommended that you enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

14. **Construct a Safe Network Environment**

    In order to better ensure the safety of equipment and reduce potential cyber risks, we recommend:

    - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
    - The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is

suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.

- Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
- It is recommended that you enable your device's firewall or blacklist and whitelist feature to reduce the risk that your device might be attacked.