


# VIP Vision Access Controller User's Manual

Four-door One-way Compact Access Controller - ACCON - 2C41
Two-door Two-way Professional Access Controller - ACCON - 2P22
Four-door One-way Professional Access Controller - ACCON - 2P41
Four-door Two-way Professional Access Controller - ACCON - 2P42
Eight-door One-way Professional Access Controller - ACCON - 2P81

# Table of Contents

# Important Safeguards and Warnings

Please read the following safeguards and warnings carefully before using the product in order to avoid damages losses and body injuries.

## Note:

- Do not install the device at position exposed to sunlight or in high temperature. Temperature rise in device may cause fire.
- Do not expose the device to lampblack, steam or dust. Otherwise it may cause fire or electric shock.
- The device must be installed on solid and flat surface in order to guarantee safety under load and earthquake. Otherwise, it may cause device to fall off or turnover.
- Do not drop or splash liquids onto the device, and do not place container with full liquid on the device to prevent liquid spilling from entering the device.
- Do not block air vent of the device or ventilation around the device. Otherwise, temperature in device will rise and may cause fire.
- Use the device only within rated input and output range.
- Install, assemble and disassemble by qualified personnel only.
- Transport, use and store the product under appropriate temperature and humidity.

## Warning:

- Please use battery properly to avoid fire, explosion and other dangers.
- Please replace used battery with battery of the same type.
- Do not use power line other than the one specified. Please use it properly within rated range. Otherwise, it may cause fire or electric shock.
- Always connect a ground (earth) wire to the access controller's chassis. Connecting the unit without a protective ground, or interruption of the grounding can cause harm to the unit or to the equipment connected to it. (2P series only)

## Notice Information

- All the designs, software and instructions here are subject to change without prior written notice.
- We would not be responsible for any damages and losses caused by improper operations or installation. Do not allow non-authorized or unqualified personnel with any kind of intervention to the product.
- All trademarks and registered trademarks are the properties of their respective owners.
- Please visit our website www.rhinoco.com.au for more information.

# 1 Pre-Installation

## 1.1 Installation Requirements & Notes

You must install the Smart PSS on a PC to add users, set up access rights and other functions of the access controller.

You must change the IP address of the PC network card in order to control the access controller. Refer to the Smart PSS User's Manual for details.

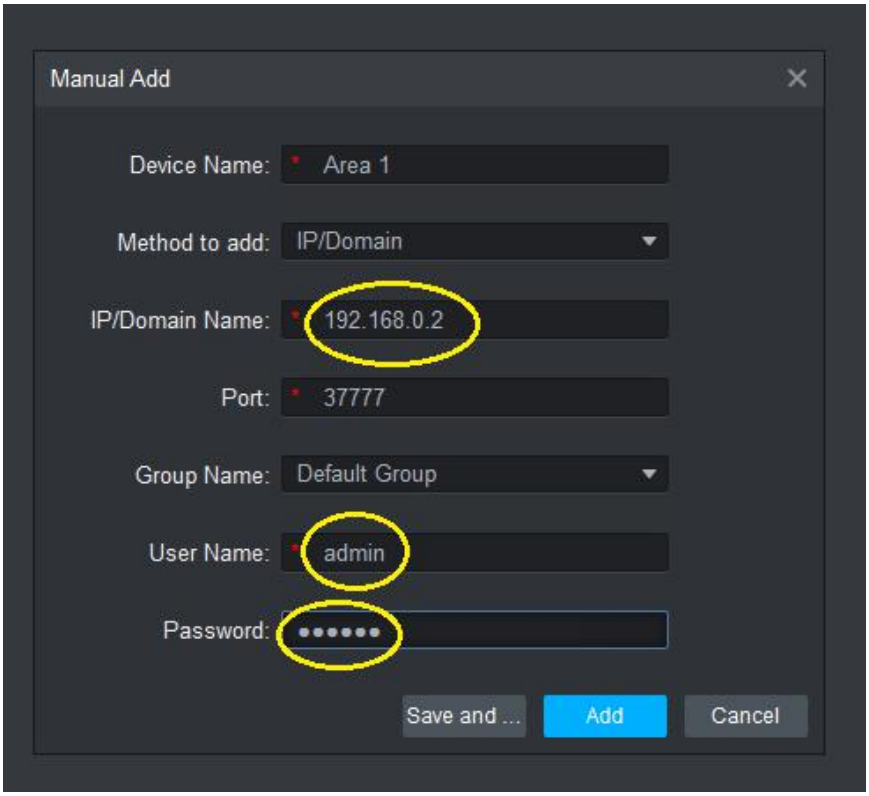
## 1.2 Factory Default Settings

You must enter the correct IP/Domain Name, User Name and Password to add the access controller to the PC platform.

The default settings are as follow:

IP/Domain Name: 192.168.0.2
User Name: admin
Password: 123456

**** If a dialogue box pops up asking for maintenance password, enter s4musvvcai*



# 1.3 Components

## Access Controller

- Supports up to 100,000 NFC cards & stores up to 150,000 events
- Supports high security NFC IC cards (13.56MHz)
- Supports NFC card readers, keypads, fingerprint readers and combinations
- Supports Wiegand or RS-485 interface to NFC card readers, keypads and fingerprint readers* (up to 4 doors)
- Intelligent functions: First card unlock, Multi-card unlock, Anti-pass back, Inter door lock, Remote verification
- Supports up to 128 normal, period and holiday schedules
- Door unlock push button inputs
- Door open/close status sensing inputs
- External alarm input(s)
- External alarm output(s)
- Internal alarms: Door time out alarm, intrusion alarm, duress alarm and tamper alarm
- Emergency features: All doors lock/unlock by two clicks
- RTC (Real Time Clock) battery backup

## RFID Card Readers & Keypads

### Fingerprint + RFID Card Reader
Model: ACRDR-2SFC

- Supports RS-485 protocol
- RFID IC card (Mifare)
- Supports cards and fingerprints
- Blue backlight
- Buzzer and Dual Colour LED indicator

### Vandal-Proof Keypad + RFID Card Reader
Model: ACRDR-2MKC

- Supports RS485 and Wiegand34 protocol
- RFID IC card (Mifare)
- Metal buttons with blue backlight
- LED indicator

| | |
|---|---|
|  | Touch Keypad + RFID Card Reader<br>Model: ACRDR-2LKC<br><br>✧ Supports RS485 and Wiegand34 protocol<br>✧ RFID IC card (Mifare)<br>✧ Sensitive touch keypad with blue backlight<br>✧ Buzzer and Dual Colour LED indicator |
|  | Waterproof RFID Card Reader<br>Model: ACRDR-2PC<br><br>✧ Supports RS485 and Wiegand34 protocol<br>✧ RFID IC card (Mifare)<br>✧ Buzzer and Dual Colour LED indicator<br>✧ Waterproof IP67 rating |
|  | Slim Waterproof RFID Card Reader<br>Model: ACRDR-2SC<br><br>✧ Supports RS485 and Wiegand34 protocol<br>✧ RFID IC card (Mifare)<br>✧ Buzzer and Dual Colour LED indicator<br>✧ Waterproof IP65 rating |
|  | Slim Waterproof RFID Card Reader + Keypad<br>Model: ACRDR-2SKC<br><br>✧ Supports RS485 and Wiegand34 protocol<br>✧ RFID IC card (Mifare)<br>✧ Buzzer and Dual Colour LED indicator<br>✧ Waterproof IP65 rating |

## Enrollment Readers

RFID Card Enrollment Reader
Model: ACENR-2C

- ✧ Plug and Play, no driver is need
- ✧ USB powered
- ✧ Buzzer and LED indicator
- ✧ Frequency: 13.56MHz

Fingerprint Enrollment Reader
Model: ACENR-2F

- ✧ Plug and Play, no driver is need
- ✧ USB powered
- ✧ Resolution: 500 dpi

## Door Release Buttons


Heavy Duty Door Release Button
Model: ACDSW100

- ✧ Sandblasted Aluminium finish
- ✧ 3 output contacts (N.O, N.C, COM)
- ✧ 3A at 36VDC max. current rating
- ✧ Mechanical design life (typical): 500,000 cycles
- ✧ Dimensions: 86 x 50 x 28.9mm

Slim, Aluminium & Stainless Steel Door Release Button
Model: ACDSW101

- ✧ Aluminium, stainless steel button
- ✧ 2 output contacts (N.O, COM)
- ✧ 3A at 36VDC max. current rating
- ✧ Mechanical design life (typical): 500,000 cycles
- ✧ Dimensions: 86 x 28 x 20mm


Aluminium Door Release Button with LEDs and Timer
Model: ACDSW101

- 3 output contacts (N.O, N.C, COM)
- Red/Green active status LEDs
- 2A at 30VAC/DC contact rating
- Adjustable timer output 1~40s
- Dimensions: 120 x 76 x 18mm

## RFID Cards

RFID IC Card
Model: ACKEY103

- High Frequency 13.56MHz RFID
- Slim
- Dimensions: 85.6 x 54 x 0.8mm

## Electric Door Strikes

Mortise Electric Door Strike
Model: ACLOC100

- Face Plate: Steel
- Keeper Depth 9.6 mm
- Lock Configuration: Fail-secure
- Door Sensor: No
- Lock Sensor: No
- Power Input: 12VDC at 400mA
- Dimensions: 160 x 31 x 31.4 mm

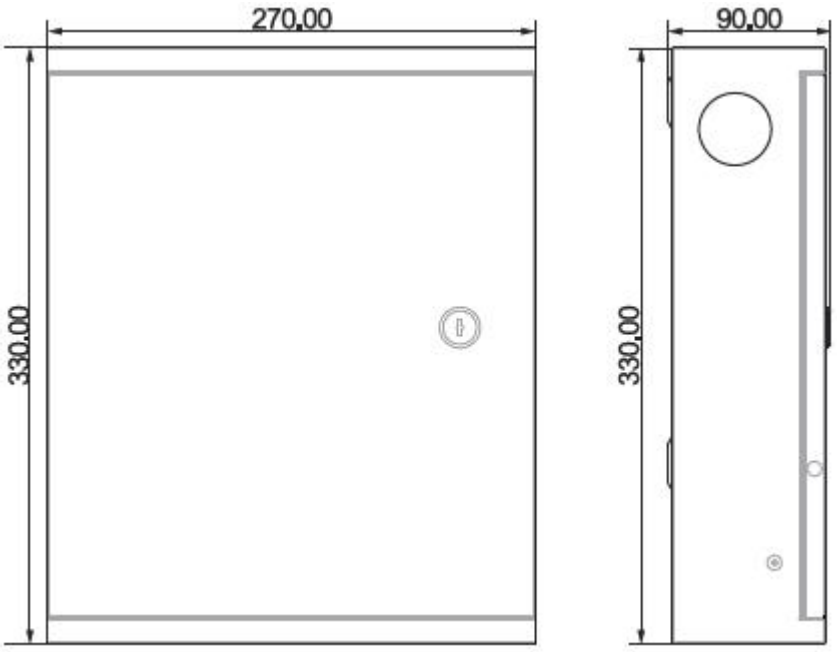
Surface Mount Electric Door Strike
Model: ACLOC101

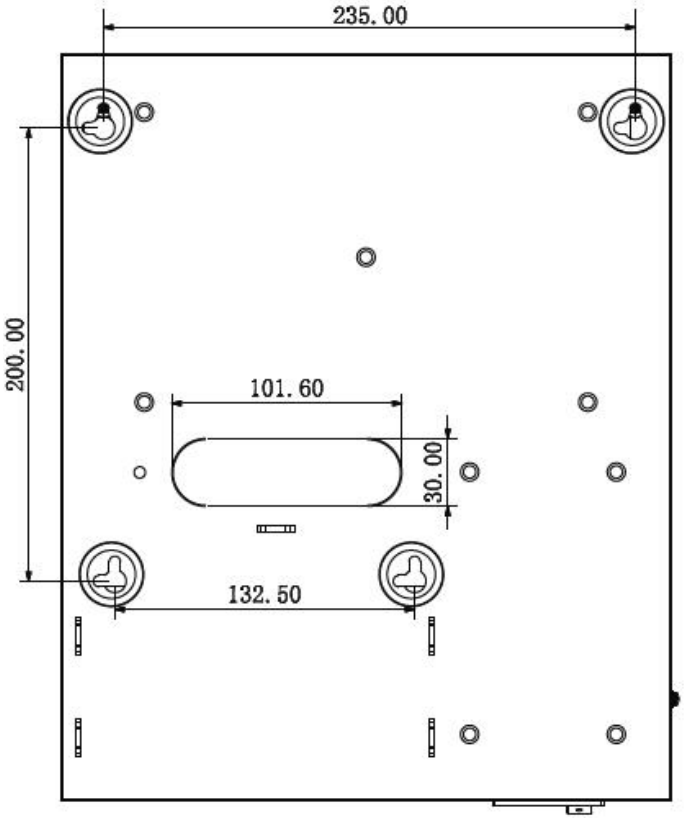
- Face Plate: Steel
- Keeper Depth 9.6 mm
- Lock Configuration: Fail-secure
- Door Sensor: No
- Lock Sensor: No
- Power Input: 12VDC at 400mA
- Dimensions: 108 x 50 x 31.4 mm

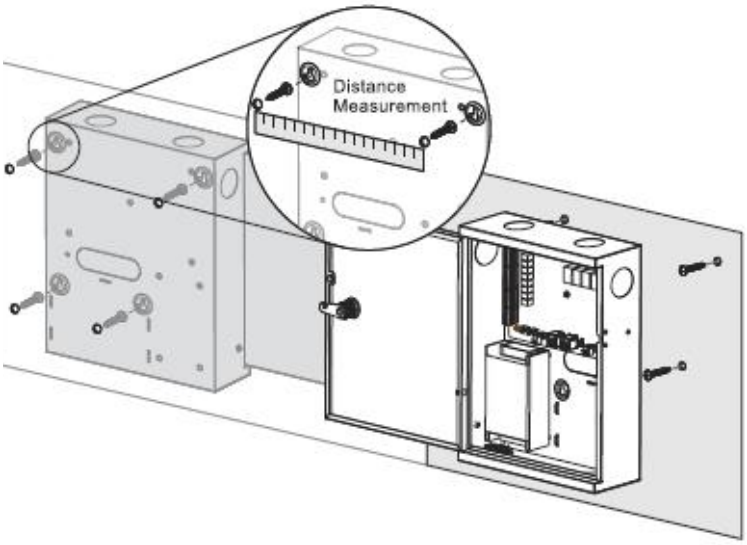
| | |
|---|---|
|  | Monitored Mortise Electric Door Strike<br>Model: ACLOC102<br><br>✧ Face Plate: Stainless Steel<br>✧ Keeper Depth: 12.7 mm<br>✧ Lock Configuration: Convertible: Fail-safe / Fail-secure<br>✧ Door Sensor: Yes<br>✧ Lock Sensor: Yes<br>✧ Power Input: 12VDC at 260mA<br>✧ Dimensions: 165 x 31 x 40.2 mm |
|  | Monitored Multi-Voltage Mortise Electric Door Strike<br>Model: ACLOC103<br><br>✧ Face Plate: Stainless Steel<br>✧ Keeper Depth: 10.8 mm<br>✧ Lock Configuration: Convertible: Fail-safe / Fail-secure<br>✧ Door Sensor: Yes<br>✧ Lock Sensor: Yes<br>✧ Power Input: 12VDC at 260mA<br>✧ Dimensions: 175 x 29 x 26 mm<br>✧ Power Input: 12/24VDC at 280/140mA<br>12/24VAC at 170/85mA |
|  | Chrome Mortise Electric Door Strike<br>Model: ACLOC104<br><br>✧ Face Plate: Chrome-plated steel<br>✧ Keeper Depth 9.6 mm<br>✧ Lock Configuration: Fail-secure<br>✧ Door Sensor: No<br>✧ Lock Sensor: No<br>✧ Power Input: 12VDC at 400mA<br>✧ Dimensions: 144.5 x 36.4 x 25 mm |

# 2 Dimensions

**Models: ACCON-2P22 ACCON-2P41**
**ACCON-2P42 ACCON-2P81**

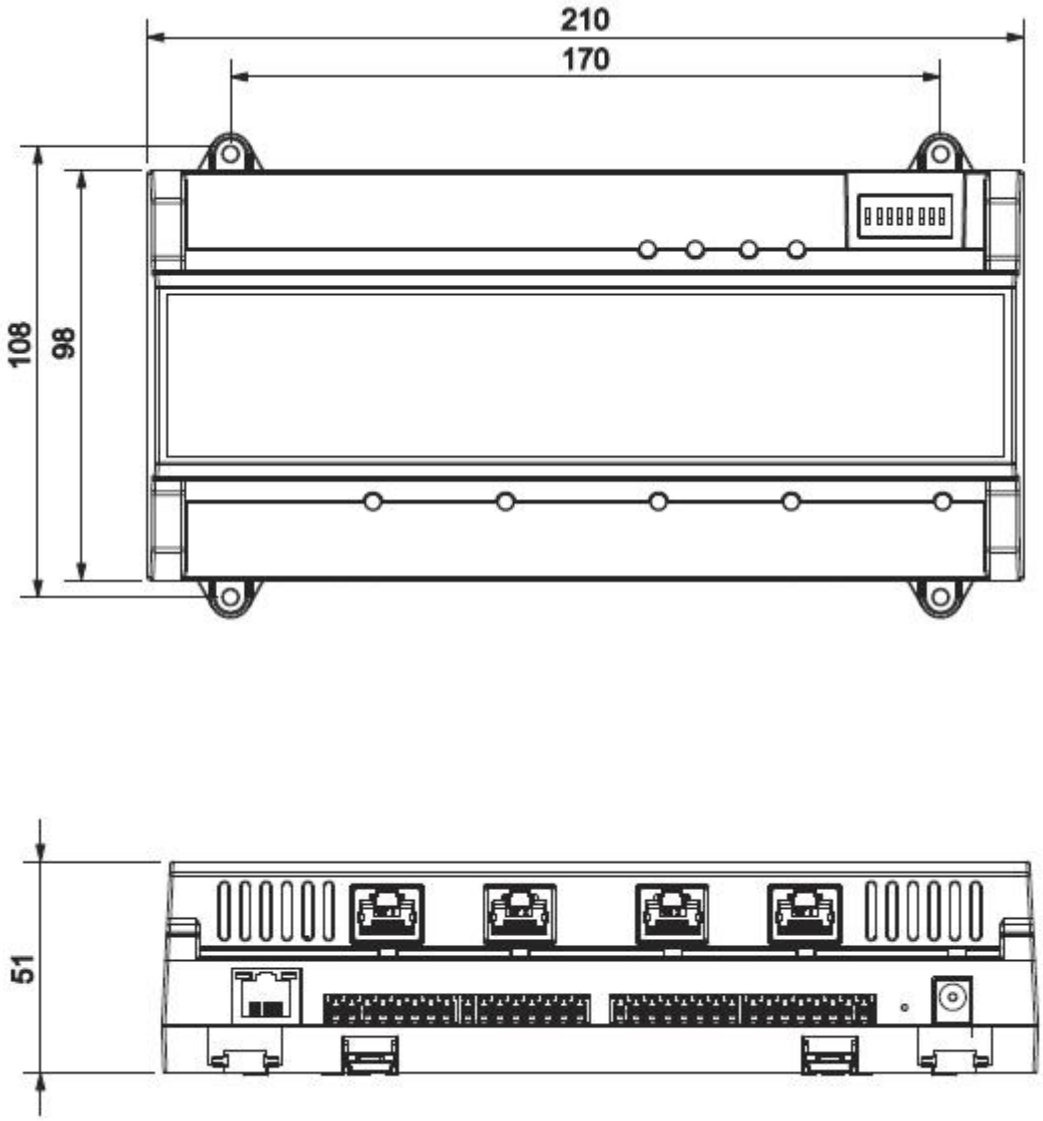



Unit: mm

**Model: ACCON-2C41**




Unit: mm

# 3 Access Controller Installation

If this is your first time installing an access controller, we recommend setting it up on the bench before installation, to familiarize yourself with the product.

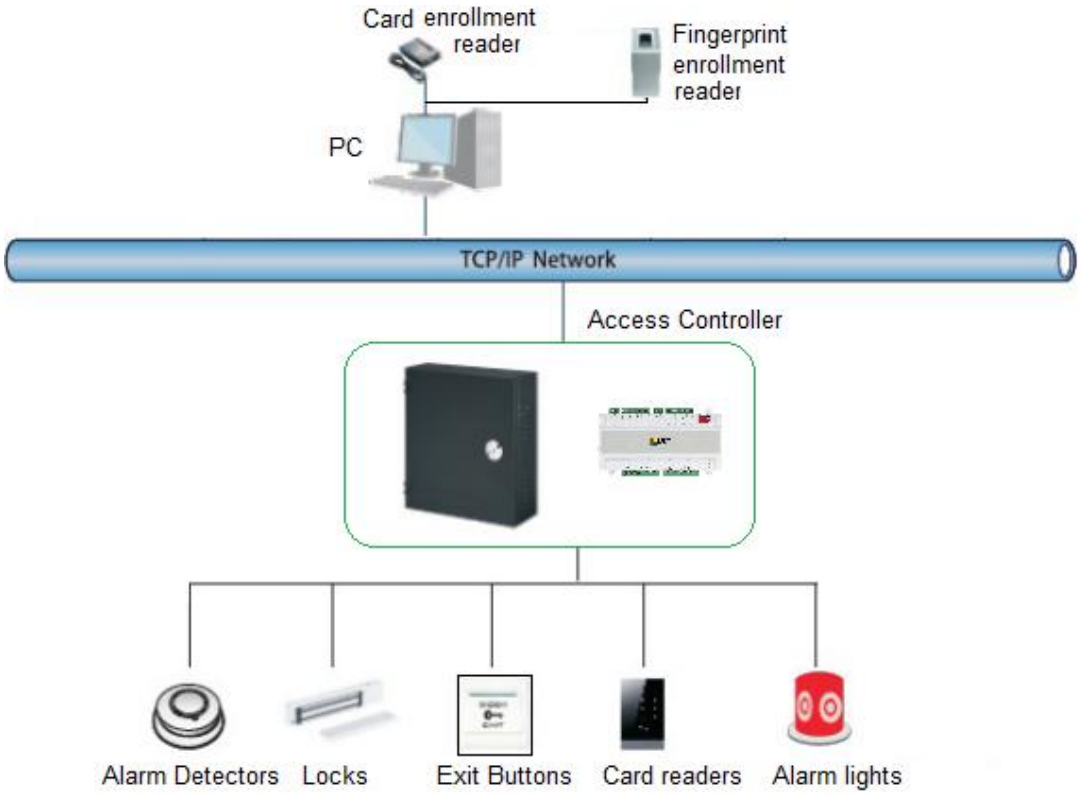
If you are setting up more than one access controller, a network switch is needed. You must use one network card (Ethernet port) for the access controller. If you need internet access, please use another Ethernet port.

The communication between the access controllers and keypads, card readers requires Cat5 cables. This is to minimize errors.

Please install separate power supply for the door locks/electric strikes. Do not use the power supply from the access controller, some electric strikes consume high current and may pull down the system voltage when the door is unlocked.

Label all cables clearly will certainly reduce the troubleshooting time. Check wiring before power up.

## 3.1 System Diagram

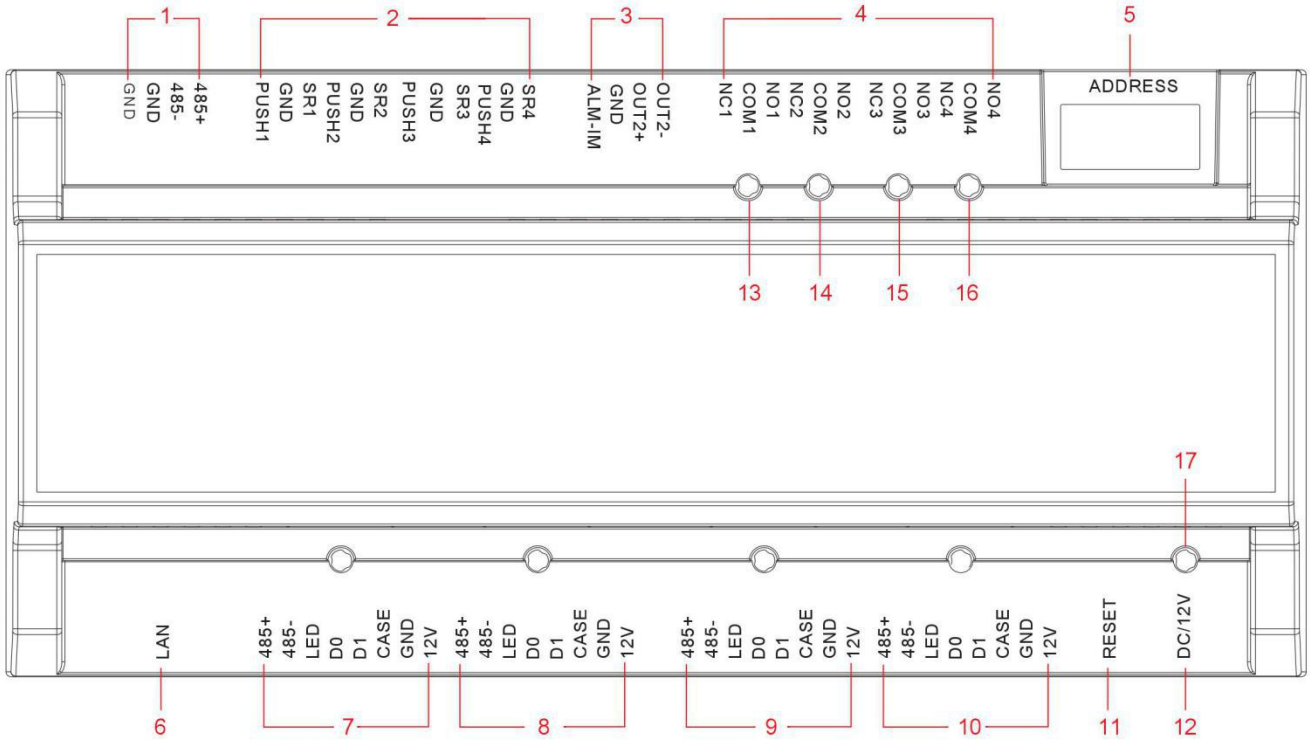



**Recommendations:**

1. Connect devices with CAT5e cables.
2. Use separate power supply for electric strikes.

# 3.2 Wiring Diagrams

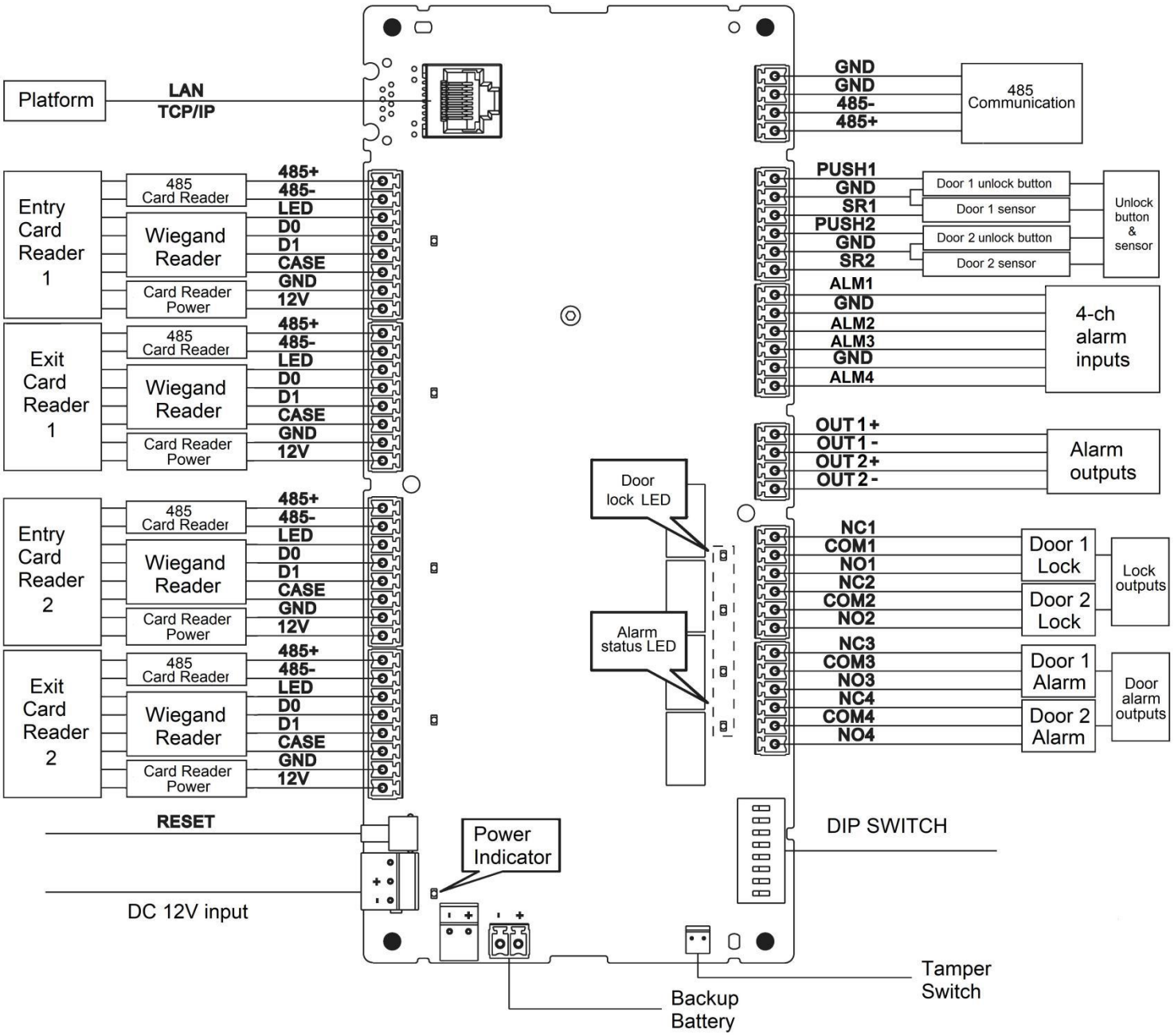
## Model: ACCON-2C41



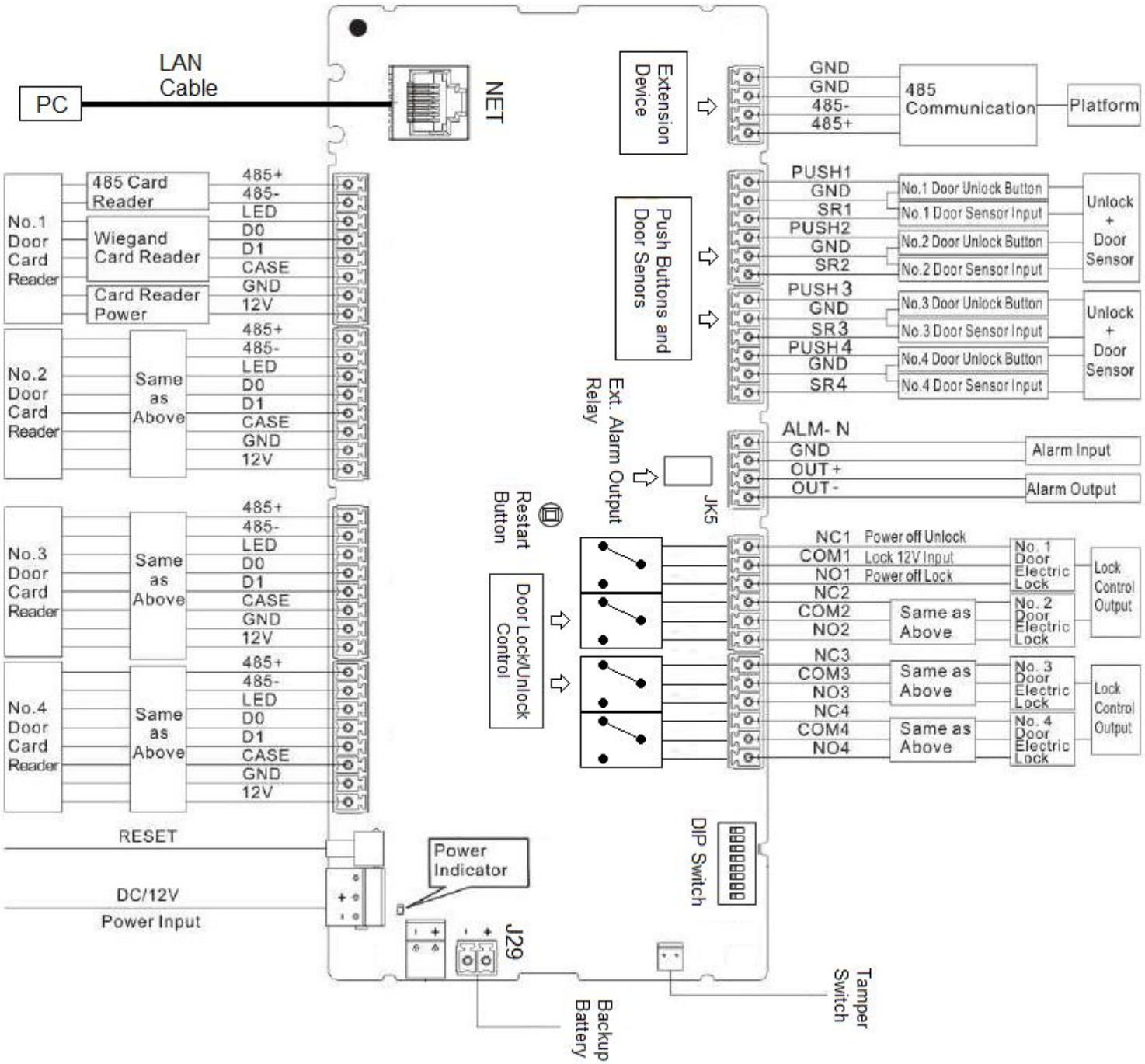

Ports are defined as:

| Port No. | Description | Port No. / Indicator | Description |
|---|---|---|---|
| 1 | RS485 communication port | 8 | Card/fingerprint reader/keypad 2 |
| 2 | Door 1 - 4 push button inputs (PB1,PB2,PB3,PB4) & Door 1 - 4 sensor inputs (SR1,SR2,SR3,SR4) | 9 | Card/fingerprint reader/keypad 3 |
| 3 | No.3, 4 doors unlock +door sensor | 10 | Card/fingerprint reader/keypad 4 |
| 4 | External alarm input (ALM-IN) /output External alarm output (OUT2+,OUT2-) | 11 | Reset button |
| 5 | DIP Switch - Use for reset to factory default settings | 12 | DC 12V input (1A) |
| 6 | Network cable input (RJ-45) | 13 - 16 | Door lock/unlock indicators |
| 7 | Card/fingerprint reader/keypad 1 | 17 | Power indicator |

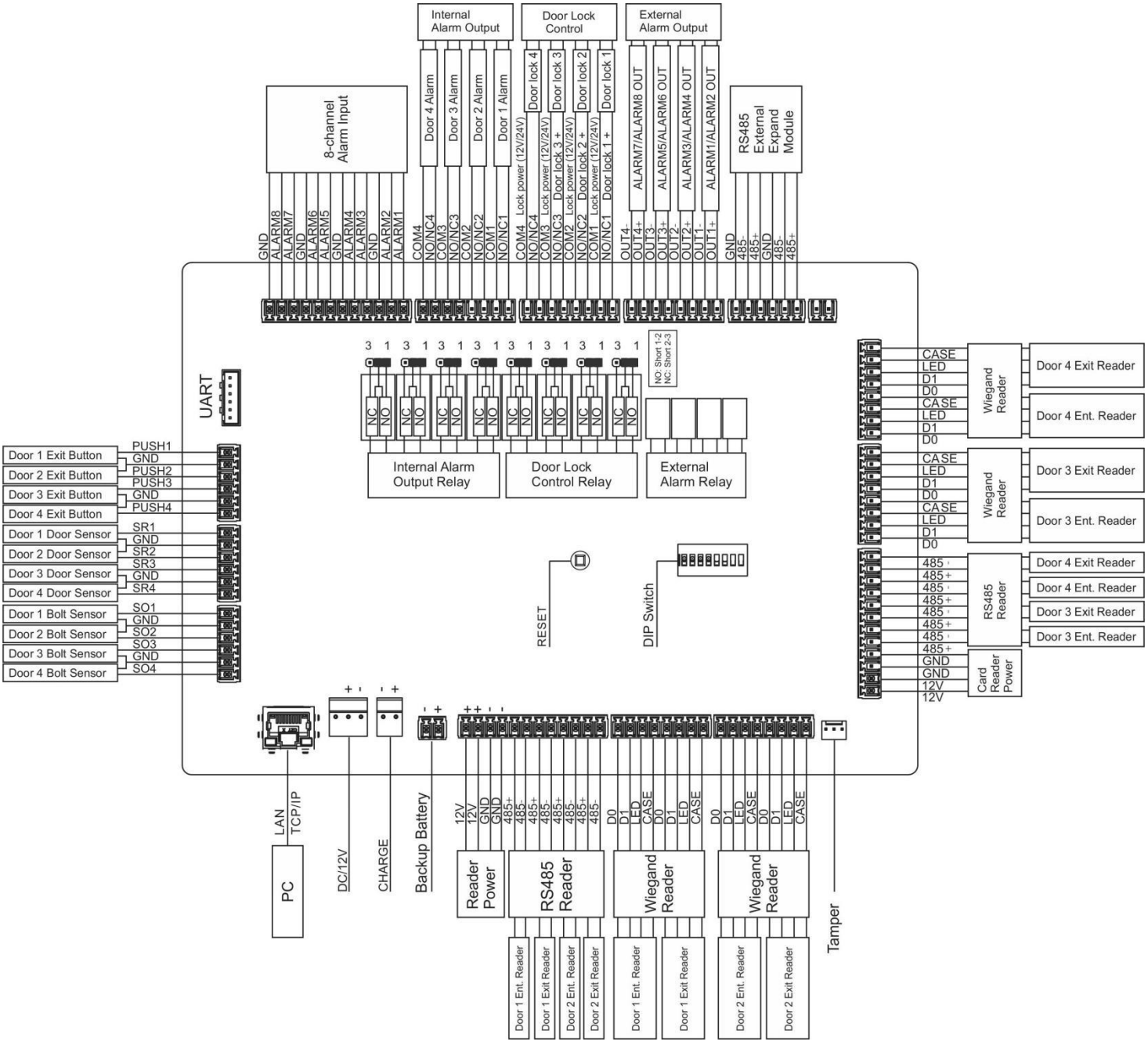
## Model: ACCON-2P22



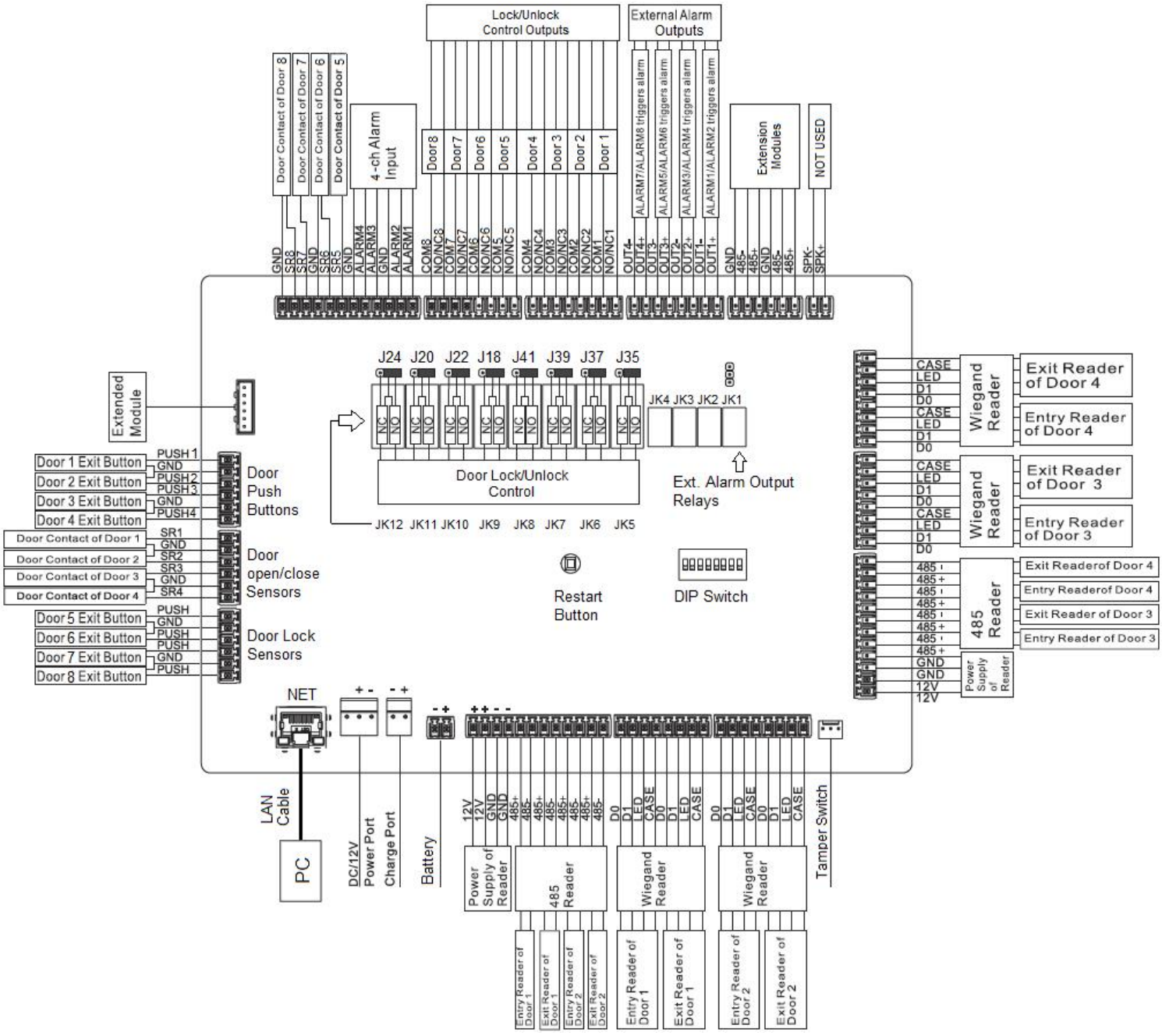
## Model: ACCON-2P41



## Model: ACCON-2P42



## Model: ACCON-2P81



# 3.3 Installation Step by Step

## 3.3.1 Setting up door lock jumpers (2P42 and 2P81 ONLY)

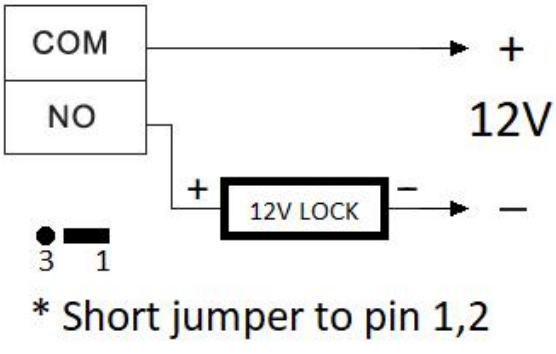
There are 8 relays and 8 jumpers for on the main board. The jumpers must be configured for proper NO (Normally Opened) / NC (Normally Closed) output. Default setting is pin 1-2 shorted, i.e. NO output - Power is supplied to the lock only when it is being unlocked. If you need NC output, please short pin 2-3.

| Relay and Jumper PCB designator | 2P42 | 2P81 |
|---|---|---|
| JK5 | Lock/Unlock control of door 1 | Lock/Unlock control of door 1 |
| J35 | | |
| JK6 | Lock/Unlock control of door 2 | Lock/Unlock control of door 2 |
| J37 | | |
| JK7 | Lock/Unlock control of door 3 | Lock/Unlock control of door 3 |
| J39 | | |
| JK8 | Lock/Unlock control of door 4 | Lock/Unlock control of door 4 |
| J41 | | |
| JK9 | Internal Alarm Output 1 | Lock/Unlock control of door 5 |
| J18 | | |
| JK10 | Internal Alarm Output 2 | Lock/Unlock control of door 6 |
| J22 | | |
| JK11 | Internal Alarm Output 3 | Lock/Unlock control of door 7 |
| J20 | | |
| JK12 | Internal Alarm Output 4 | Lock/Unlock control of door 8 |
| J24 | | |

## 3.3.2 Connecting door locks

a) Fail Secure type door lock connection - Supply power to unlock.

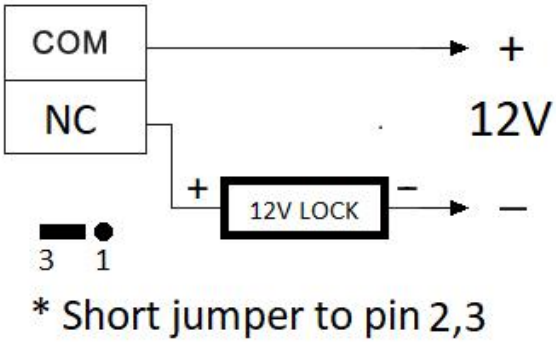
Typical Fail Secure type door lock: Electric strikes, drop bolts (fail secured type).




b) Fail Safe type door lock connection - Remove power to unlock.

Typical Fail Secure type door lock: Electromagnetic locks, drop bolts (fail safe type).

****** It is strongly recommended to use separate power supply for door locks if more than 4 locks are installed.***

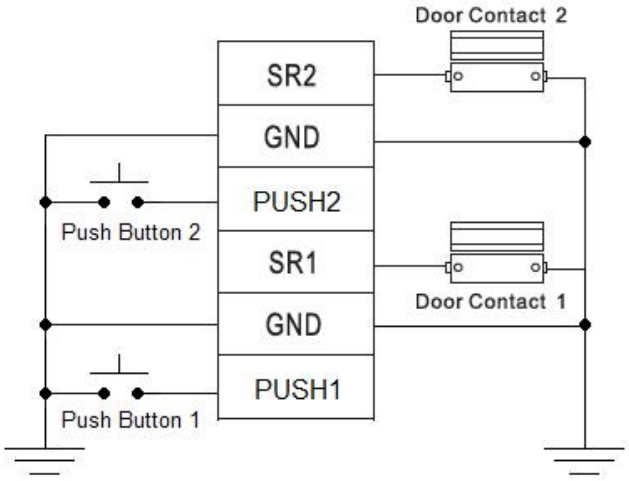


## 3.3.3 Connecting exit buttons and door open/close sensors

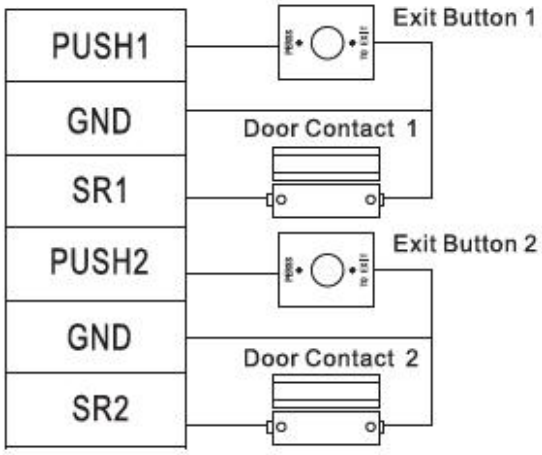
All Exit button inputs are **ACTIVE LOW**, i.e. connect to GND(0V) to unlock the door.

All Door open/close sensors inputs are **ACTIVE LOW**, i.e. when a door is closed, the voltage on the corresponding SR input (SR1, SR2… ) should become GND(0V). If the door is opened, the corresponding SR input should be open circuit (No connection).

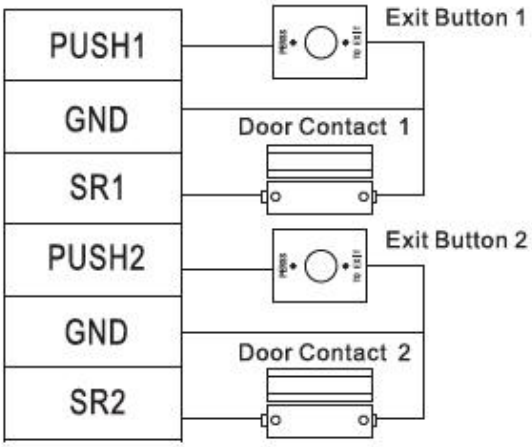
### Model: 2C41

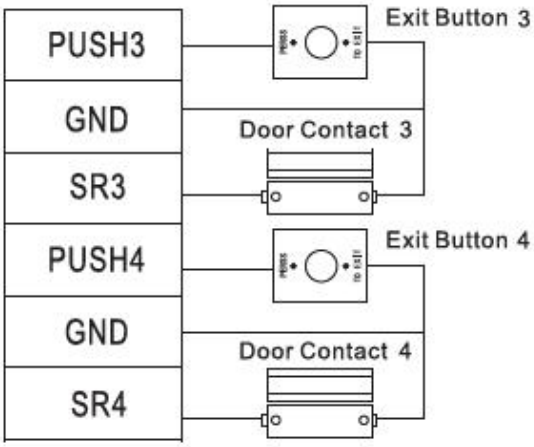



### Model: 2P22

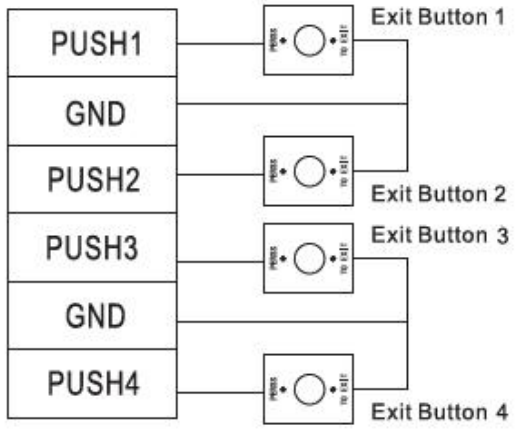


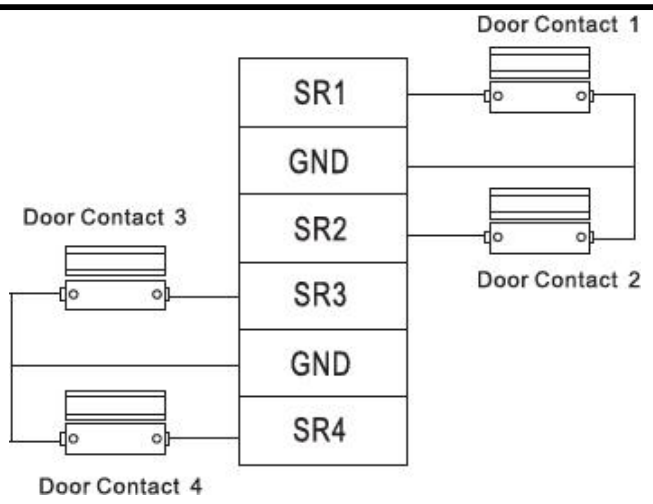

### Model: 2P41



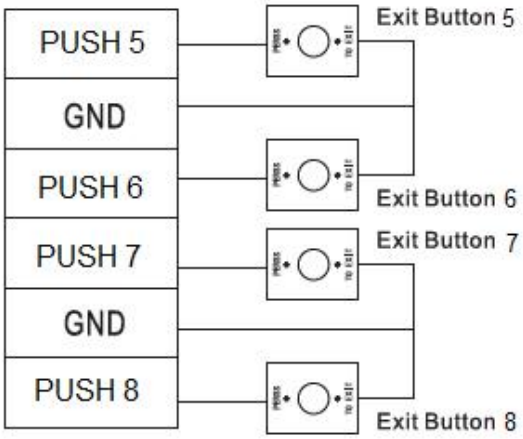



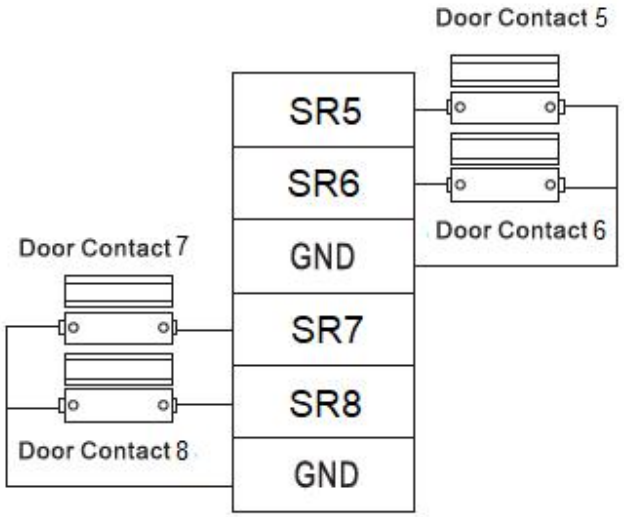
## Model: 2P42 / 2P81




## Model: 2P81 ONLY



## 3.3.4 Connecting card readers, fingerprint readers and keypads

You can select to connect either 485 bus or Wiegand bus. VIP access control panels and readers support both format. ***Note: Must use 485 bus for Fingerprint readers.***

a) If 485 readers are used, connect as the following table:

| Control Panel Wiring Terminals | Cable Colour (Reader side) | Description |
|---|---|---|
| 485+ | Purple | 485 readers connection |
| 485- | Yellow | |

b) If Wiegand readers are used, connect as the following table:

| Control Panel Wiring Terminals | Cable Colour (Reader side) | Description |
|---|---|---|
| LED | Brown | Wiegand readers connection |
| D0 | Green | |
| D1 | White | |
| CASE | Blue | |

| Reader Type | Cable Type | Max. Length |
|---|---|---|
| 485 Reader | CAT5e network cable | 100m |
| Wiegand Reader | CAT5e network cable | 100m |

## 3.3.5 Connecting external alarm inputs (if necessary)

External alarm inputs can be used to connect external devices such as latching switch, smoke alarm sensors or other security sensors.

The ALRAM inputs are **ACTIVE LOW**, that means when this pin is connected to GND (0V), it will trigger the external alarm output relay(s).

**Important:** When ALARM1 input is pulled LOW, all doors will be unlocked as long as the input pin voltage remain LOW.

Typical application: A latching switch is connected to ALARM1 input. If the switch is ON, all doors will be unlocked for emergency evacuation.

**Warning:** Do not connect ALARM1 if high security level is required.

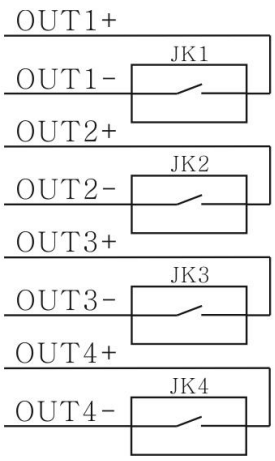
## 3.3.6 Connecting external alarm outputs (if necessary)

If any one of the external alarm inputs is triggered, the corresponding output relay will stay on for 15s.

The following table is for 2P42 and 2P81 ONLY.

For 2P42: Two External Alarm inputs share one set of External Output relay.

| External Alarm Input | Relay | External Alarm Output Terminal Block CON10 |
|---|---|---|
| ALARM1 | JK1 | OUT1+, OUT1- (Pin 1-2) |
| ALARM2 | | |
| ALARM3 | JK2 | OUT2+, OUT2- (Pin 3-4) |
| ALARM4 | | |
| ALARM5 | JK3 | OUT3+, OUT3- (Pin 5-6) |
| ALARM6 | | |
| ALARM7 | JK4 | OUT4+, OUT4- (Pin 7-8) |
| ALARM8 | | |




For 2P81: Four External Alarm inputs for four set of External Output relay.

| External Alarm Input | Relay | External Alarm Output Terminal Block CON10 |
|---|---|---|
| ALARM1 | JK1 | OUT1+, OUT1- (Pin 1-2) |
| ALARM2 | JK2 | OUT2+, OUT2- (Pin 3-4) |
| ALARM3 | JK3 | OUT3+, OUT3- (Pin 5-6) |
| ALARM4 | JK4 | OUT4+, OUT4- (Pin 7-8) |

## 3.3.7 Connecting power cable (2P series) / DC power adaptor (2C)

For 2P series, connect the power cable located at the bottom left hand corner of the metal case and power up.

For 2C series, plug the DC power adaptor into the power socket of the main unit.

Ignore any beep sound generated by the control panel and reader when power up. The beep sound may last for 15 seconds when power is applied for the first time.

## 3.3.8 Connecting network cable

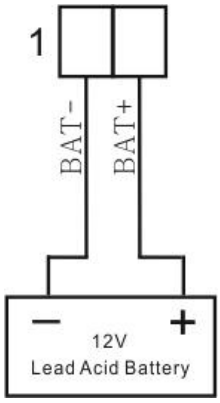
Connect a CAT5e LAN cable on NET connector of the access controller panel. Connect the other side of the cable to the network port of a PC.

## 3.3.9 Connecting a backup battery (2P series only)

A 12V sealed lead acid battery with a minimum capacity of 7AH must be used.

Connect CON1 pin 1 to **NEGATIVE** terminal of the battery.
Connect CON1 pin 2 to **POSITIVE** terminal of the battery.

****** Be careful with the polarity of the battery! Wrong connection will result in system damage.***



# 4 Smart PSS PC Console

Smart PSS is an all-in-one, full-featured application for configuring access control systems, surveillance camera, network video recorders, video walls and intercom systems.The software provides efficient device management and is user friendly.

## 4.1 Cybersecurity Recommendations

Mandatory actions to be taken towards cybersecurity

1) Change Passwords and Use Strong Passwords:

   The number one reason systems get “hacked” is due to having weak or default passwords. It is recommended to change default passwords immediately and choose a strong password whenever possible. A strong password should be made up of at least 8 characters and a combination of special characters, numbers, and upper and lower case letters.

2) Change Passwords Regularly

   Regularly change the credentials to your devices to help ensure that only authorized users are able to access the system.

3) Disable Auto-Login on Smart PSS:

   Those using Smart PSS to view their system and on a computer that is used by multiple people should disable auto-login. This adds a layer of security to prevent users without the appropriate credentials from accessing the system.

4) Use a Different Username and Password for Smart PSS:

   In the event that your social media, bank, email, etc. account is compromised, you would not want someone collecting those passwords and trying them out on your video surveillance system. Using a different username and password for your security system will make it more difficult for someone to guess their way into your system.

5) Lock the Access Controller:

   After installation, make sure the door of the access controller is lock to prevent any unauthorized physical access or modifications to your system. Keep the key in a safe place.

6) Isolate Access Controller Network

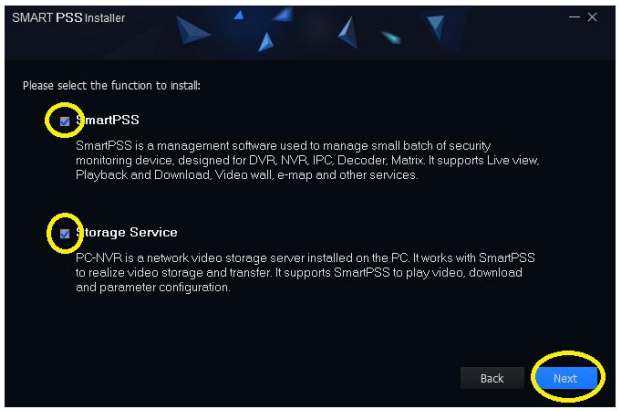
The network your access controller resides on should not be the same network as your public computer network. This will prevent any visitors or unwanted guests from getting access to the same network the security system needs in order to function properly.

# 4.2 Smart PSS Installation Step by Step

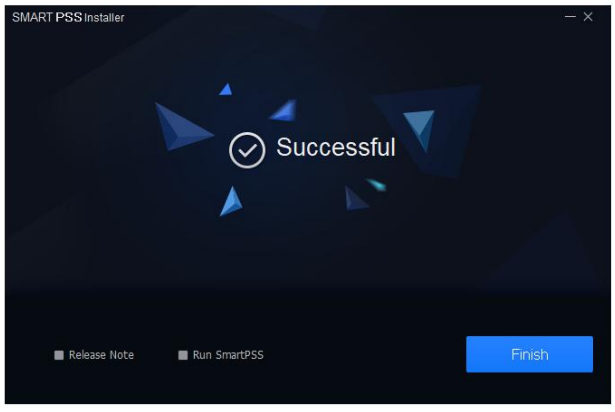
## 4.2.1 Install the Smart PSS software

Download the latest version of Smart PSDD software from Rhino Website (www.rhinoco.com.au). After that, double click the Smart PSS setup file to start installation.

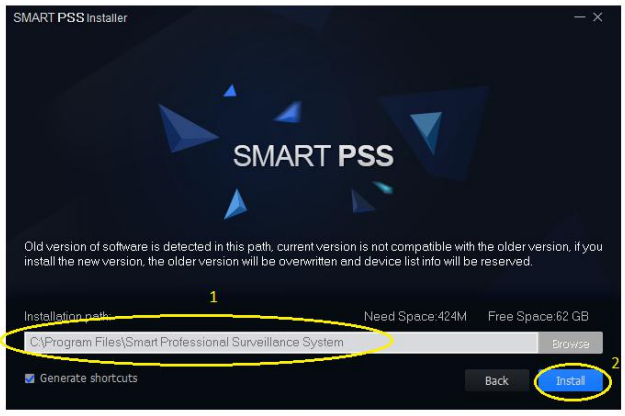

Must check the “accept agreement” box.




Check both boxes for complete software installation.




Wait until the “Successful” message is shown on the screen.




Change the installation folder if necessary and click “Next”.

## 4.2.2 Set password for the Smart PSS

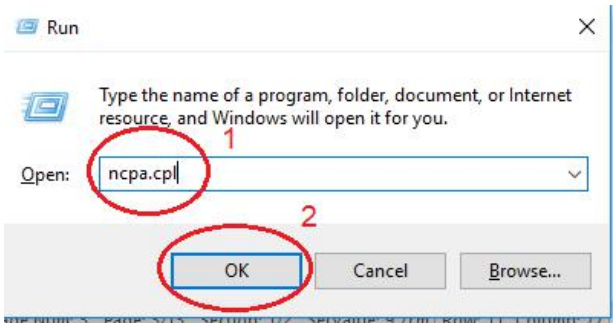
Double click  icon to run the Smart PSS. When the program prompts to set a password, enter the password and check “Auto Login after Registration” and click “Next”. The password must be 8-digits with numbers and alphabet characters.


Then, answer some Password Protection questions and click “Finish”.

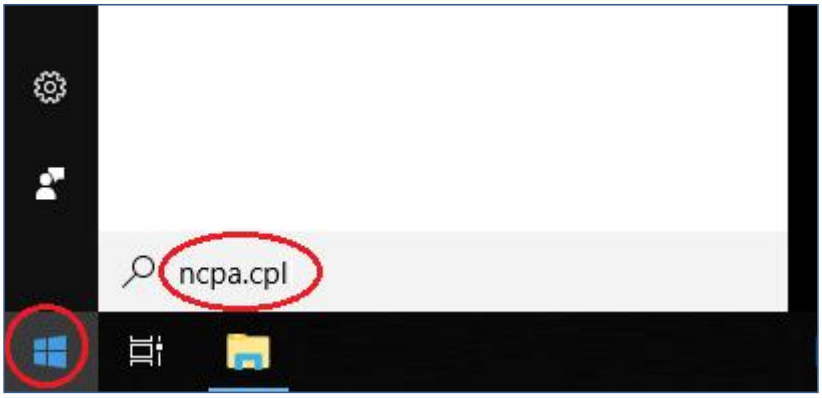
## 4.2.3 Configure the PC network card (Ethernet card)

The default IP address of the VIP Access Controller is 192.168.0.2, you must change the PC network card IP address to this subnet, i.e. you must set the IP of the PC network card to 192.168.0.xx where xx is a number from 0 to 255 other than (2 is used by the access controller). We recommend setting xx to a bigger number to reduce the possibility of having conflict with other devices. Let's set the IP of the network card to 192.168.0.199 for example.

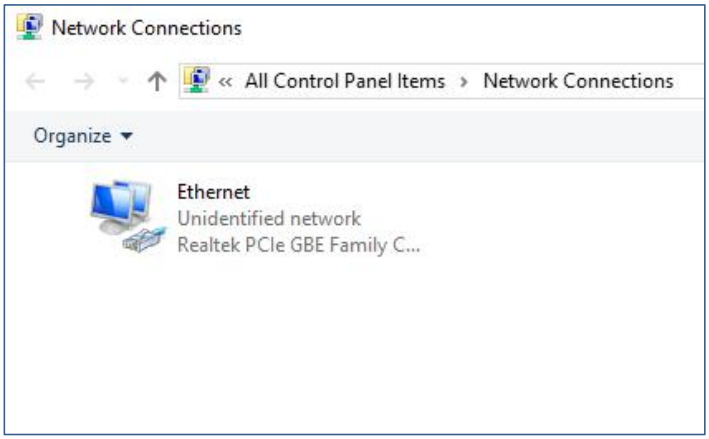
i) Press and hold the Windows logo key and then press R. A little command box will appear in the bottom left corner. Type "ncpa.cpl" and click "OK"




if your keyboard doesn't have the Windows logo key then drag the mouse to bottom left corner of the screen and click the Windows logo and type "ncpa.cpl" and press "ENTER".

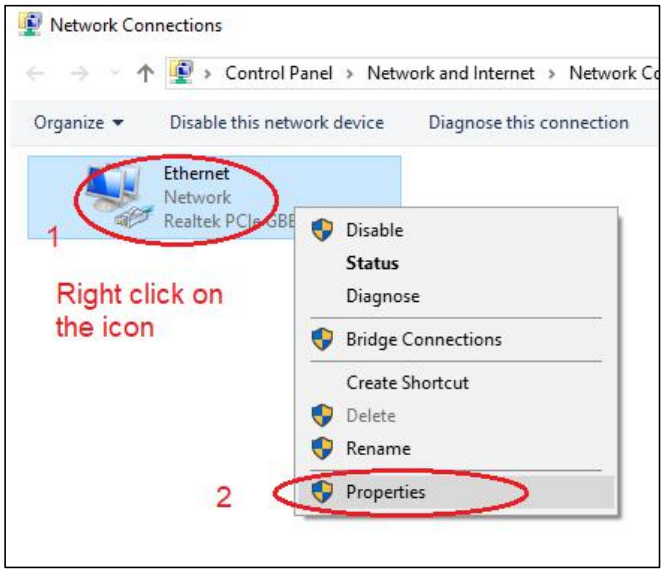



You should see the following screen if the above steps are done correctly.

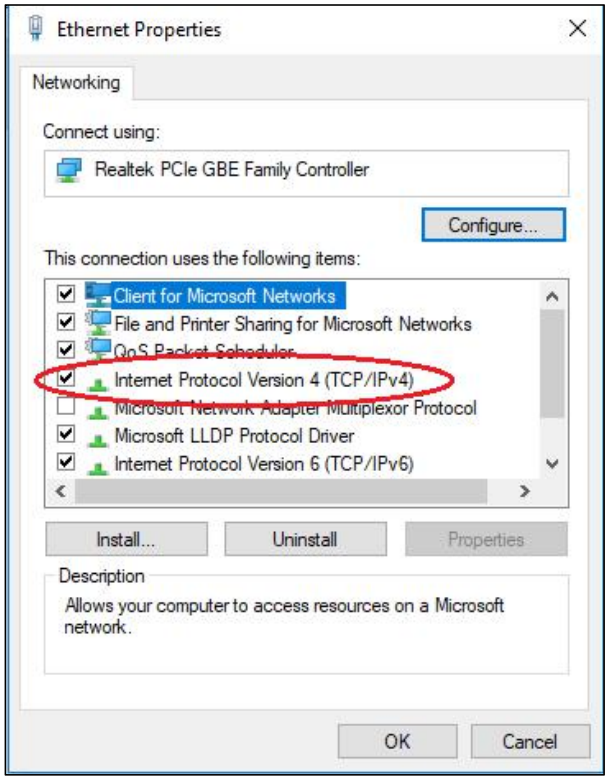


ii) Right click on the Ethernet icon and right click the mouse button.

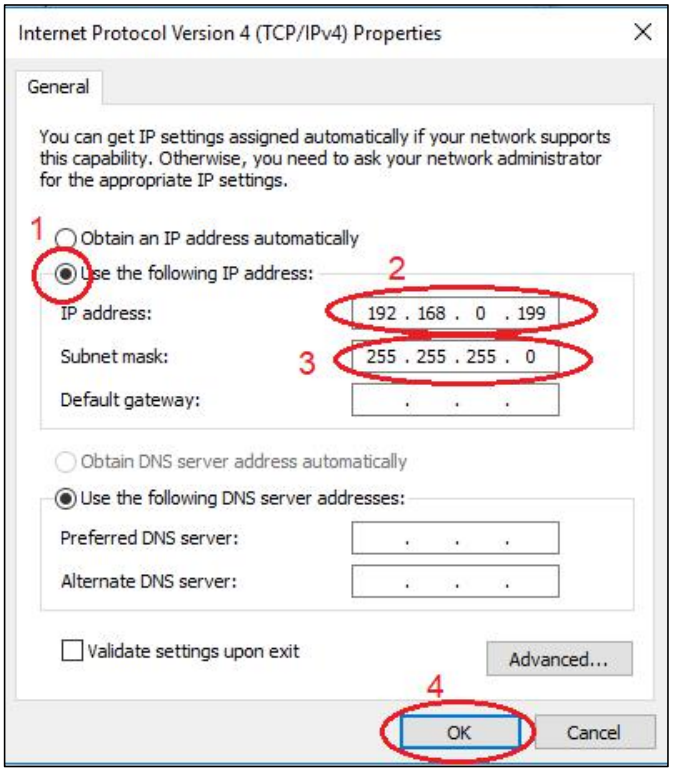
Note: Since the name “Ethernet” is changeable, it may be different in your PC. Just select the network card which is connected to the access controller.

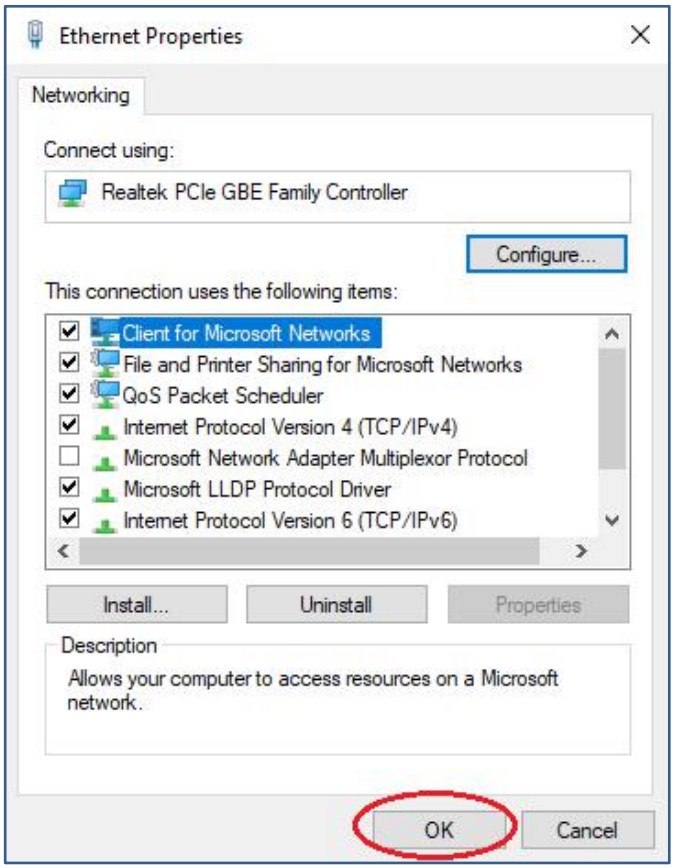



iii) Double click the item “Internet Protocol Version 4 (TCP/IPv4)




iv) Enter information as shown below:

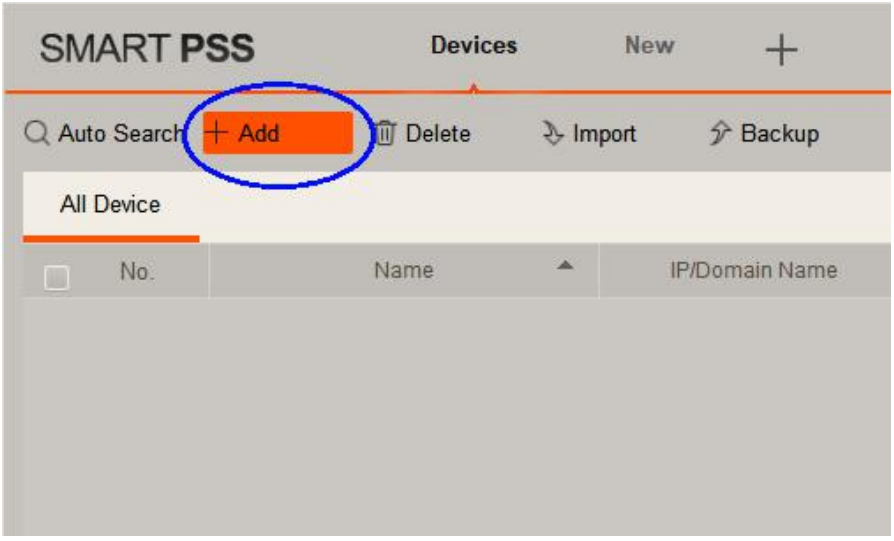




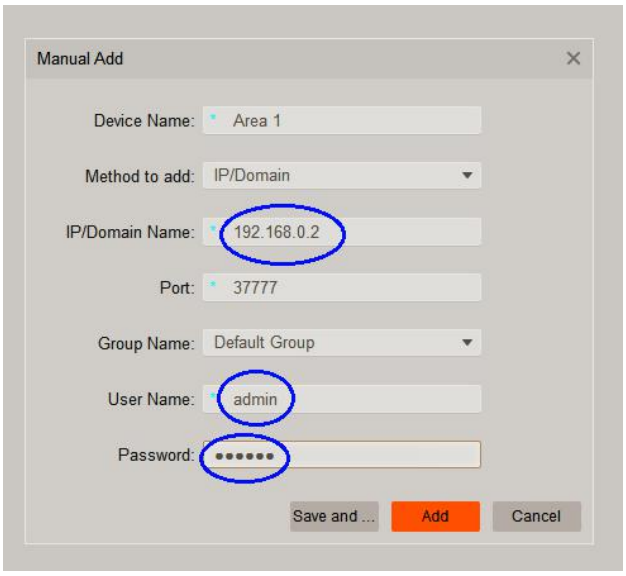

## 4.2.4 Add the access controller to Smart PSS

Now run the Smart PSS by clicking the Smart PSS icon .

i. To add VIP access controller, click the “+Add” button.



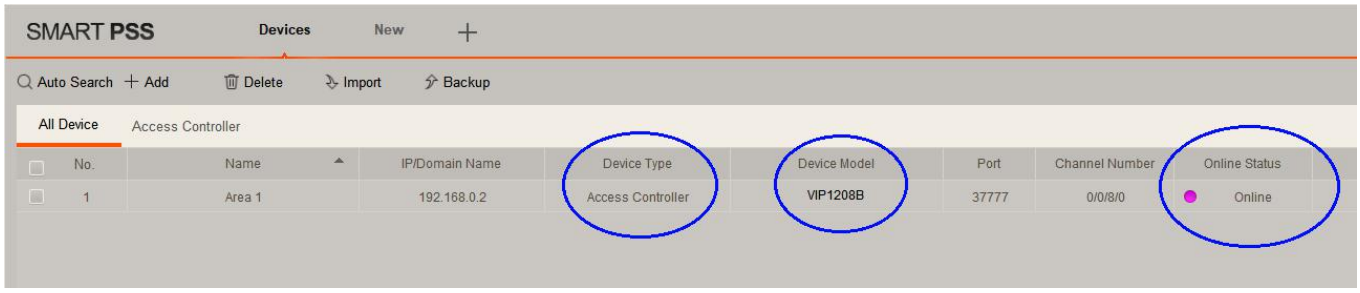
ii. Enter all parameters and then click “Add” button to add the device.




Default User Name is admin Default Password is: 123456

***Important: If the user name or password is incorrect, the access control will not be online.***

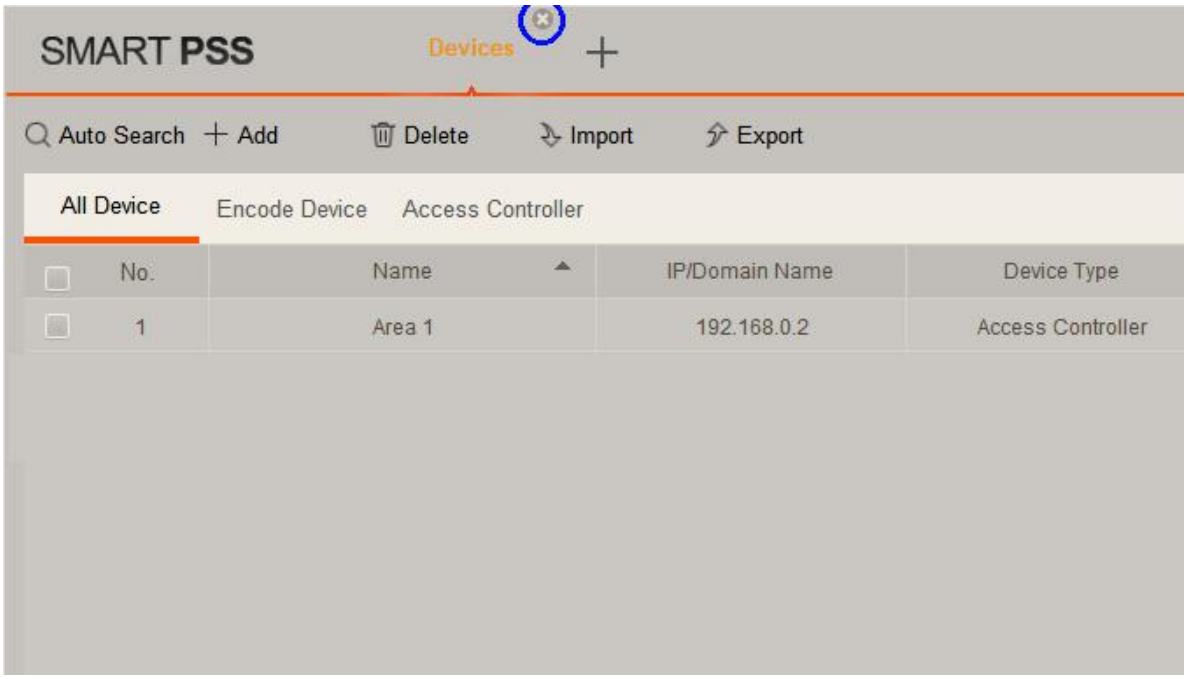
iii) If the device is successfully added, you can see the device type and a green circle indicating the online status.



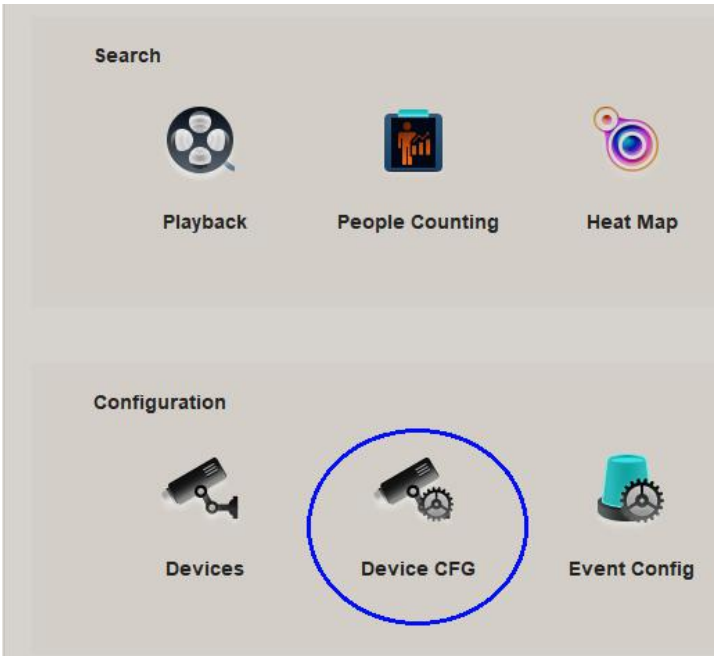
## 4.2.5 Synchronize time with PC

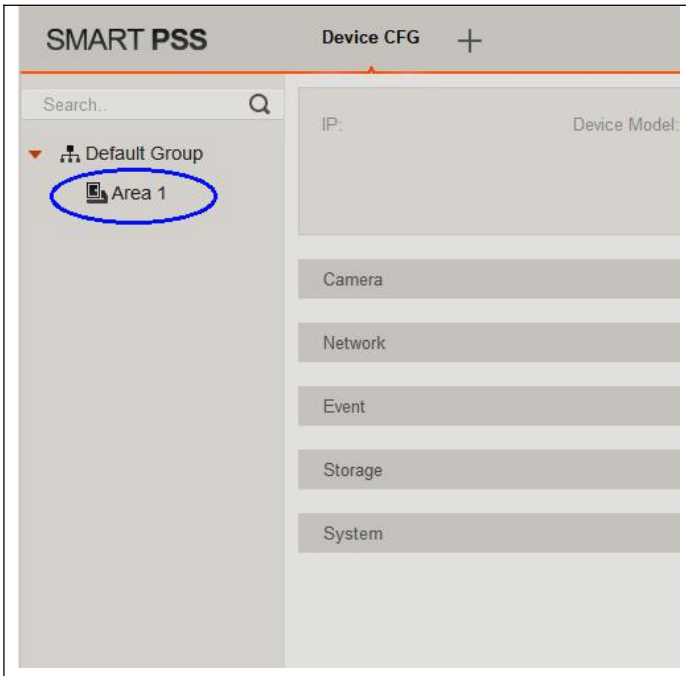
It is very important that you must synchronize the time/date of the access controller with PC otherwise the access time may not be exactly the same as the real time.

i. Drag the mouse to the “Devices” menu item on the top left of the “Add Devices” screen and click the “X” symbol to exit to the main screen.

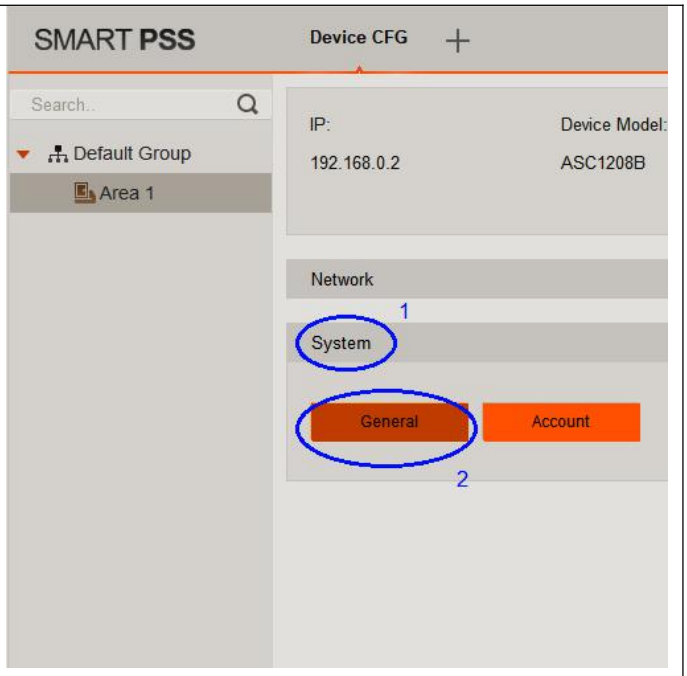



ii. Click the Device CFG icon to enter the device configuration menu.



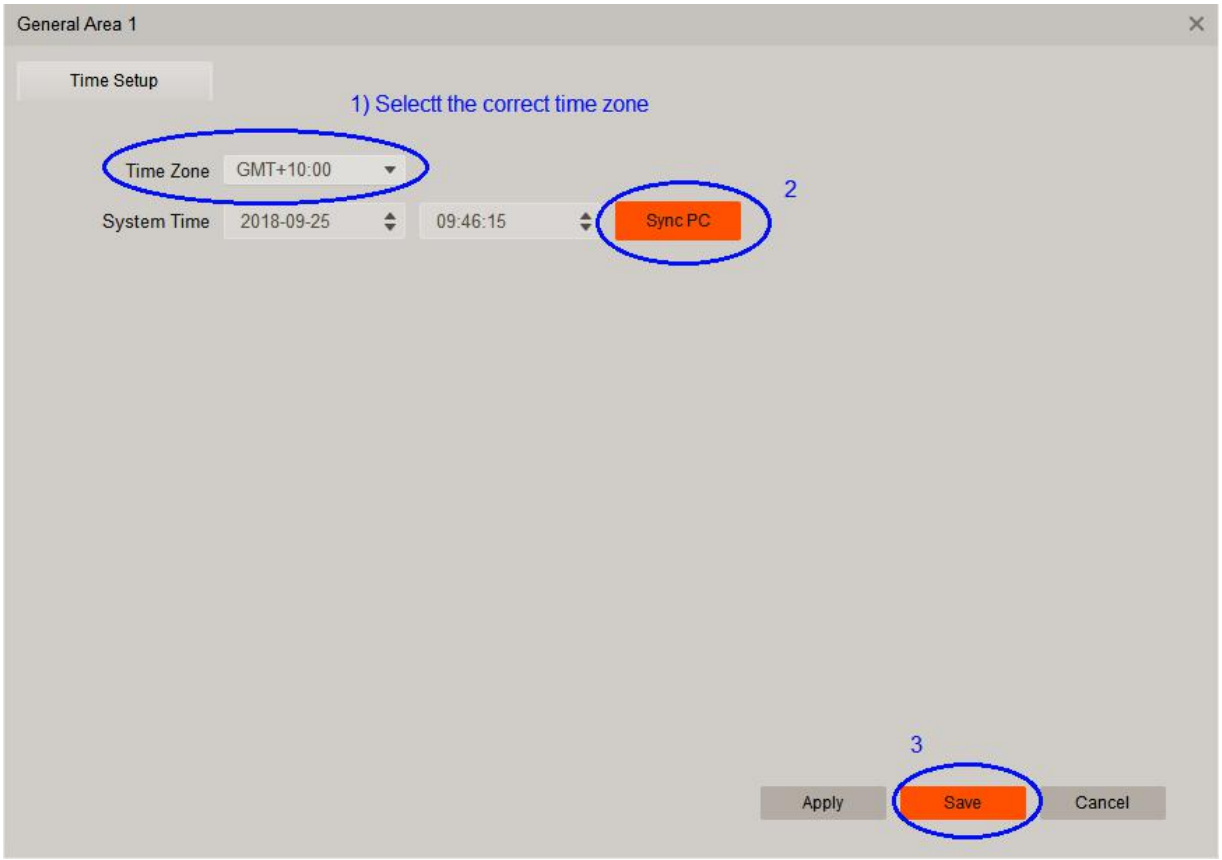



iii. Click the access controller name defined earlier.



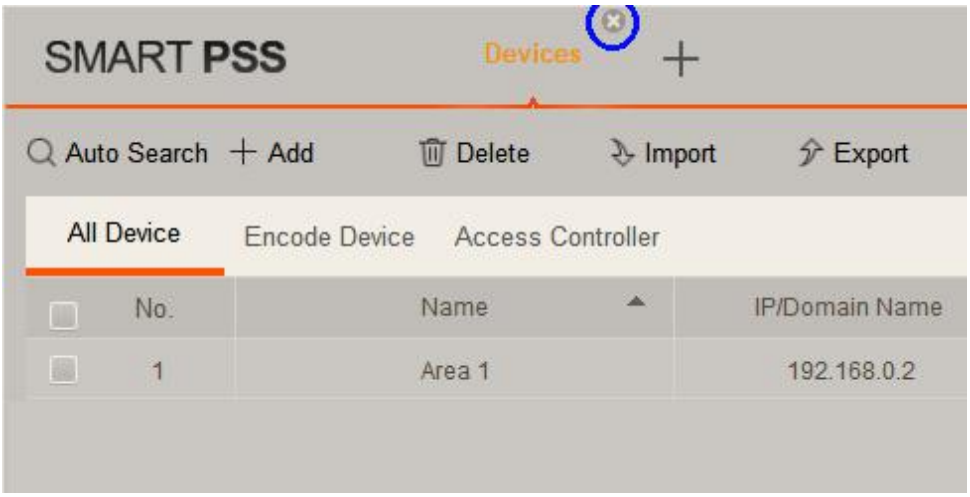

iv. Click “System” and then “General” button.

v. Select the correct time zone and click “Sync PC” to synchronize the time with PC. After that click “Save” to finish synchronizing the time with PC.

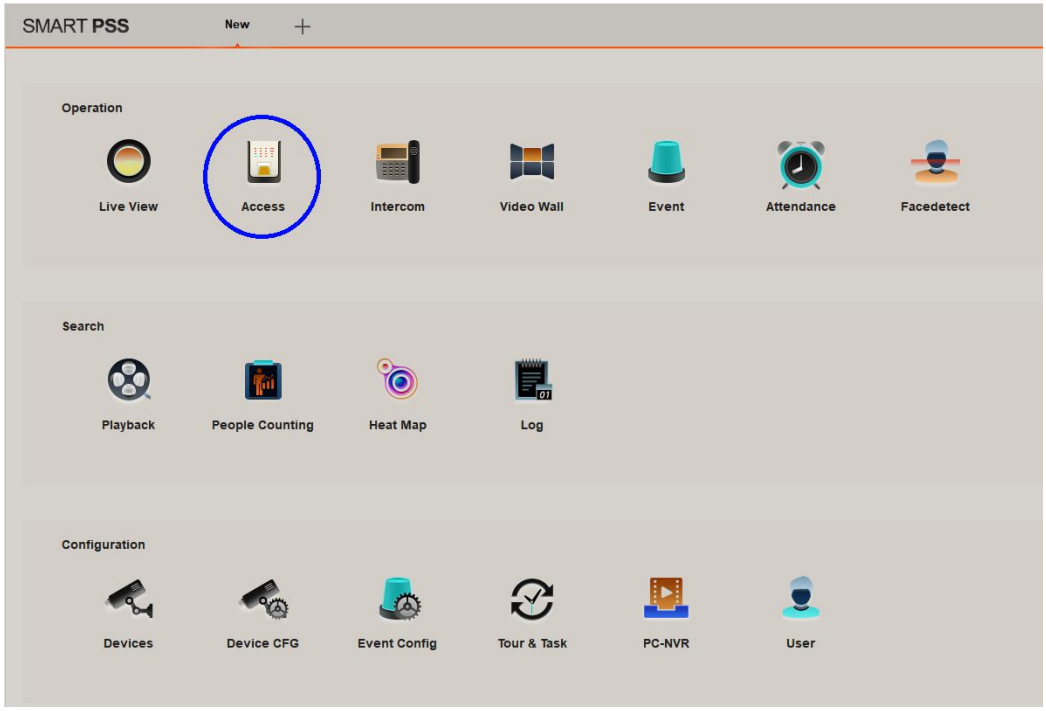


## 4.2.6 Add users

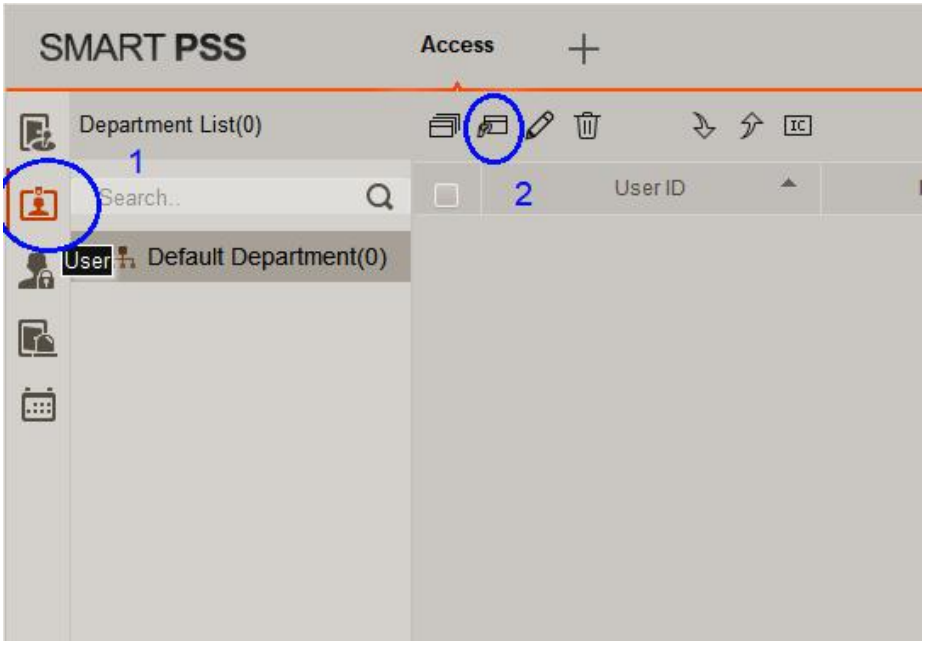
i. Drag the mouse to the “Devices” menu item on the top left of the “Add Devices” screen and click the “X” symbol to exit to the main screen.



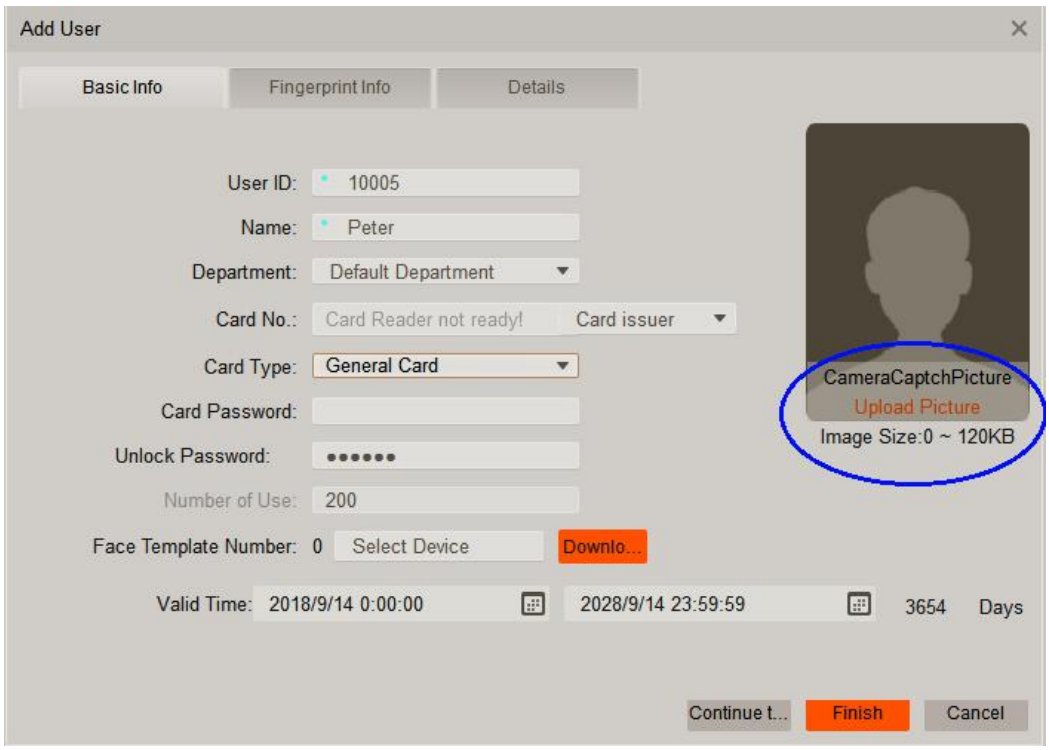

ii. Double click the “Access” icon to enter the access controller console.



iii. After entering the console screen, click the user icon on the top left hand corner of the screen to enter User Menu. Then click the manual add icon to start adding user information.




iv. Enter all user information in the box.




**User ID:**
Maximum 10 digits with no leading zero

**Name:** Name of the user

**Card No.:** Put a IC card on the USB reader, click on the Card No. box, the card number will be read out automatically. Remove the card when you see the card number

**Card Type**: Select the user level

**Card Password:** ***Ignore***

**Unlock Password:** enter a 6-digit keypad password for this user. **All users must have different password.**

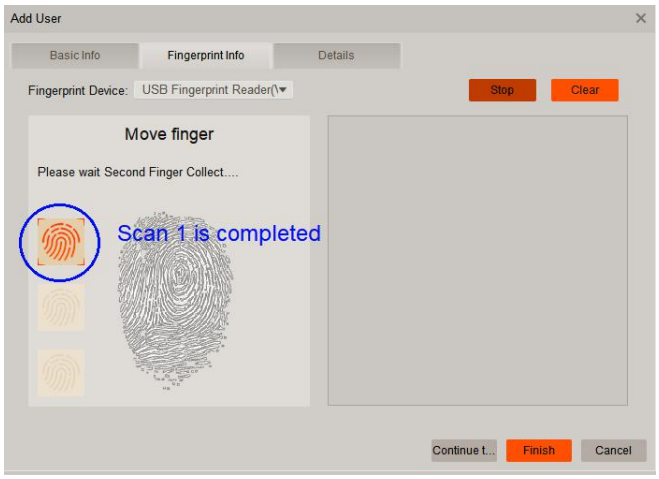
**Number of Use:** Enter the access times limited to **Guest Card** only

**Face Template Number:** Not applicable **Valid Time:** Validity of the card for this user

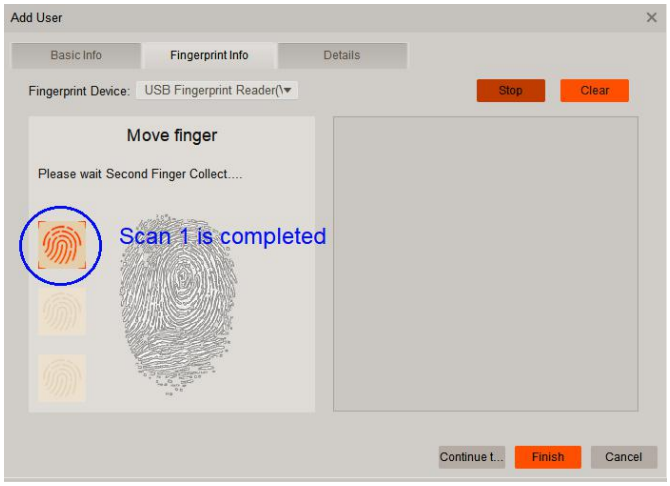
You may add the photo of the user by clicking “Upload Picture” or take a picture from an VIP brand USB camera. Other brands may not be compatible with the system.

Note: User photos are essential if you need to use the Remote Verification function.

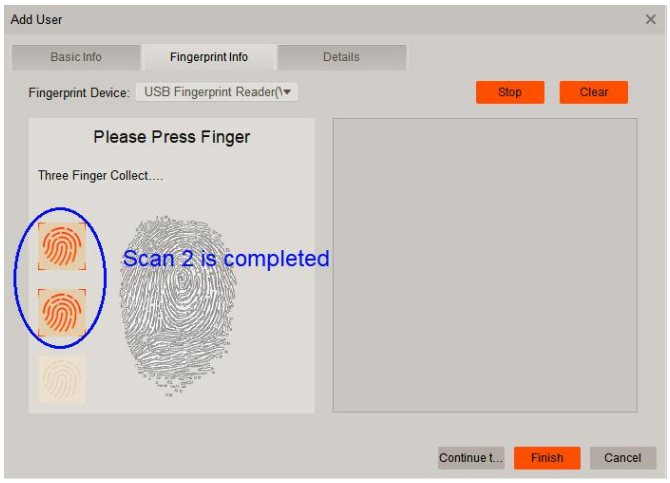
## 4.2.7 Add fingerprints




i. Plug the USB Fingerprint Enrollment Reader to the PC USB port.
ii. Click the Fingerprint info tab
iii. Make sure “USB Fingerprint Reader” is selected in the Fingerprint Device section.

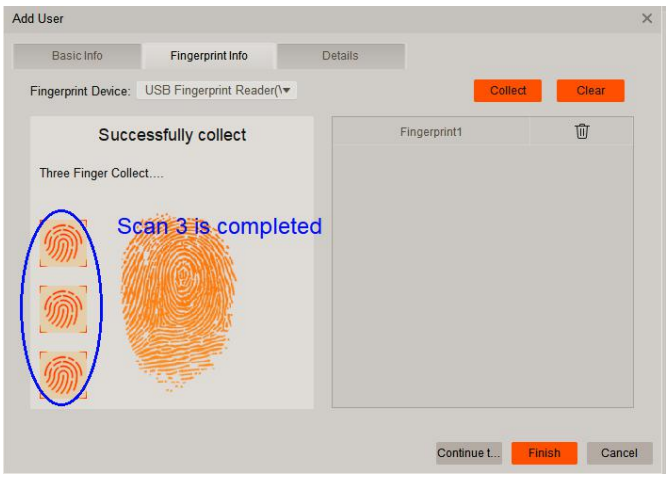



iv. Make sure the finger to be read is clean and not too dry or too wet. Put a finger on the fingerprint reader and click “Collect” button.
v. The reader will collect 3 times. When the you see the blue fingerprint icon on the left appears, it means that scan 1 is completed.




vi. Raise the finger for 1 second and press the **SAME FINGER** on the reader again.

vii. Scan 2 will start when the reader detects a finger is pressed.

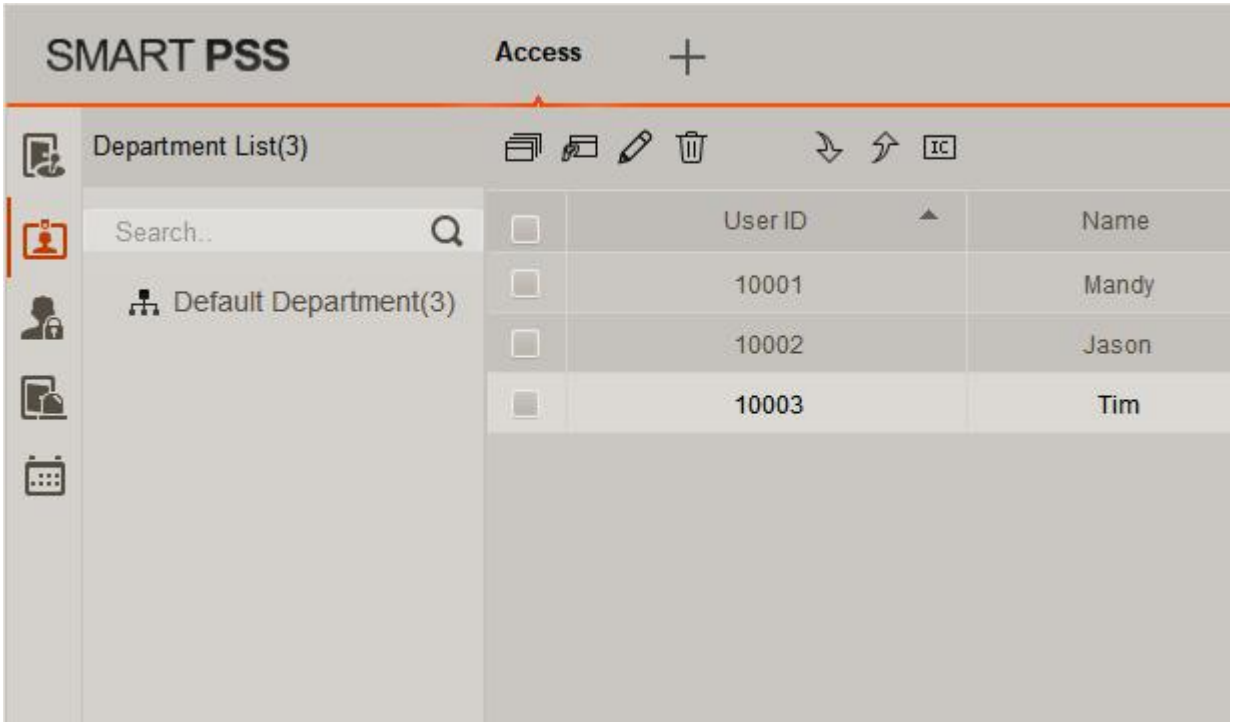



viii. Raise the finger for 1 second and press the **SAME FINGER** on the reader again.

ix. Scan 3 will start when the reader detects a finger is pressed.

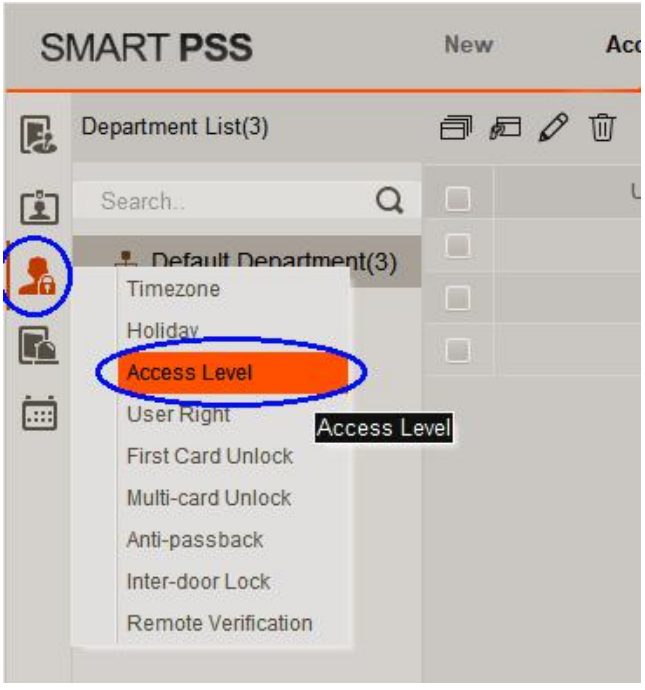
Click “Continue” to add next user or “Finish” to finish adding users.

x. Now you can see all the users added on the User Screen.

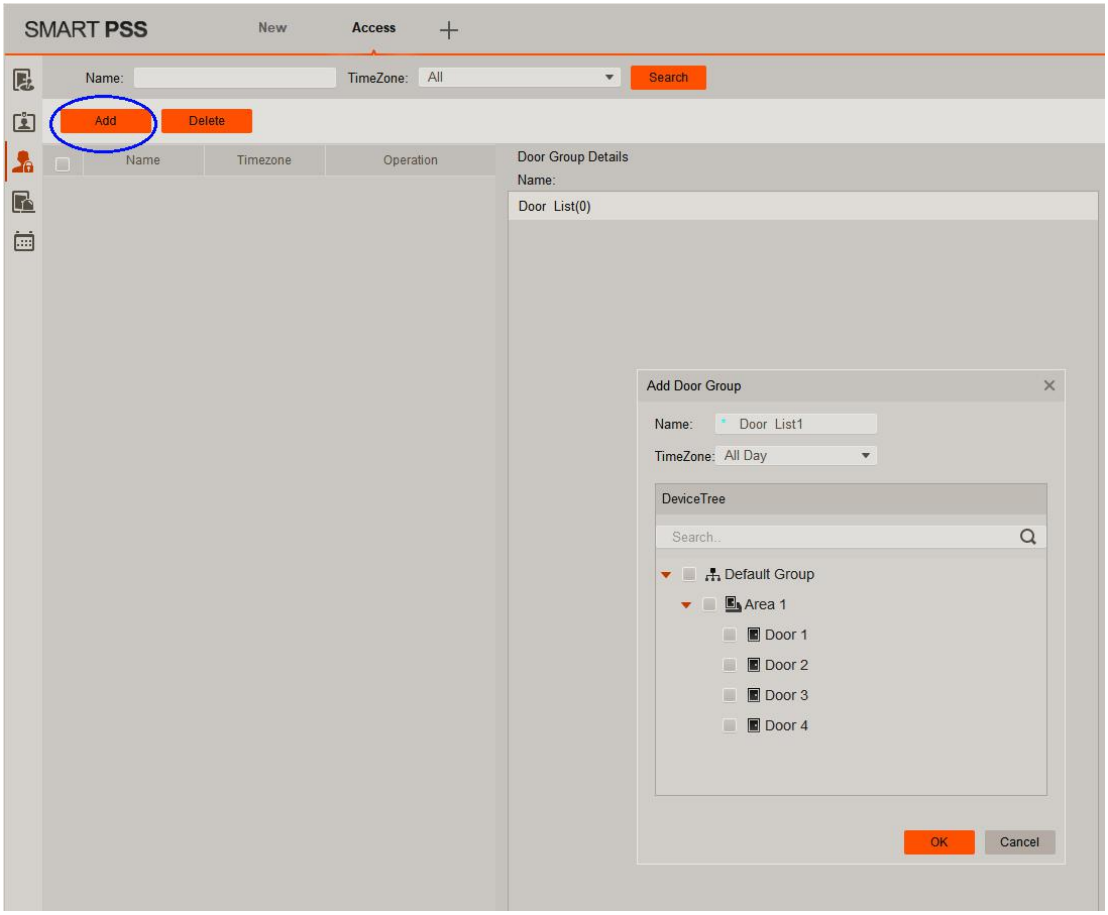



## 4.2.8 Add door groups

i. Click  icon on the main menu and then click “Access Level” to enter the access level screen

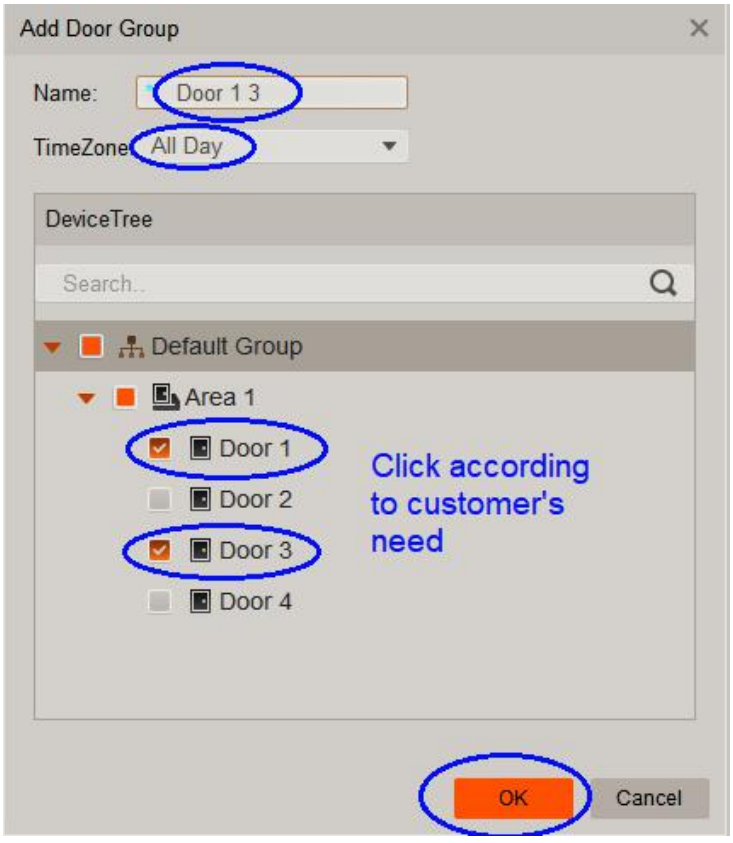


ii. Click the Add button and the following screen will be displayed:




iii. Now Enter the name for the Door group and timezone and the doors where the users belong to this group can gain access.

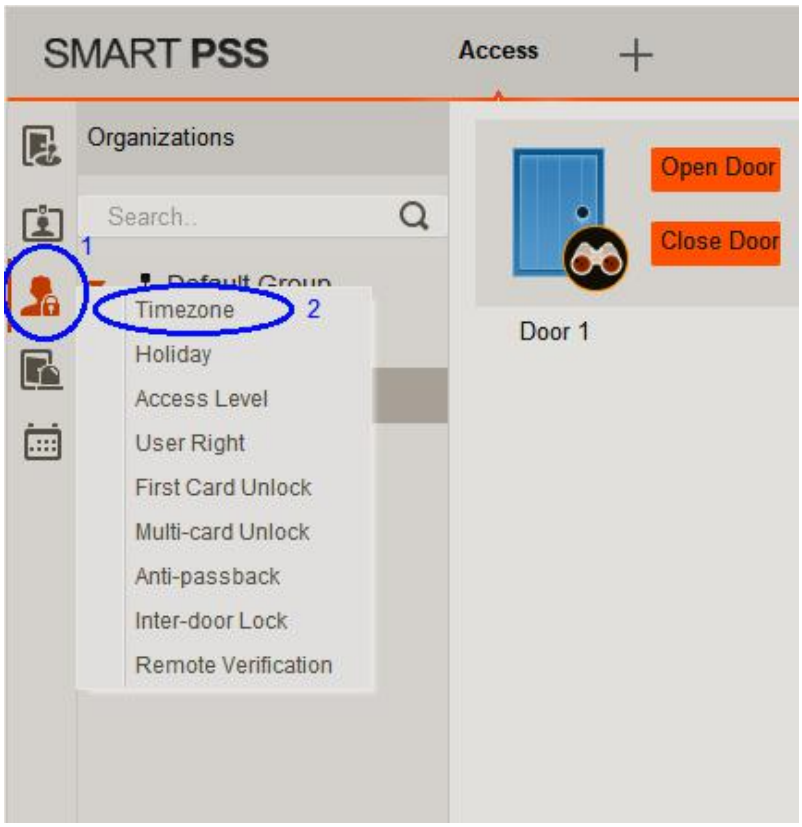
In this example, Door group “Door 1 3” can be accessed by users belong to this group all day. They can only access door 1 or door 3 only.



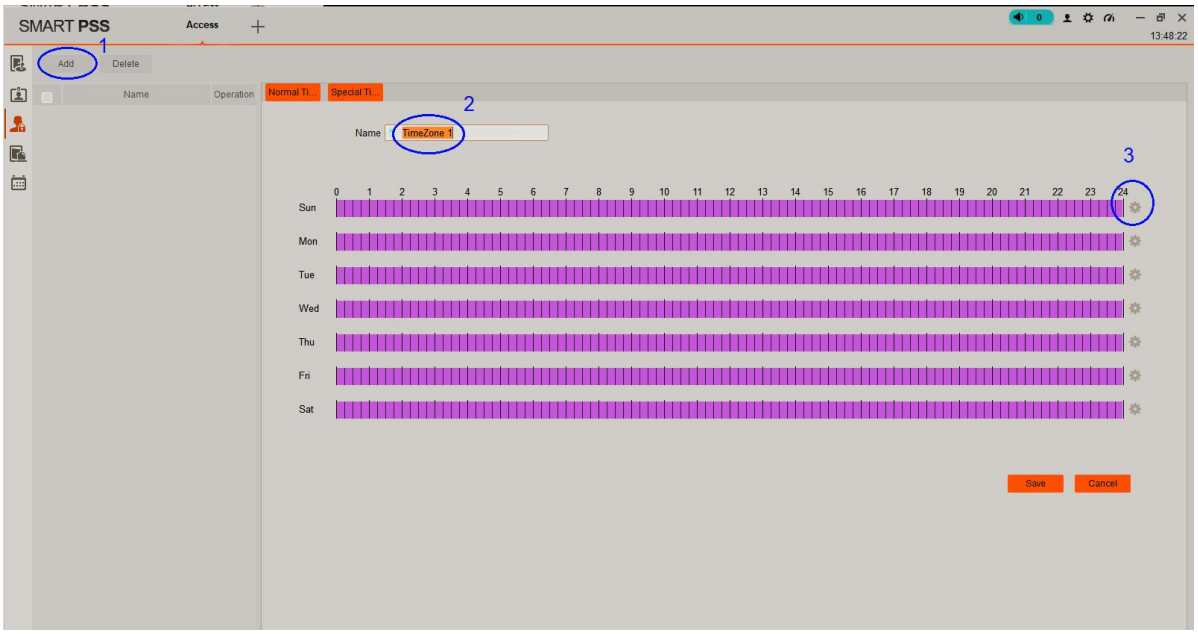

iv. Repeat step ii until all door groups are created.

## 4.2.9 Set time schedules

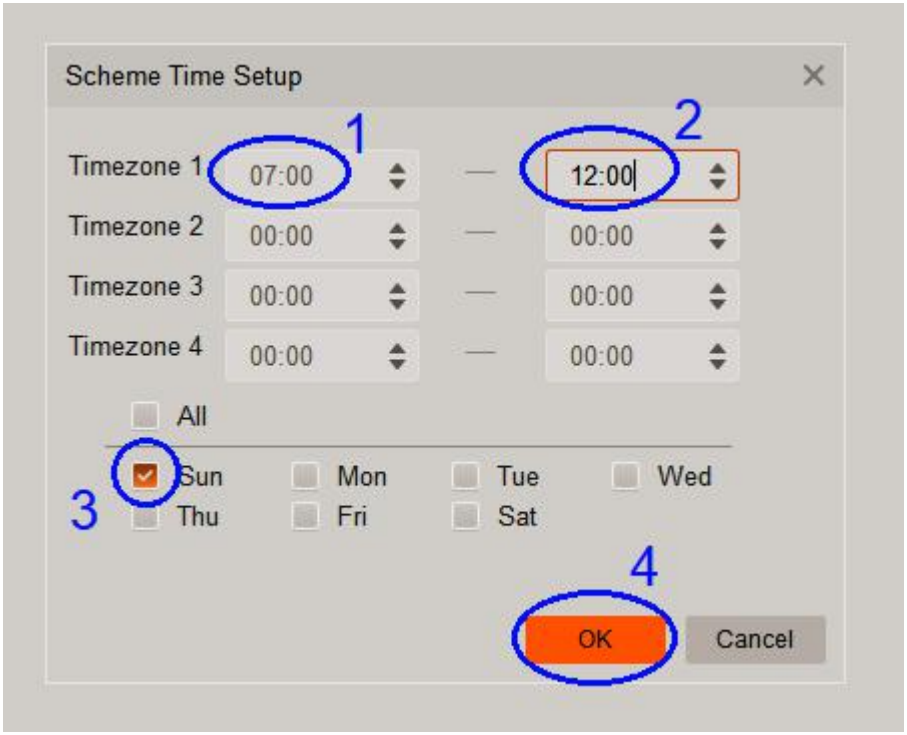
a) Click  and then Timezone to select Time Zone Setup.



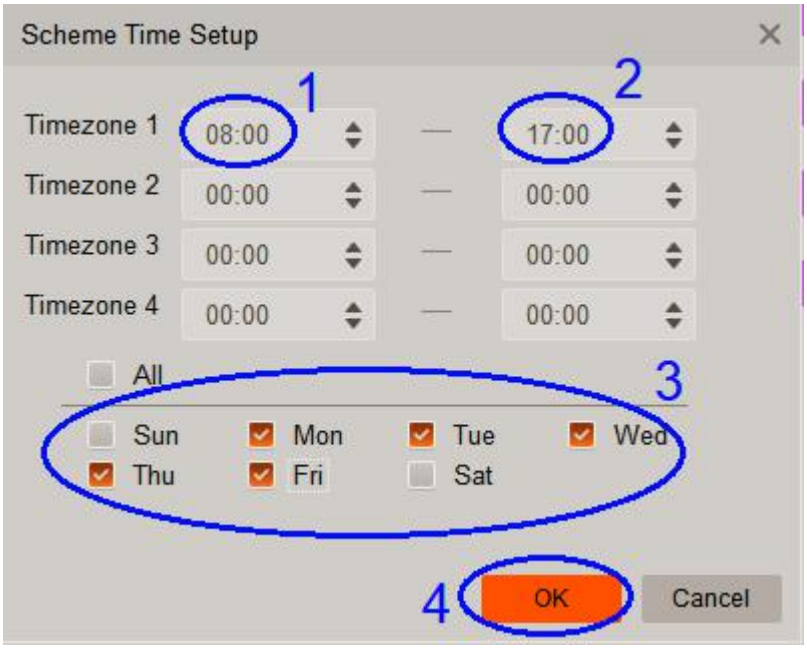

b) Click “Add” and then enter the name of the time schedule. Press  to set the time schedule.



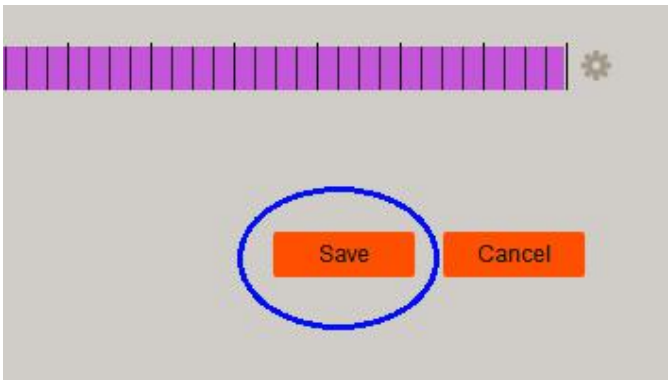
c) Set the time and the day of week when the doors are allowed to access.




d) Multi-select is allowed.



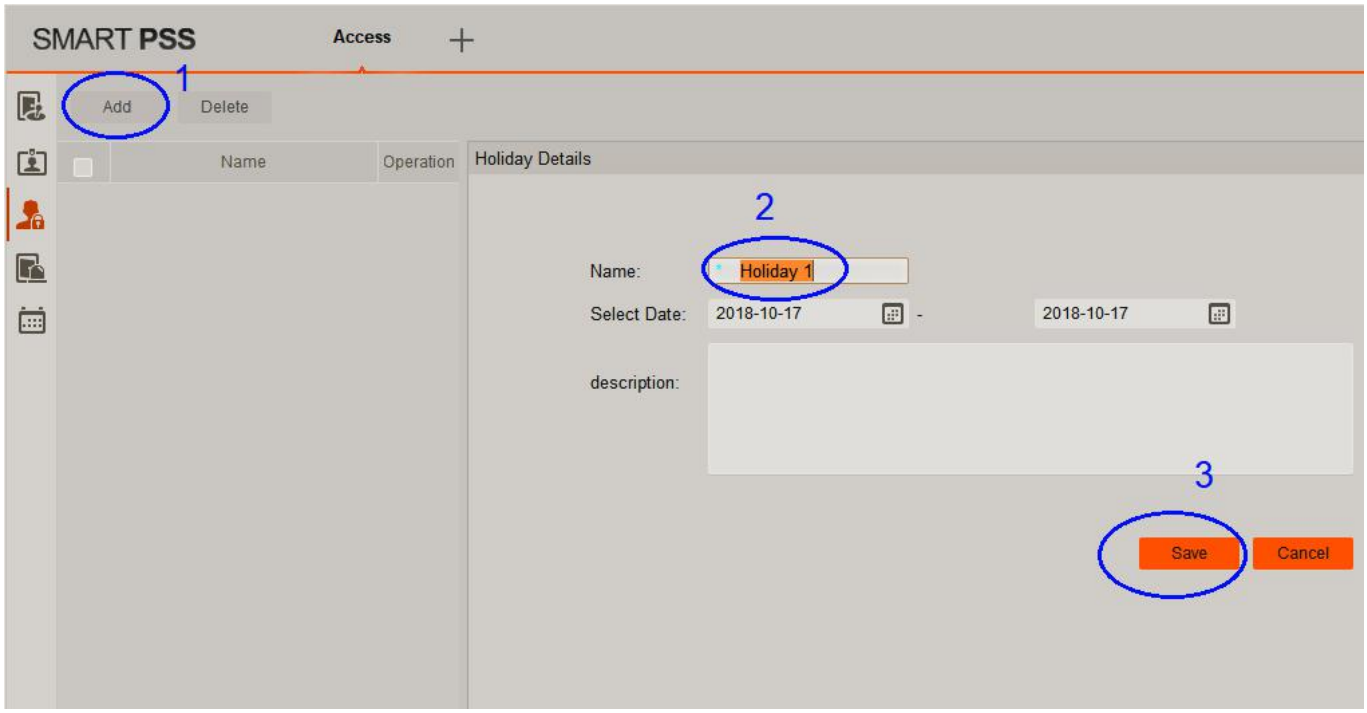

e) Click Save when done.



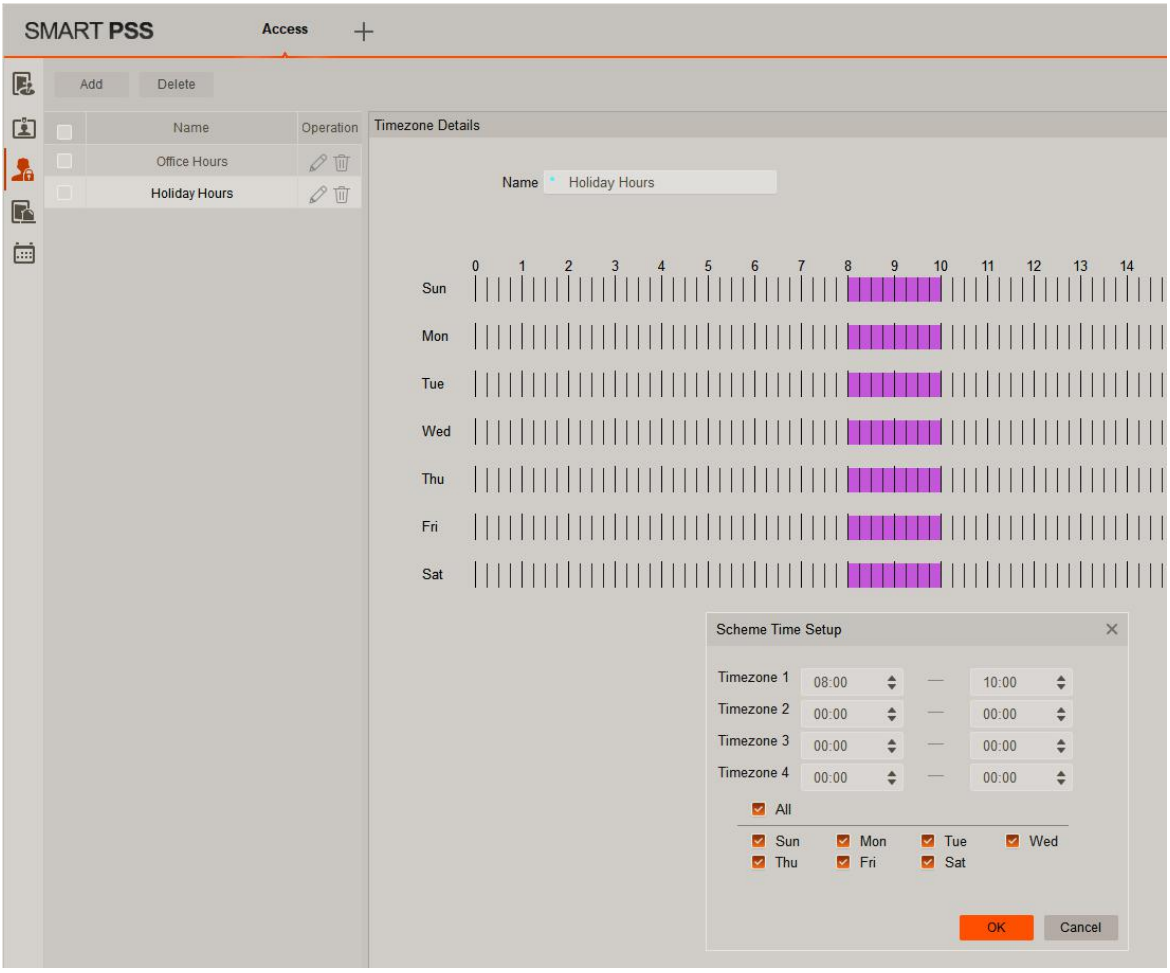
## 4.2.10 Set holiday schedules

a) Click  and then Holiday to select Holdiay schedule setup.

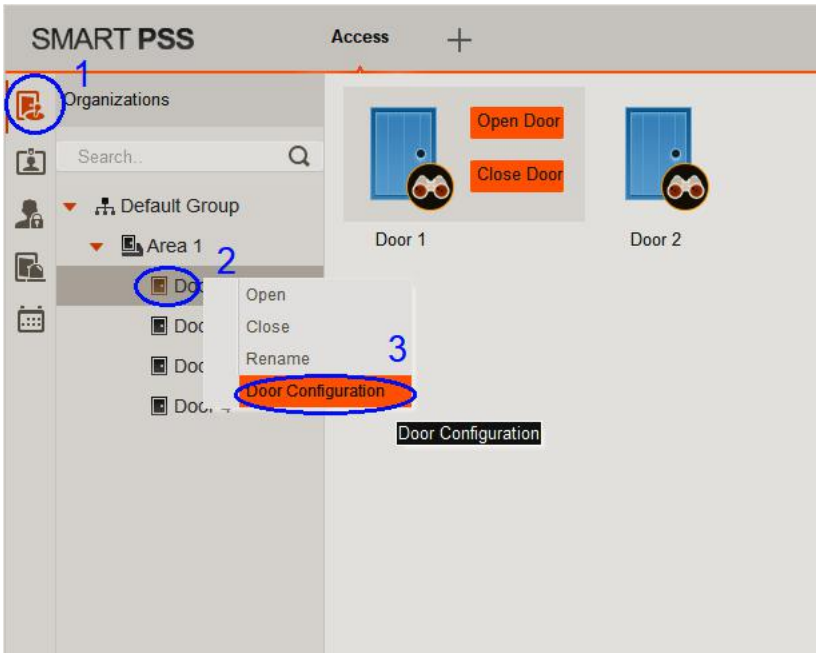

b) Click “Add” and then enter the name of the holiday schedule. Seelect the dat and click “Save” when finished.



c) Set holiday time schedule to restrict the time when the users can get access. In the following example, authorized users can get access at 08:00-10:00 during holiday.

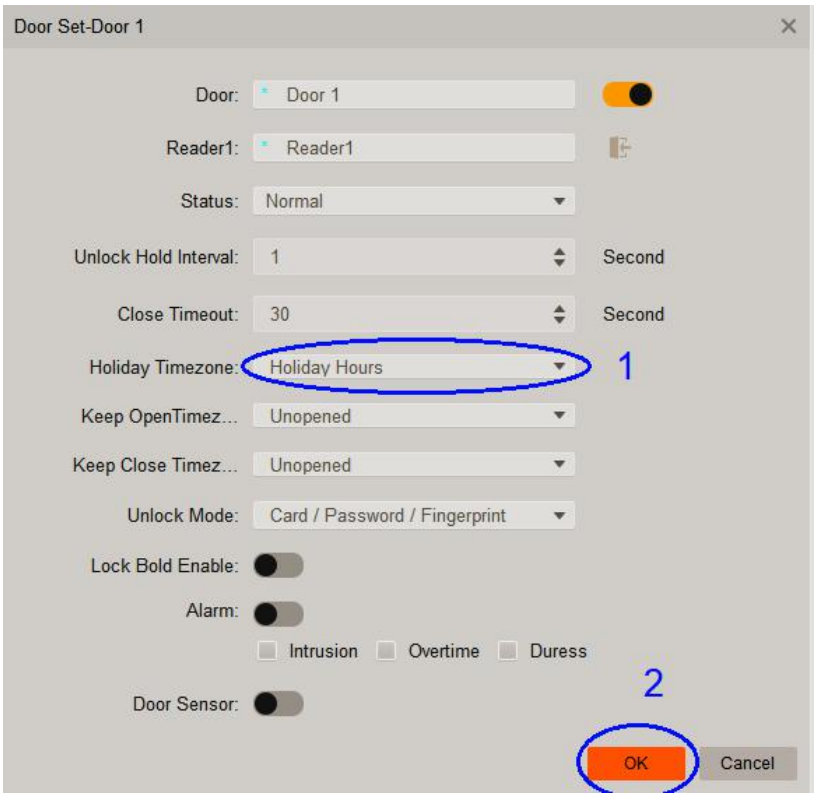



d) Restrict which door(s) the user can get access by “Door Configuration”.



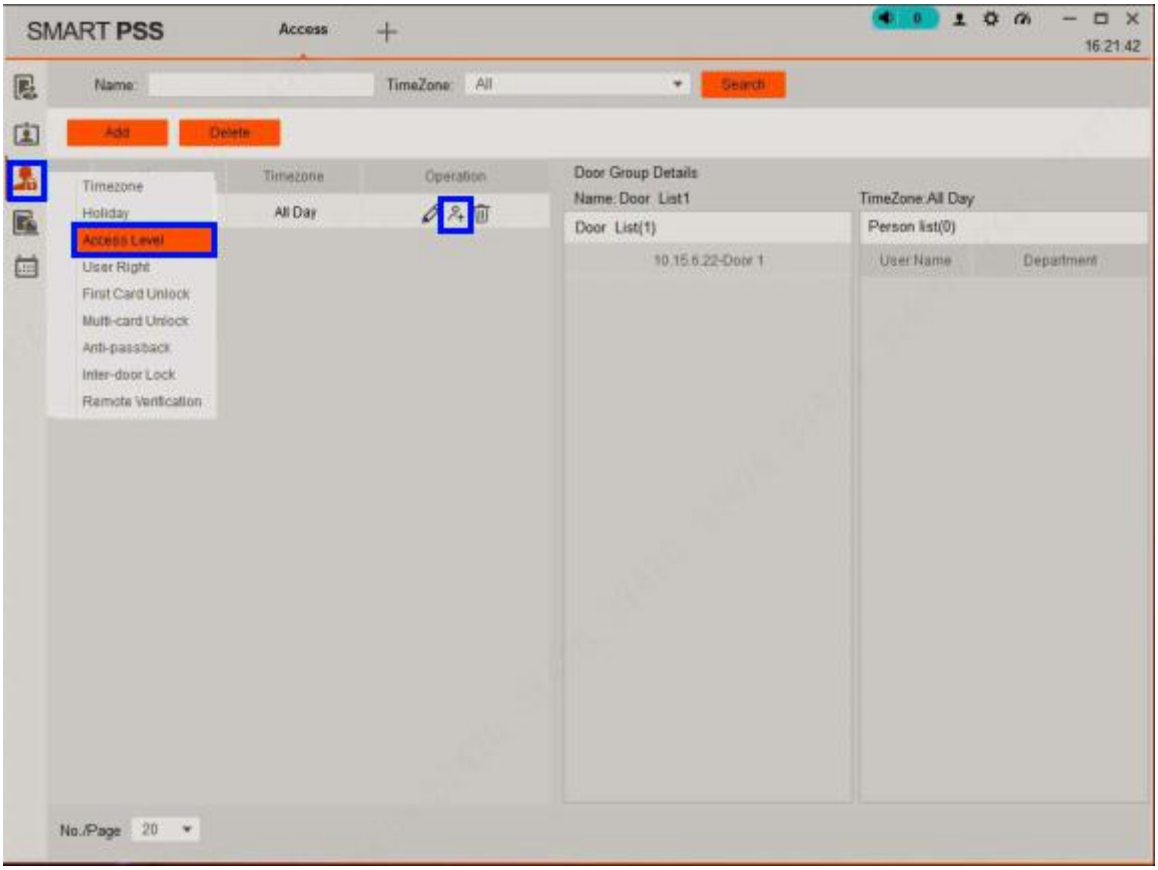
e) Select the Holiday Timezone then click OK when done.

In this example, on 2018-10-17 (Holiday), users can get access between 08:00-10:00 at Door 1 only.



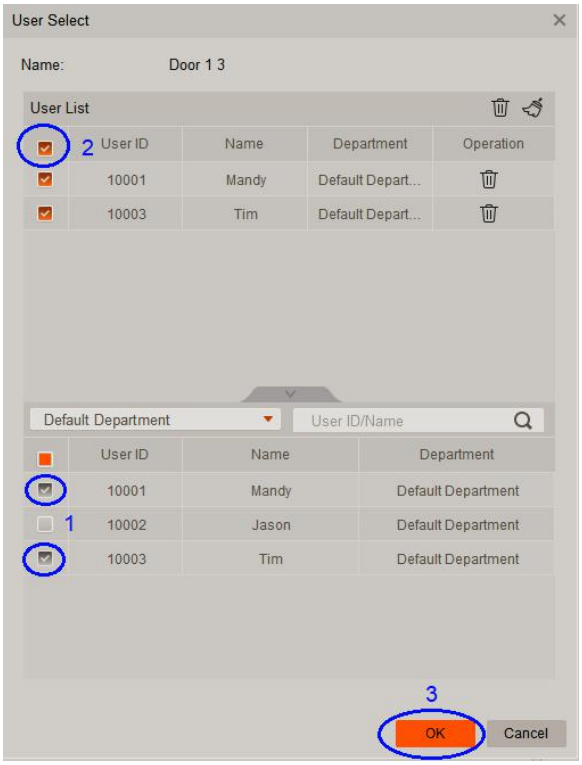
## 4.2.11 Assign user access levels

i. Click  , and then click “Access Level” and the  icon.




ii. When the “User Select” dialog box pops up, select the user’s department from the drop down list and click, or enter the user’s ID or name directly. You may also click the magnifier icon  to list all users out.

iii. Select users to be assigned to this door group and click OK button.




In this example, we've assigned users Mandy and Tim to group "Door 1 3". They have access to door 1 and door 3 only anytime.

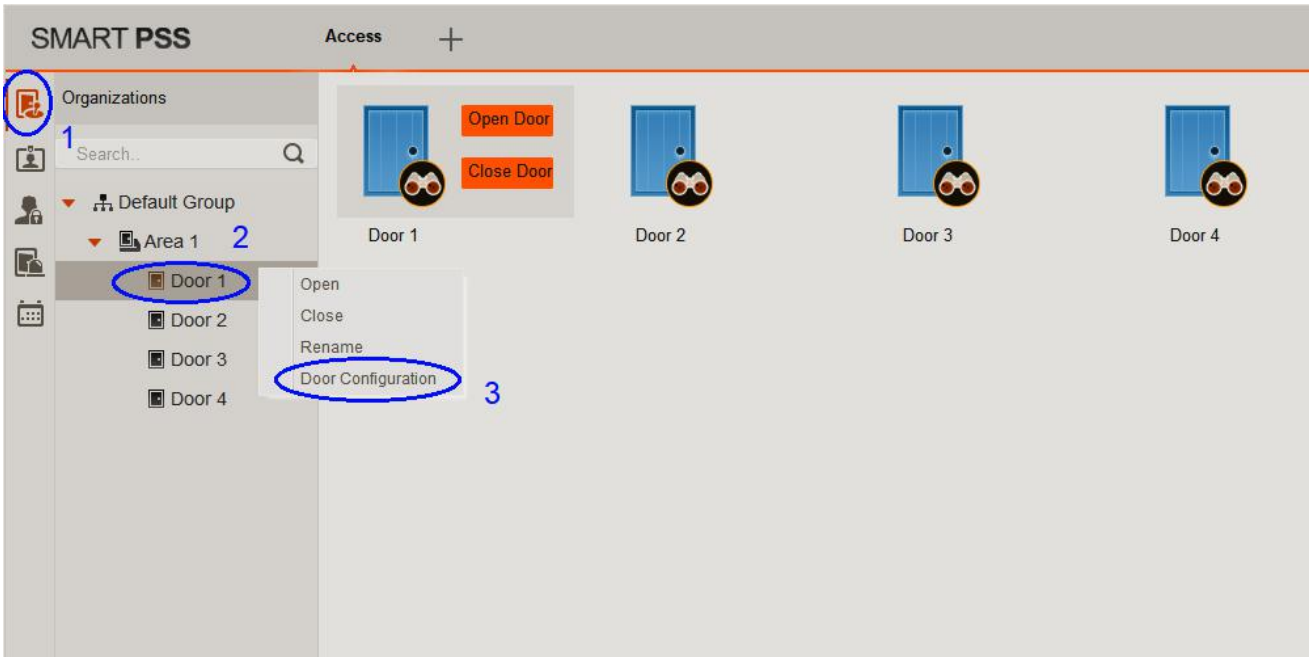
iv. Use the icon  to delete a user or  to delete all users.

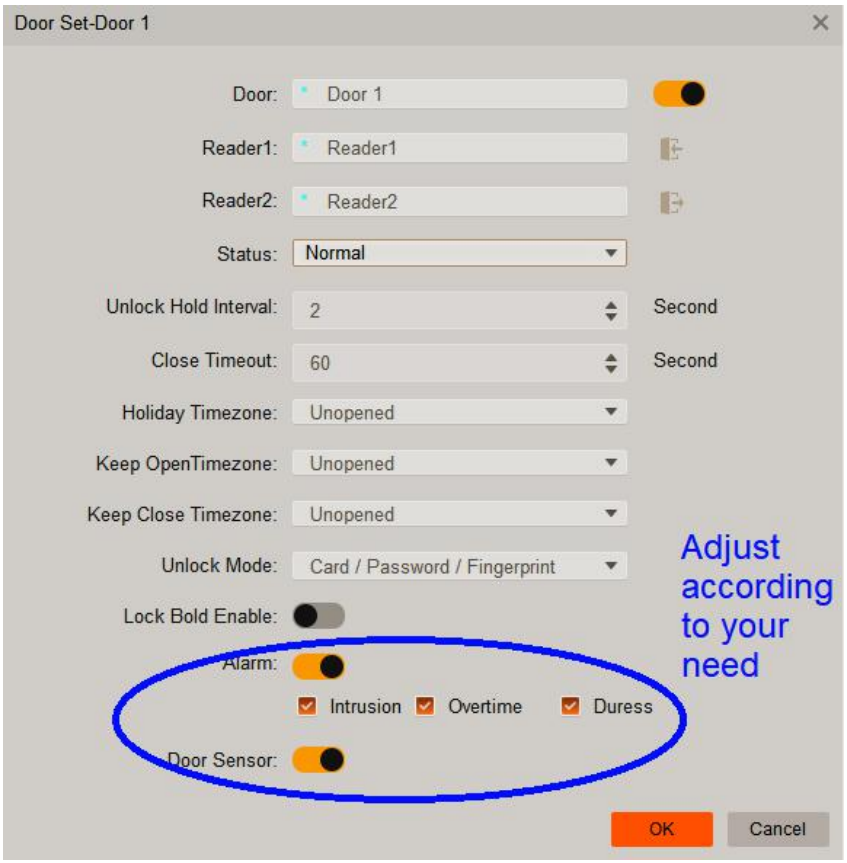
v.

## 4.2.12 Configure doors

i. Click the Console icon.

ii. Choose the door to be configured by **right click** the door name and click Door Configuration.






Door: Name of the door

Reader1: Name of the entrance reader

Reader2: Name of the exit reader

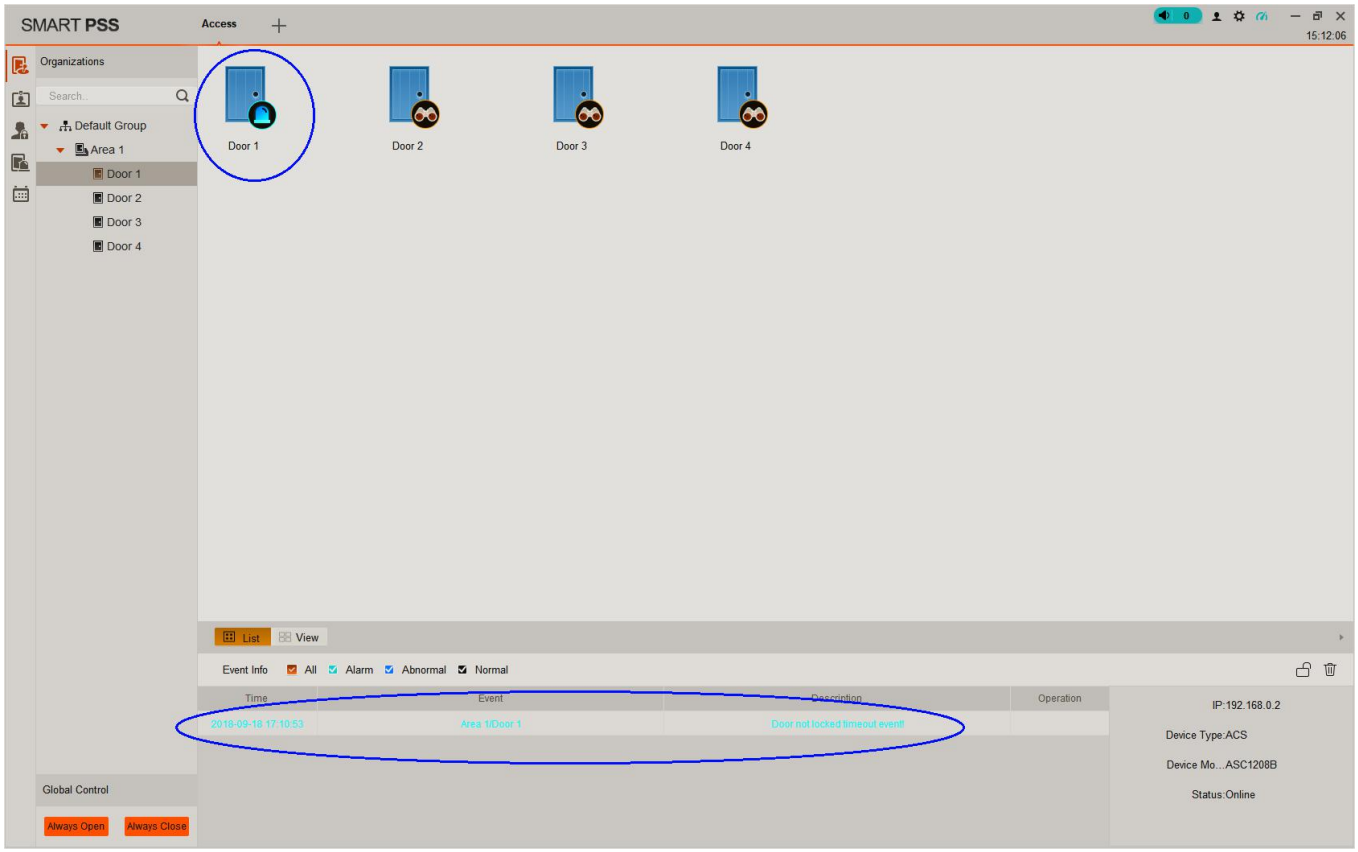
Status: Normal, Always Open, Always Close

Unlock hold interval: The time that the relay stays on to unlock.

Close Timeout: The timeout period if a door is leave opened before alarm is triggered.

****** Door Open/Close status switch must be connected for Intrusion and Overtime alarms to work.***

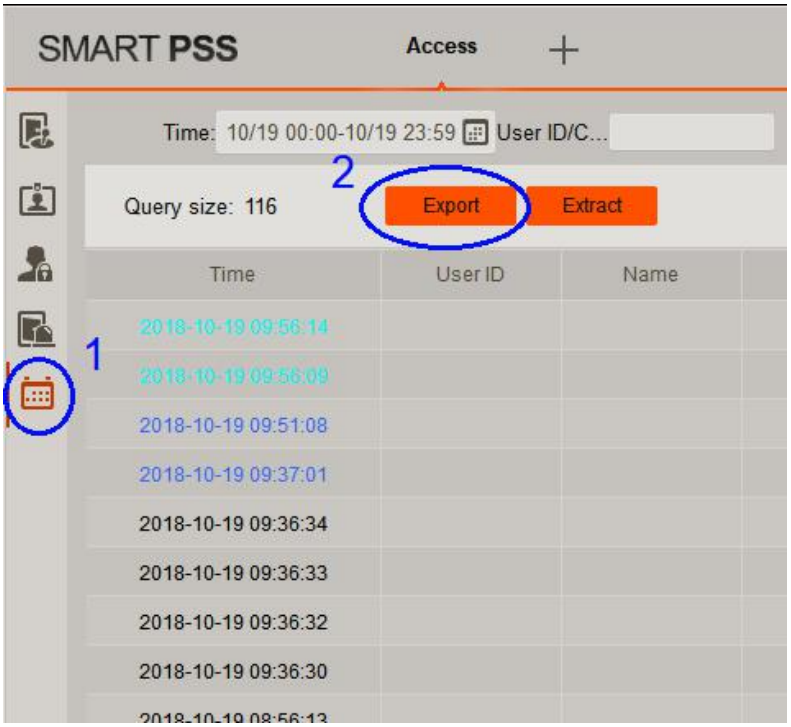
If the alarm is triggered, the following screen will be shown:



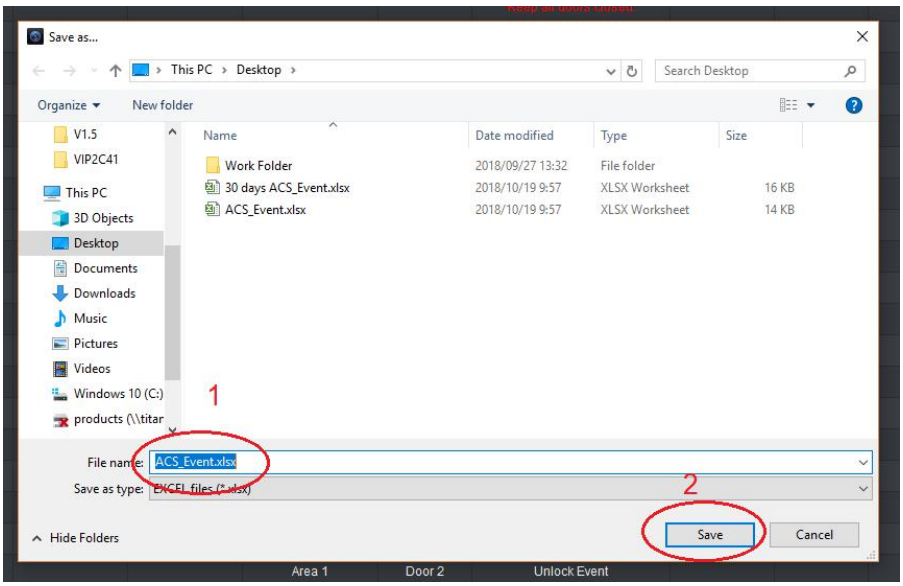
## 4.2.13 Log Records and Log Files

VIP access controller supports up to 150,000 log records. The log records can be exported to a file for data analysis.

a) Click the “Log” button on the side menu then click “Export” button. A dialog box will be shown.




b) Choose the folder and the name of the log file and click “Save”. The file format is Microsoft Excel compatible.



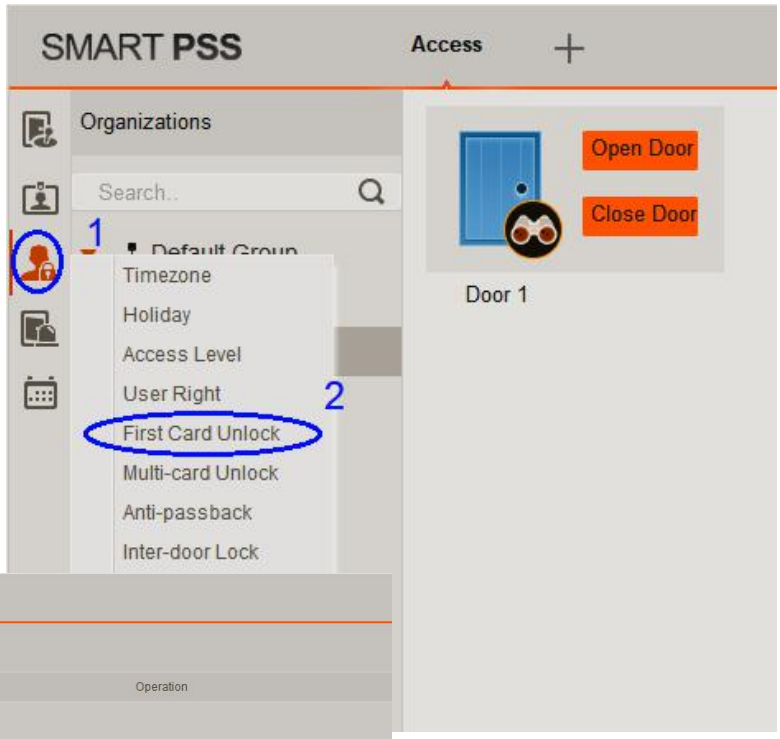
# 4.3 Advanced Functions

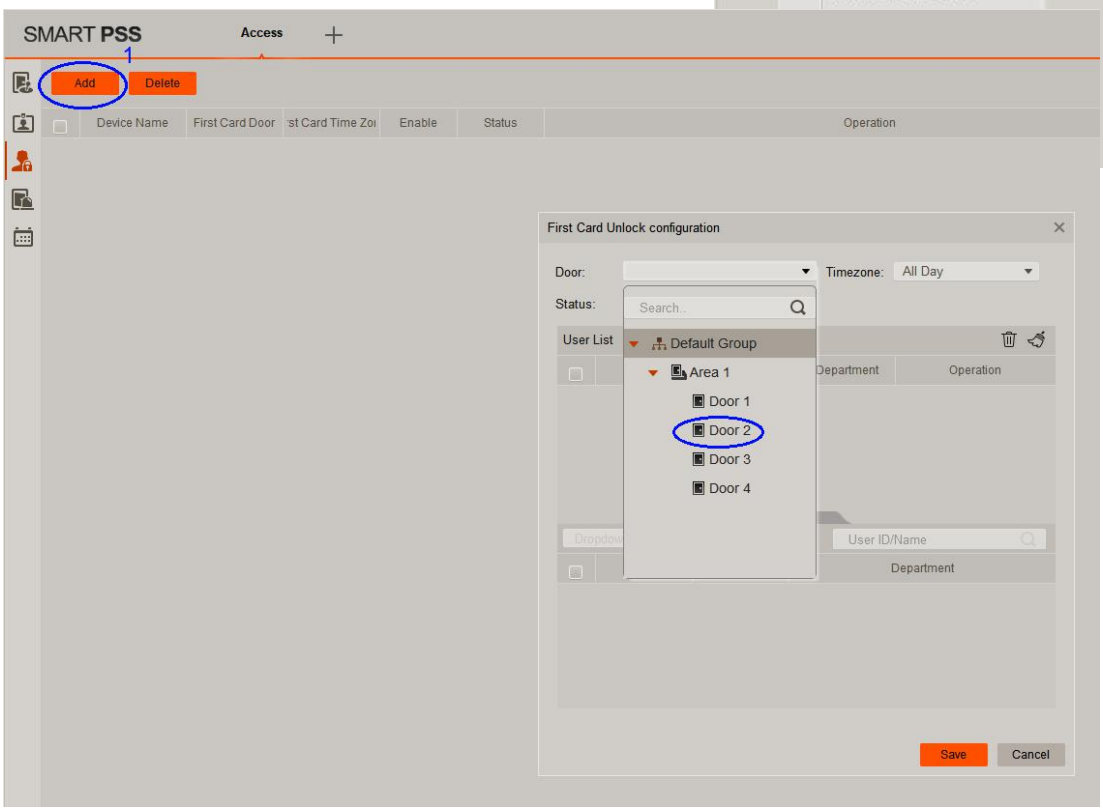
In addition to basic enter/exit functions, there are many advanced functions to further enhance the security levels. They are the First Card Unlock, Multi-card Unlock, Anti-passback, Inter-door Lock and the Remote Verification.

## 4.3.1 First card unlock

The specified doors must be unlocked by appointed users first, then other users can open the door afterward. It ensures that the door is always opened by appointed users before other users with lower access rights. For example, a shop manager must open the door earlier than the shop workers to make sure that the manager is in the shop when other workers come to work.

i. First click the “Upload User to Device” icon, then select “First Card Unlock.



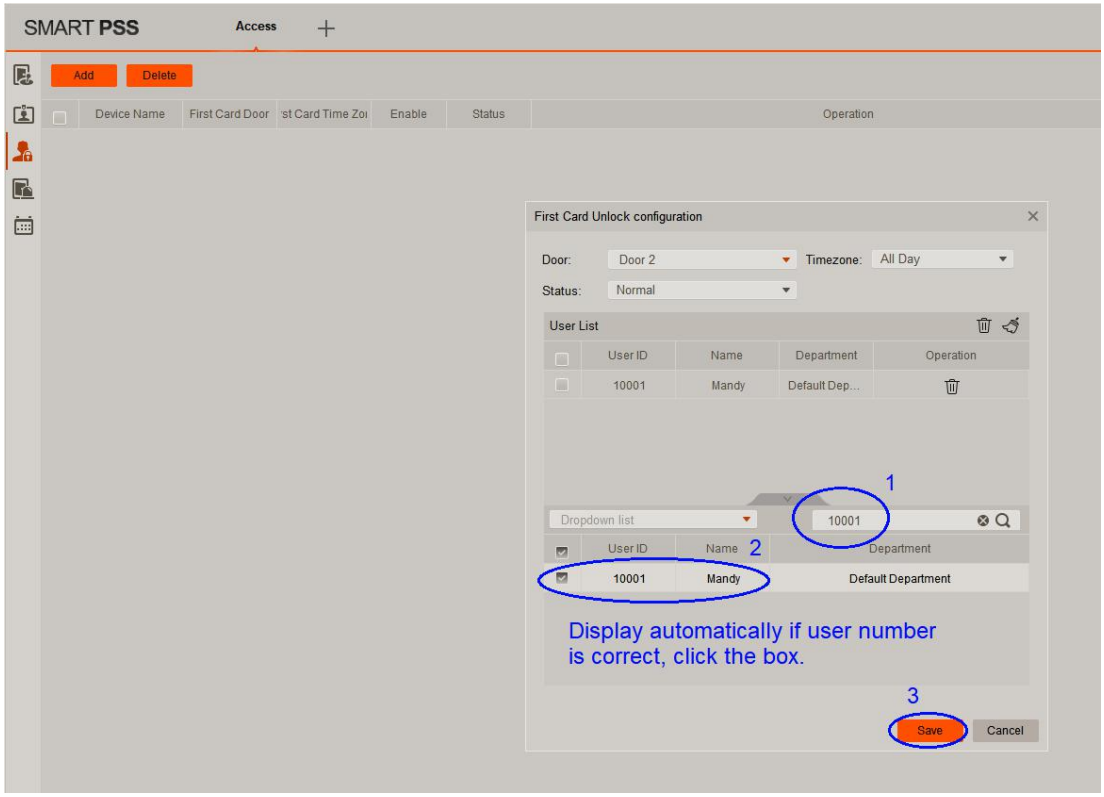



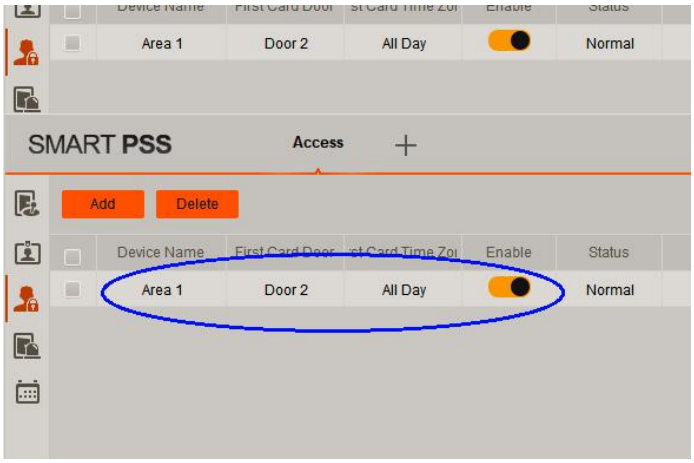

ii. Click the “Add” button and select which door is to be “First Card Unlocked”

iii. Enter the user ID or user name to be the “First Card Unlock” holder.

iv. The name will be displayed automatically if the information is correct

v. Click “Save” when done.



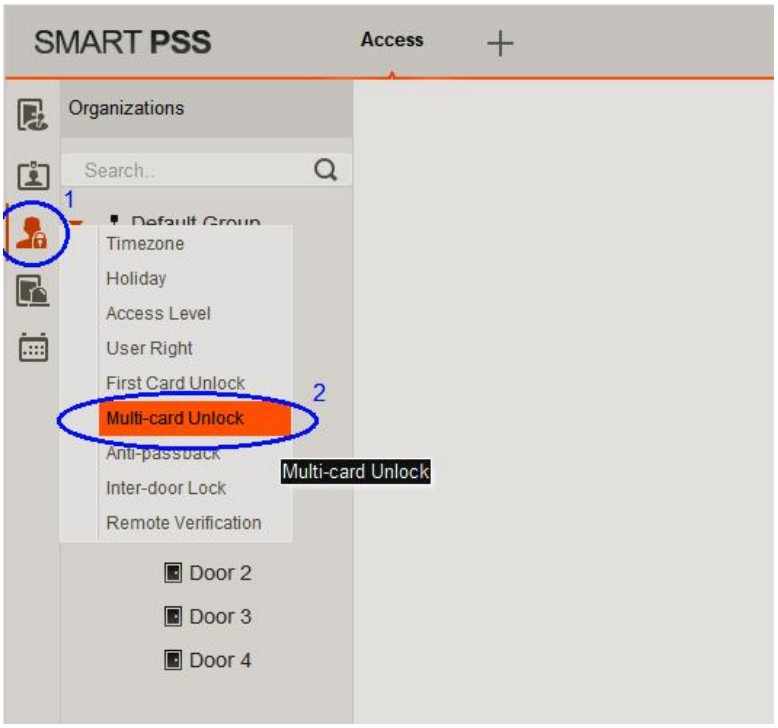




***vi.*** The Door information to be “First Card Unlocked” is shown.

In this example, Mandy is the supervisor to “First Card Unlock”. She must open Door2 before anyone does.

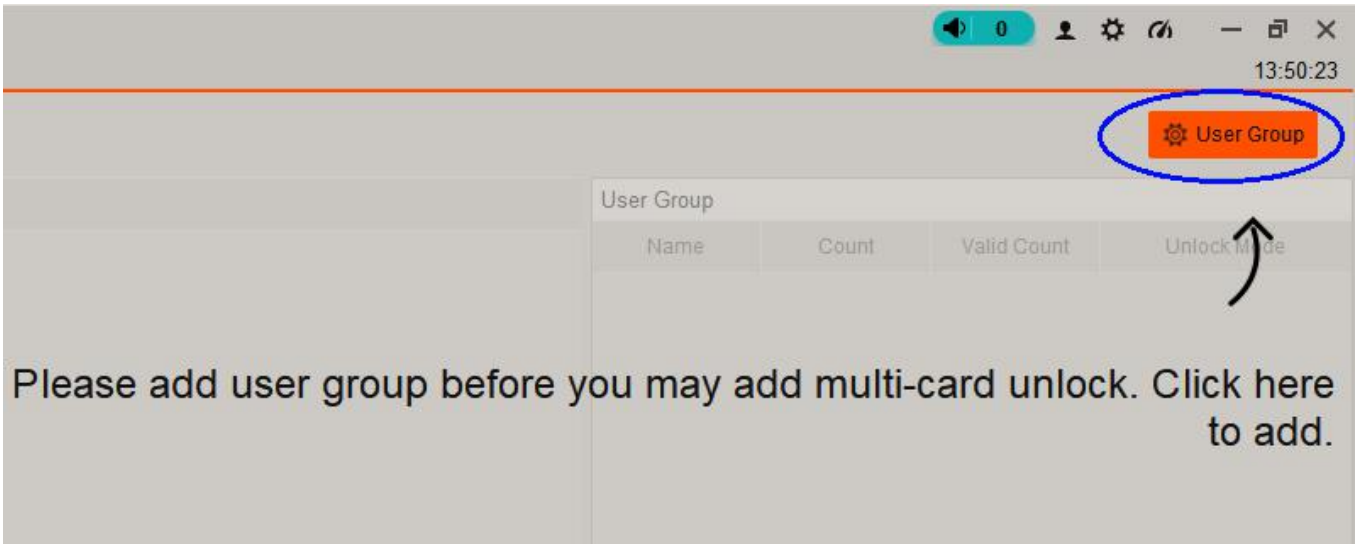
## 4.3.2 Multi-card unlock

The door is to be unlocked by **TWO** groups of user in specified order. This is similar to the First Card Unlock but it allows unlocking by anyone of the group members or unlocking by all of the group members.

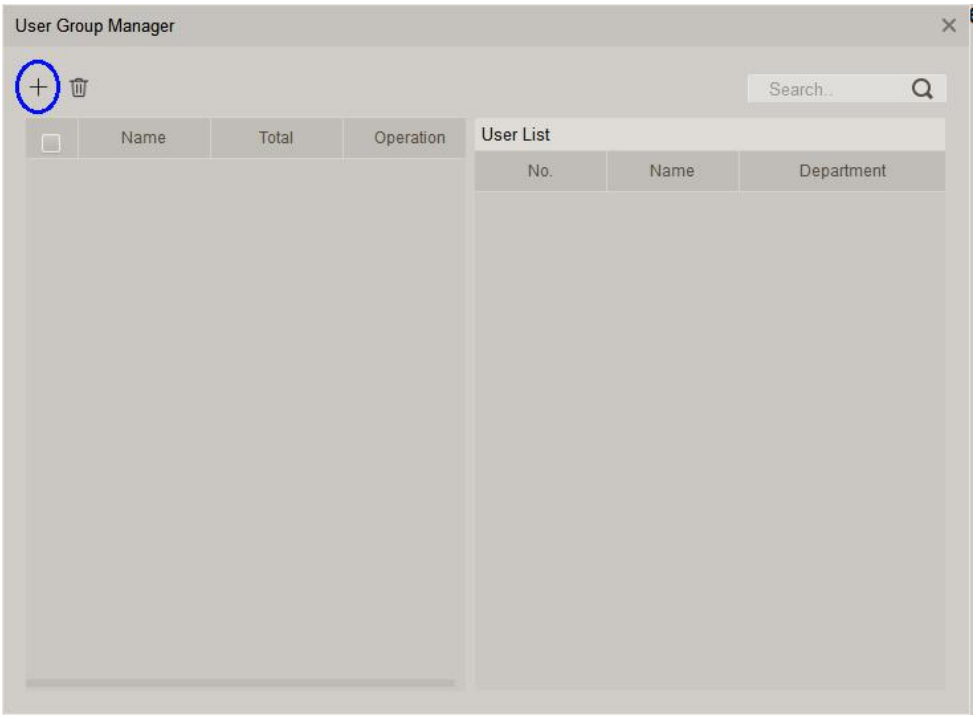



i. First click the “Upload User to Device” icon, then select “Multi-card Unlock”.

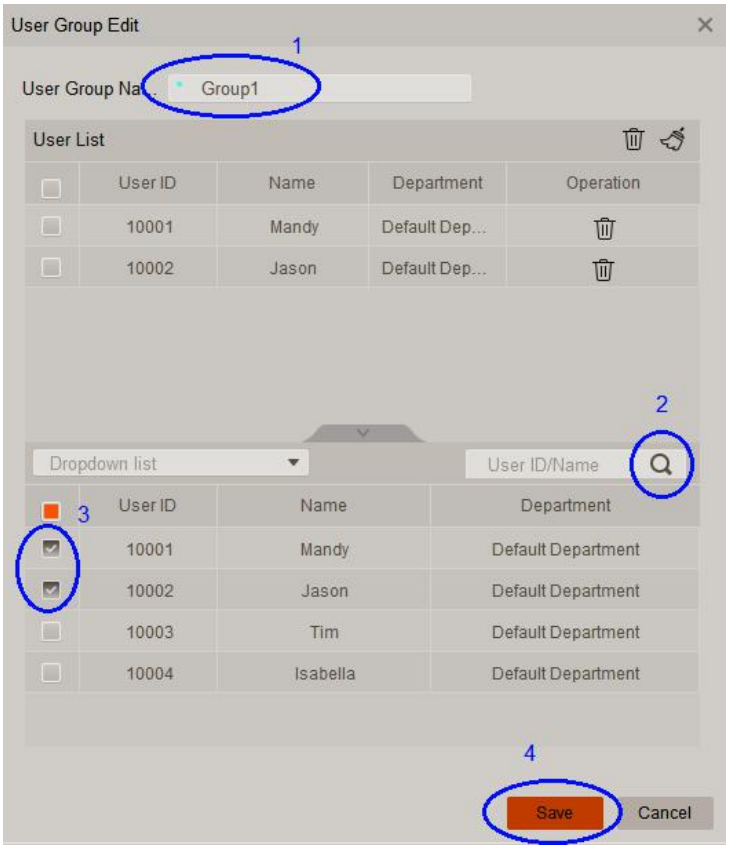
ii. Must add User Group first.

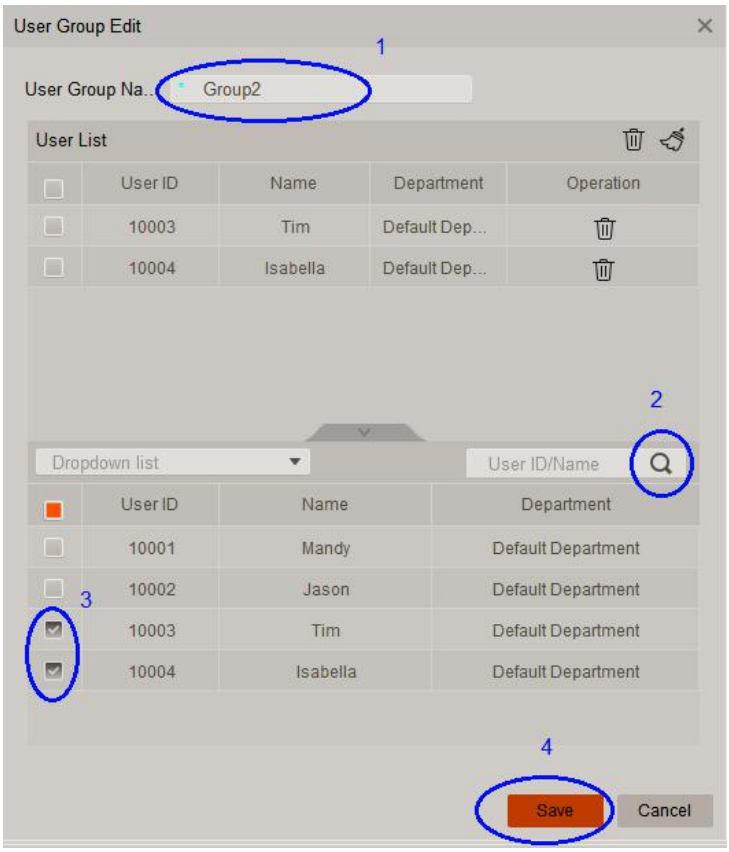


iii. Click the “+” symbol to add user group.
iv. Name the user group
v. Click the magnifier icon to search for users to be added.
vi. Click the users in this group.
vii. Click Save to finish.
viii. Repeat step iii to vii until all the groups are added.

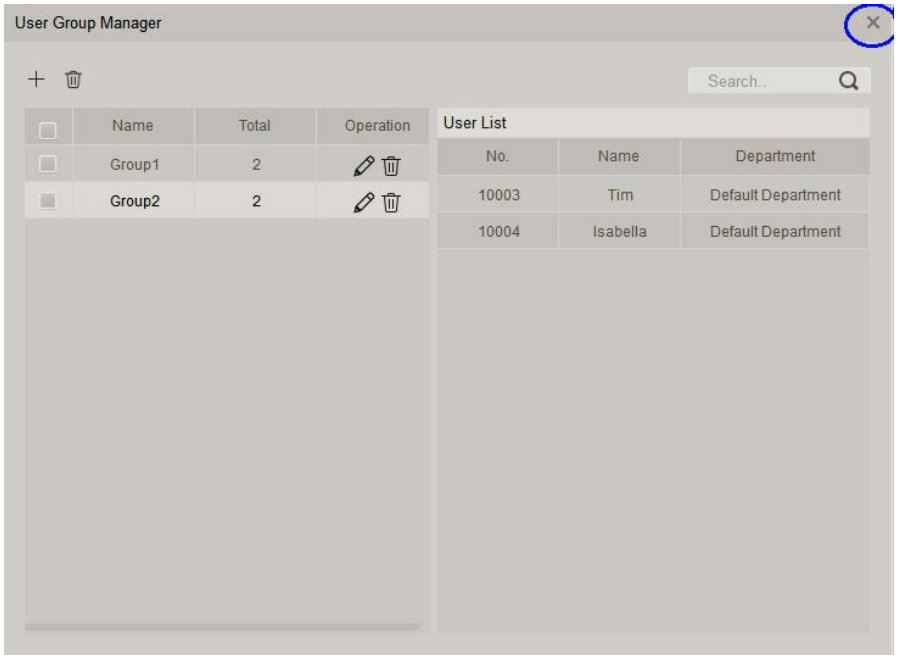



In this example, Mandy and Jason are in Group 1, Tim and Isabella is in Group 2.



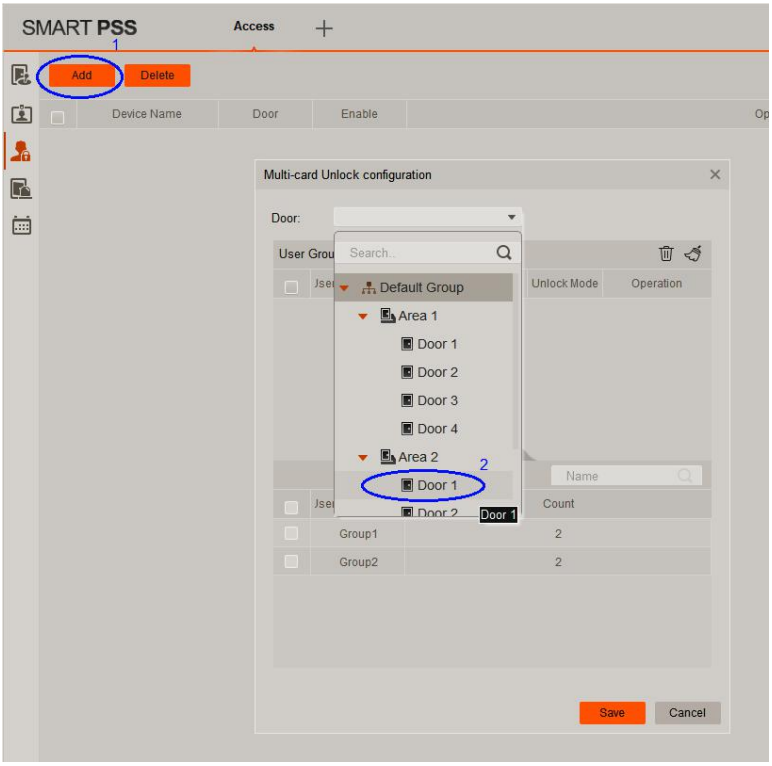



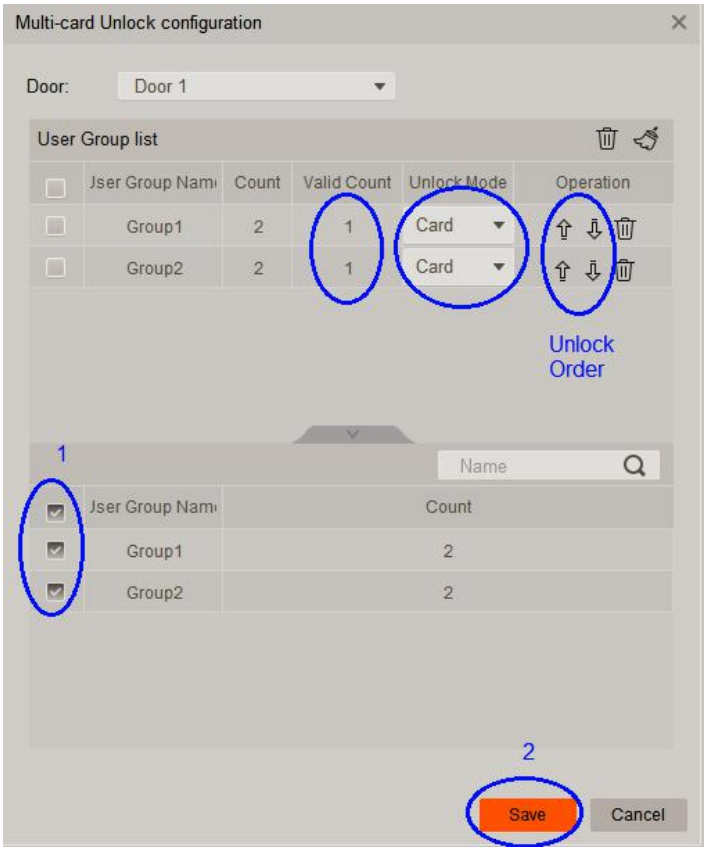
ix. Close the User Group Manager window.




x. Click Add button.

xi. Select the door to be “Multi-unlocked”



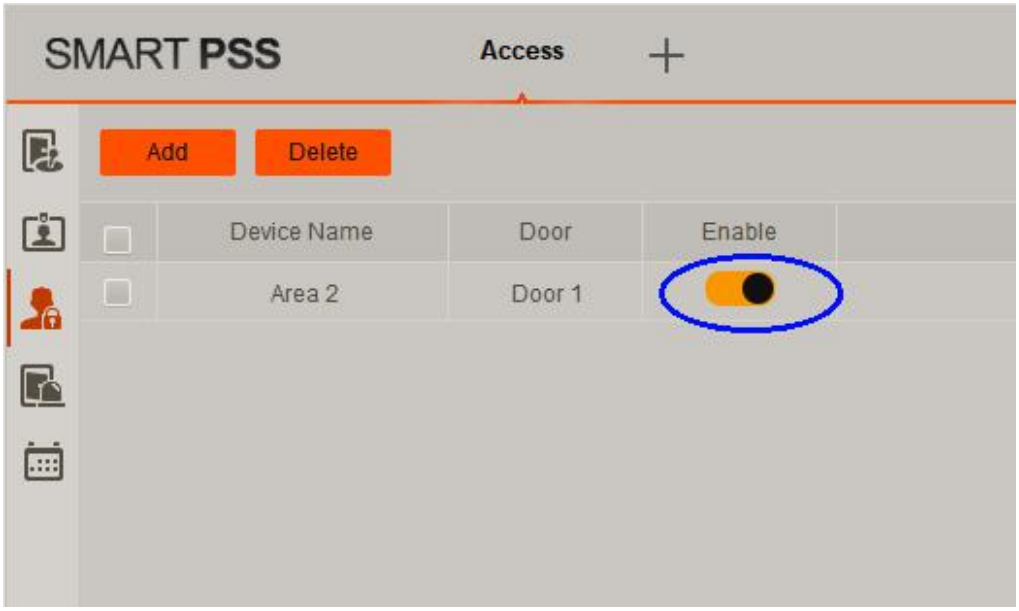




xii. Click the door groups and click SAVE to finish.

Note: You can select different unlock mode for each user to unlock: Card, Fingerprint or Password.

Valid Count: Number of users per group requires to Multi-Unlock, in our example, one user per group.

xiii. Once the set up is finished, you will see the following screen.You can enable or disable this function by the slide switch.




In the above example, Group 1: Mandy and Jason, Group 2 : Tim and Isabella.

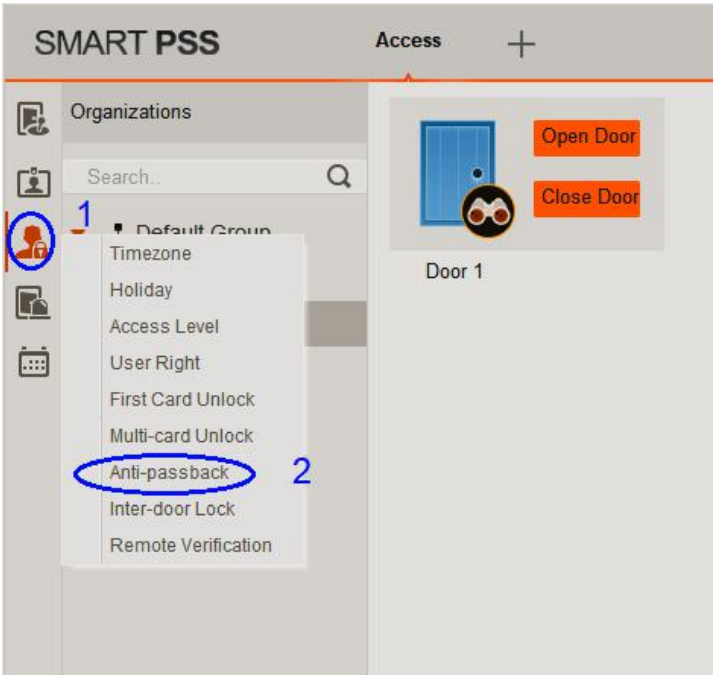
So, Mandy or Jason must unlock first and then Tim and Isabella can unlock, i.e. 1 group member from each group.

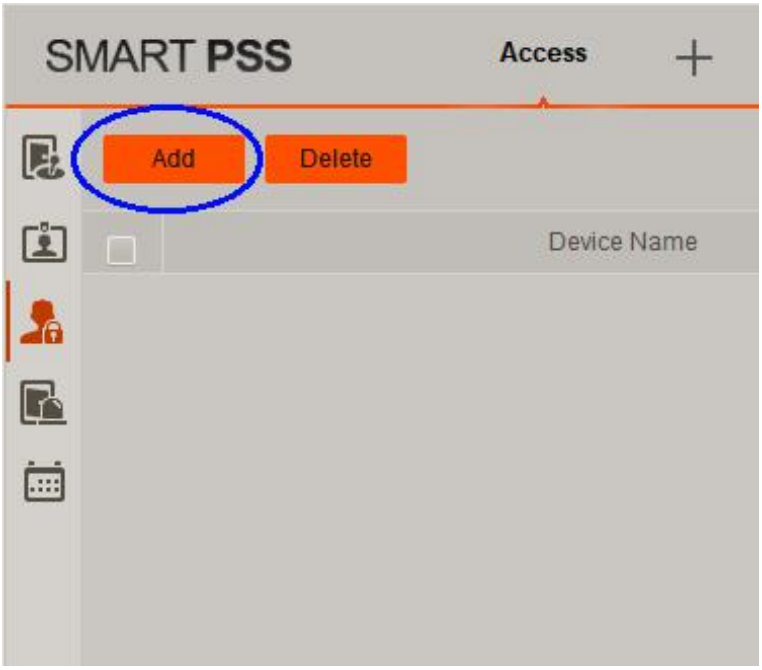
If Valid Count in both groups are set to 2, two group members in each group must be unlock, i.e. 4 users to unlock. The order is: Group 1 Mandy + Jason, then Group 2: Tim + Isabella. The unlock order within the same group is not important.

## 4.3.3 Anti-passback

The function is useful if there are two different doors for the entrance and exit. Once an user enters via the entrance door, he/she cannot open the entrance door again. If he/she wants to leave, he/she must use the exit door. Typical application: Car park.

i. First click the “Upload User to Device” icon, then select “Anti-passback”, then click the “Add” button to select doors to be “Anti-passback”.

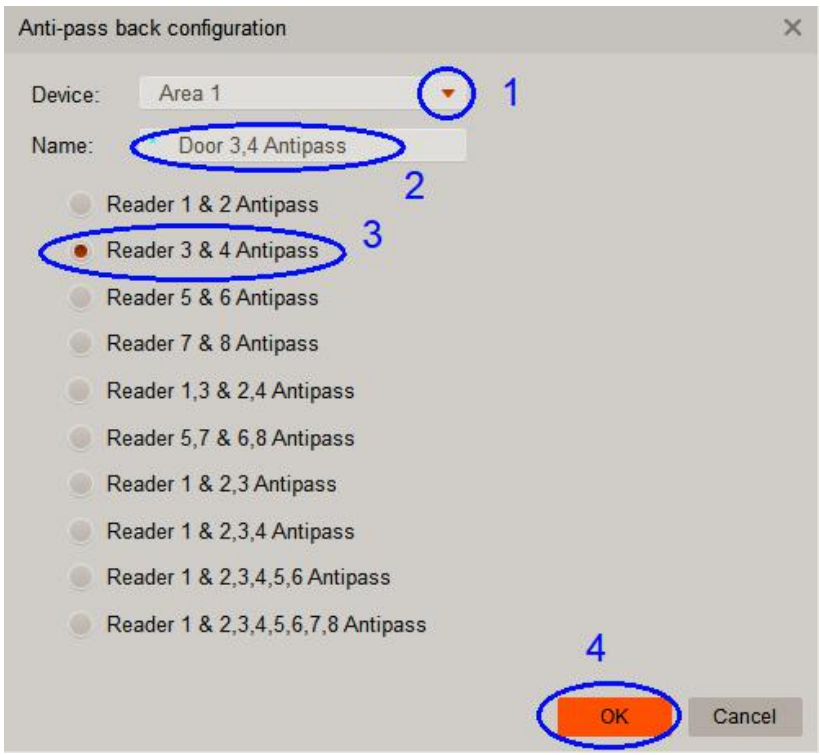



ii. Select Device (the name of the access controller) by clicking the drop down list.

iii. Name the Anti-passback rule.

iv. Select the doors to be Anti-passback

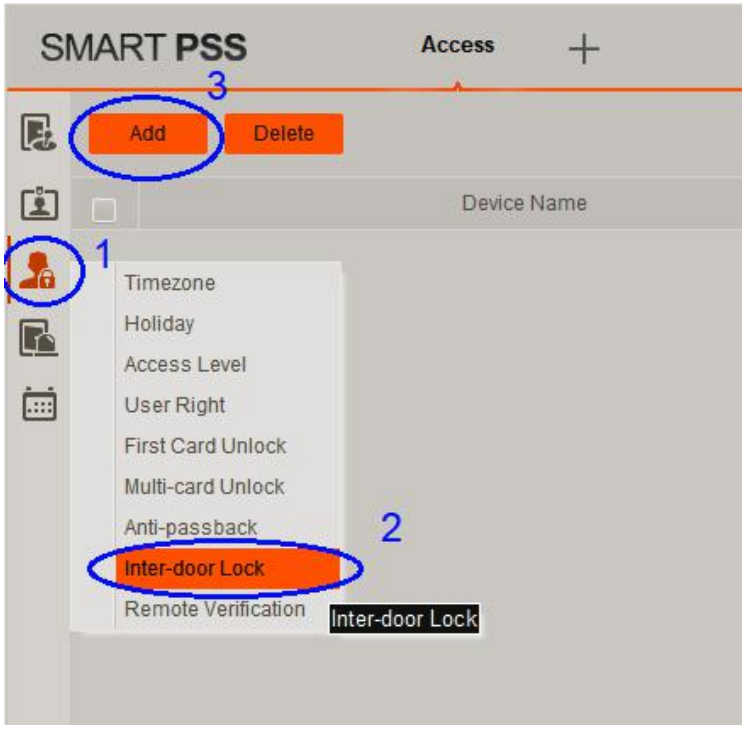



In this example, Area 1 access controller door 3 and 4 are “anti-passback”.
i.e. Users must enter from door 3 and leave from door 4, once they entered door 3, they cannot open door 3 again and must leave from door 4.

## 4.3.4 Inter-door lock

Door B cannot be opened if Door A is not closed. Typical application: Bank security doors. (Must install door open/close status sensors for this function to work)

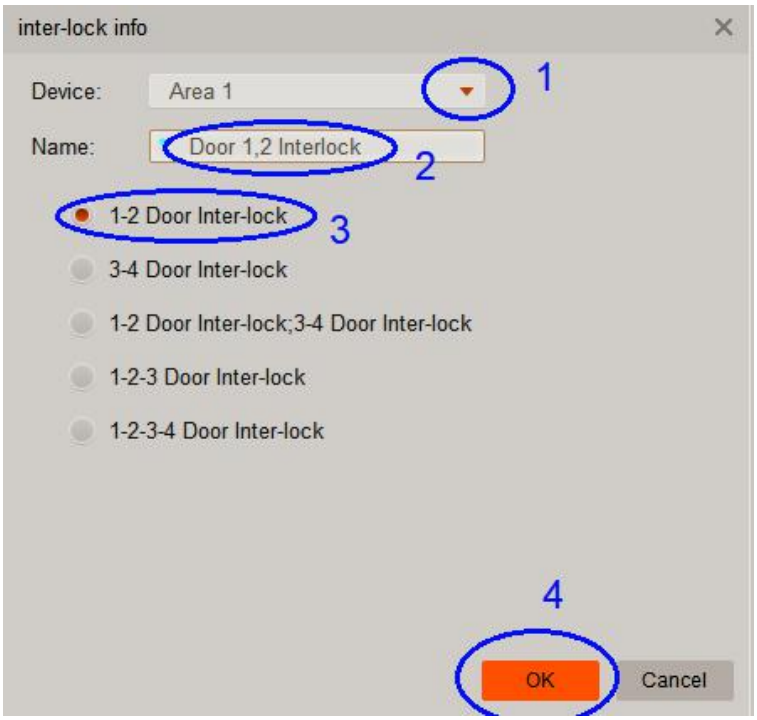
i. First click the “Upload User to Device” icon, then select “Inter-door Lock”, then click the “Add” button.




ii. Select Device (the name of the access controller) by clicking the drop down list.

iii. Name the Inter-lock rule.

iv. Select the doors to be Inter-lock




In this example, Area 1 access controller door 1 and 2 are “inter-lock”.
i.e. If Door 1 is not closed, users cannot open Door 2. Similarly, Door 1 cannot be opened if Door 2 is not closed.

***Important: MUST enable Door sensor in the “Door Configure” for this function to work properly.***

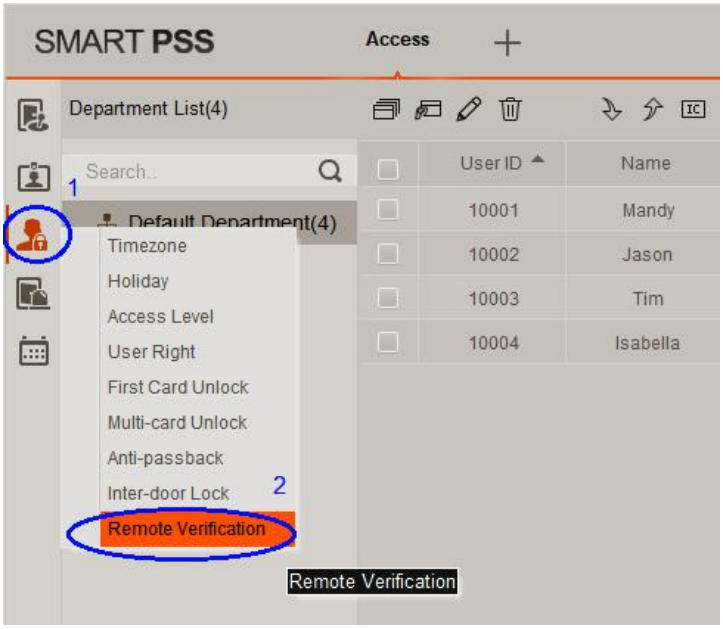
## 4.3.5 Remote Verification

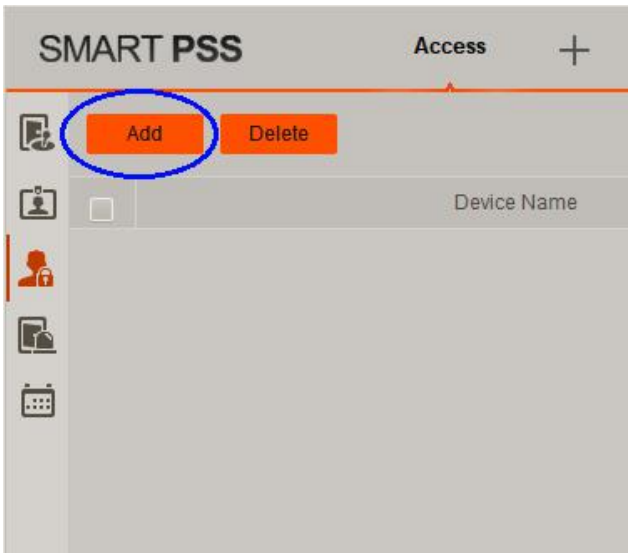
When enabled, every user with access rights to enter a door will be verified by photo stores in the system. When a user taps the access card at the door requires remote verification, the Network Surveillance Camera at that door will show his/her image. Also, a window with that user's photo is pop-up so the operator can verified. If the photo matches, the operator must open the door **manually** by clicking the "Open" button.

It is useful if human verification is required in some areas where high security is needed.

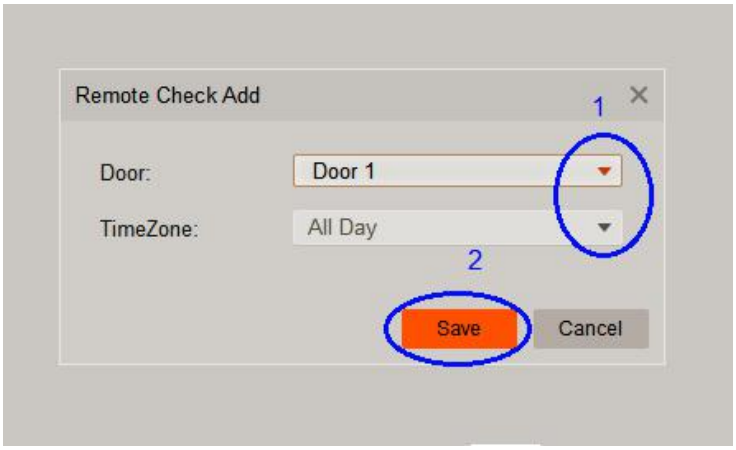
**Note:** ***Once this function is activated, the door must be opened MANUALLY after verification. Entering keypad password or tapping card on the card reader cannot open the door automatically anymore.***

i. First click the "Upload User to Device" icon, then select "Remote Verification", then click the "Add" button.

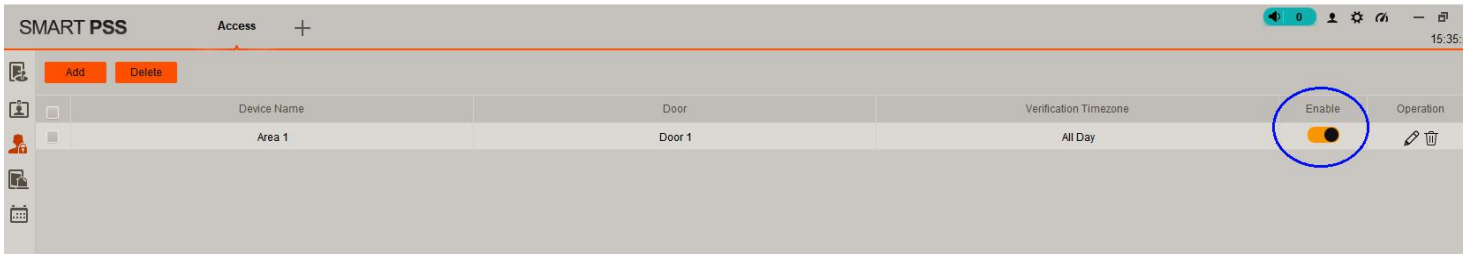



ii. Click to select the door and time need Remote Verification to be enabled and click "Save" button.

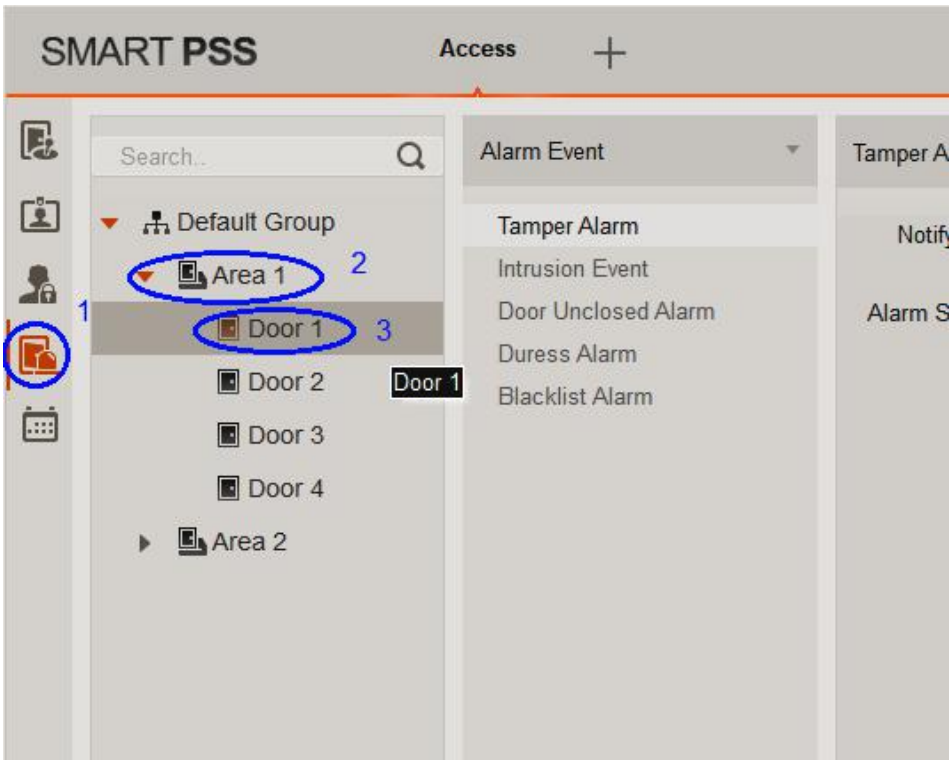


iii. Once the set up is finished, you will see the following screen.You can enable or disable this function by the slide switch.

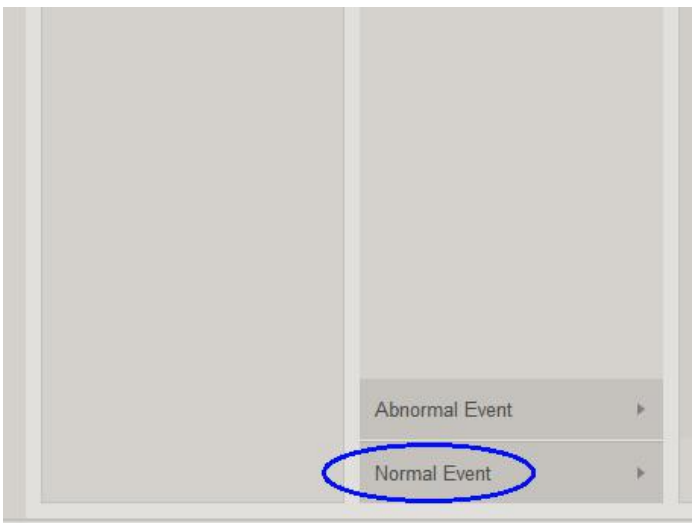


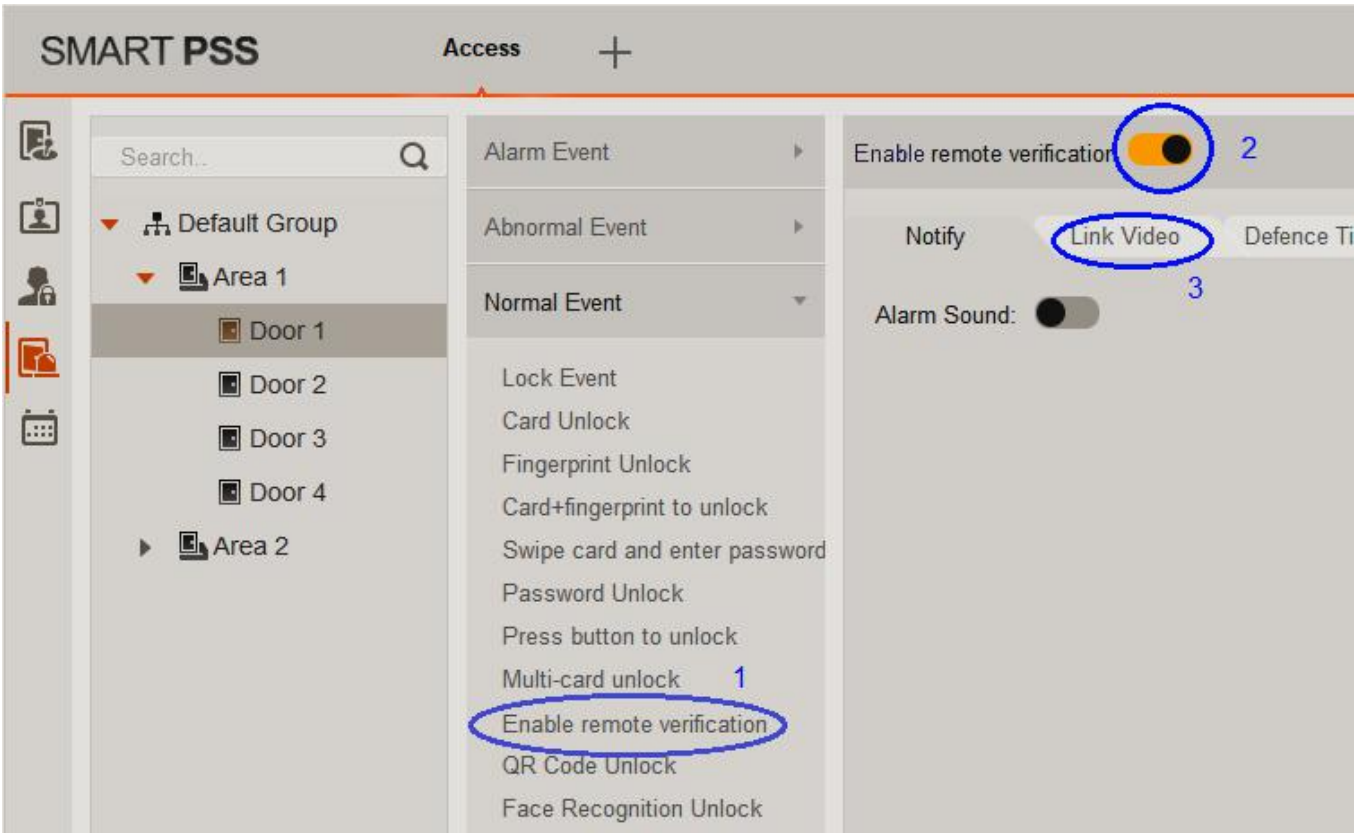

iv. Wait, wait, wait… Not finished yet!

v. Click the event icon, double click Access Controller (Area 1) and the door to be “remote verified”. In this example, Door 1 of Area 1 is selected.



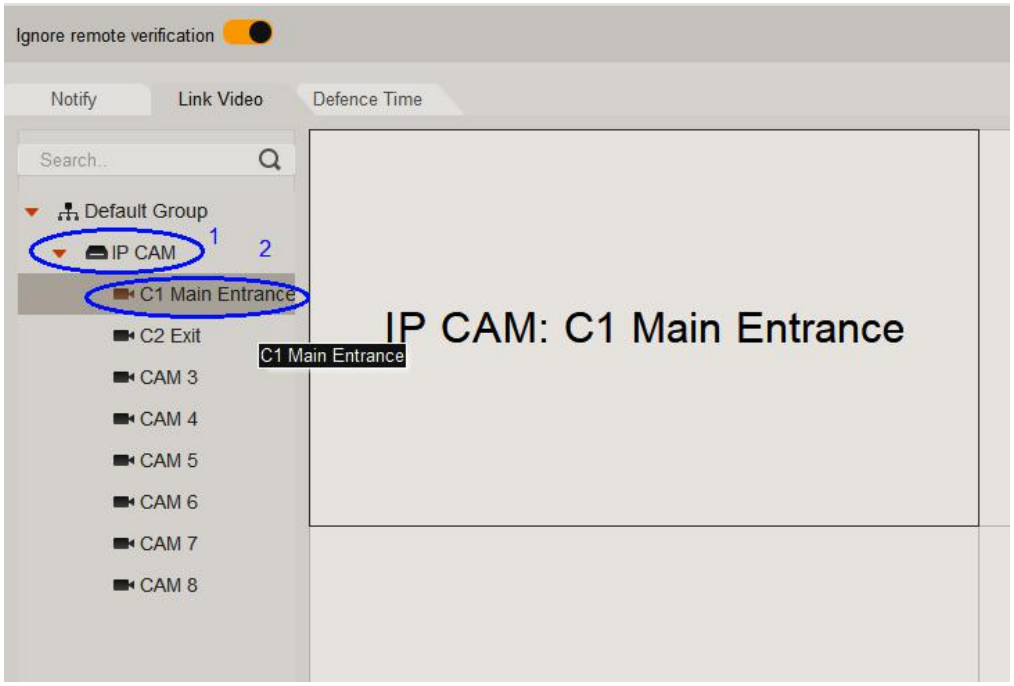

vi. Look at the bottom of the screen and click “Normal Event”






vii. The “Normal Event” jumps up to top when clicked. Now select the “Enable remote verification” and turn on the slide switch, then click the “Link Video” tab to select the camera to be opened when a user taps the card at specified door, in our example, Door 1.

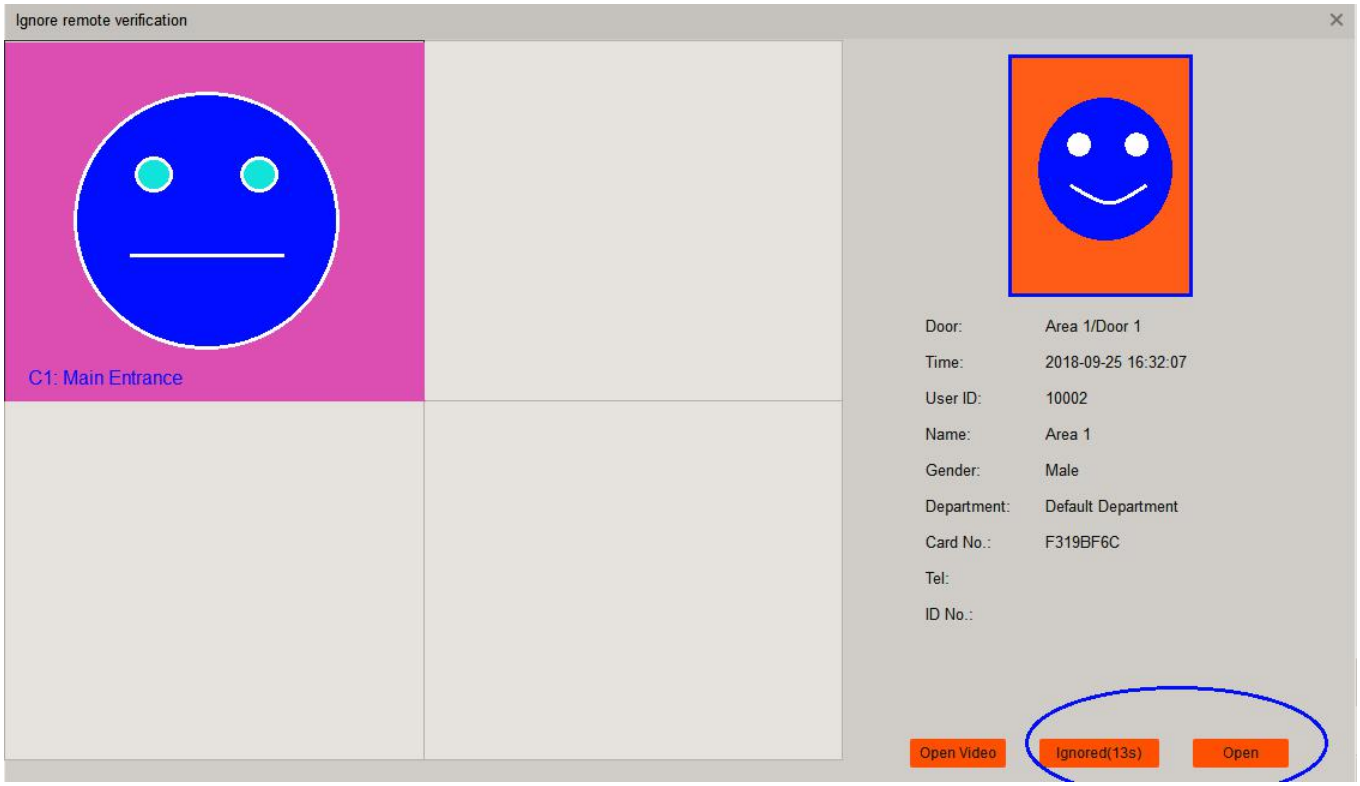
viii. Double click the IP Cam controller (Network Video Recorder - IP CAM in this case) and select the camera to be turned on.



x. Make sure the slide switch “Auto Open Video” is on (Blue colour) and click “Save” button to finish.

Now set up of remote verification has been completed.

In our case, if someone tap the card at Door 1, the monitor will display his/her photo and switch the camera locates at Main Entrance on so that the operator can verify the face of the one at Main Entrance match the photo of the card holder or not. If they match, operator **MUST** click “Open” button to unlock the door. If “Ignored” is clicked or no action is taken within 15 seconds, the door will remain unlocked.




Note: To activate this function, you must set the IP address of the Network Video Recorder to be in the same subnet of the access controller. In our case:

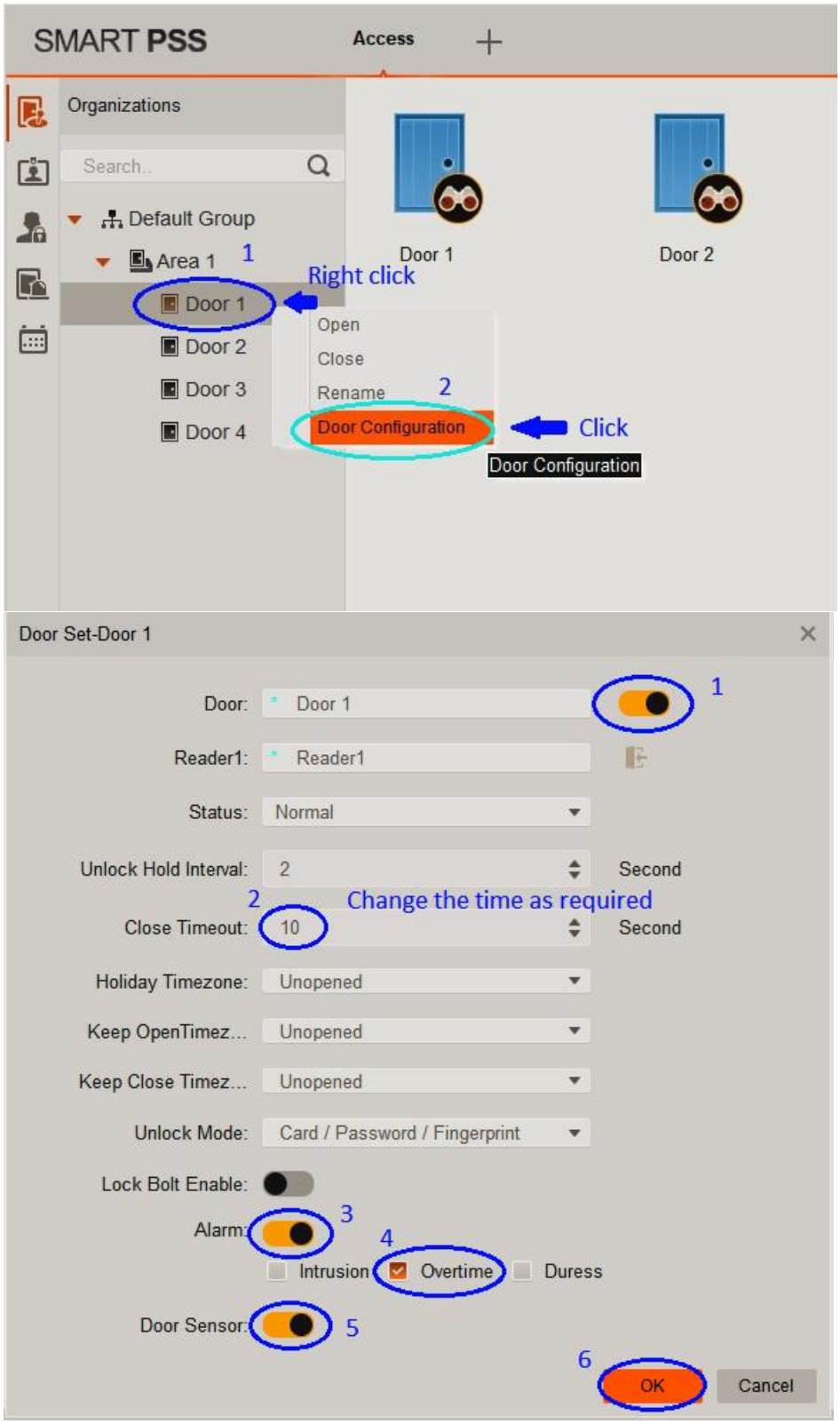
| | |
|---|---|
| Access Controller IP Address: | 192.168.0.2 |
| PC IP Address: | 192.168.0.199 |
| Network Video Recorder IP Address: | 192.168.0.108 |

## 4.3.6 Door open timeout

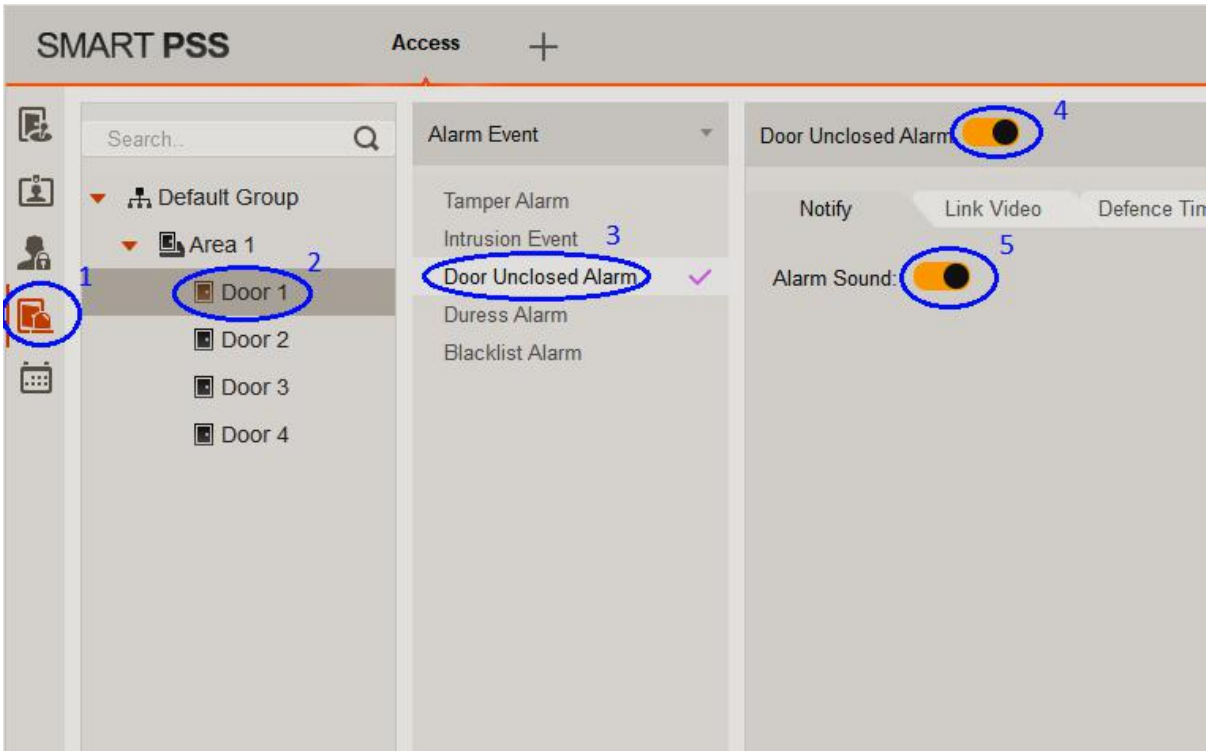
VIP access controller is able to notify the operator when a door is opened for a time exceeding the preset period. You must first add the door sensor (reed switch) to feed back the status of the door to the access control. Then, follow the steps below to configure SMART PSS.

### Adding door sensor for the door open timeout function

Step 1 - Configure the door



Step 2 - Tell Smart PSS what to do when door is kept opened for a long time. In this example, to tell the Smart PSS to report an alarm event.




Click Save button (Not shown here, lower right corner of the screen) to continue.

When finished, the PC speak will sound if the door is opened for a period longer than the preset period.

**Note:**
1) Smart PSS must be installed and running on a PC when the notification is required.
2) PC must equipped with a speaker.
3) The notification is a continue short and quick beep sound for about 1 second only.

# 4.4 Events

Simply speaking, an event is when incident A occurs, B will take some kinds of action. “Remote Verification” mentioned above is a good example. If someone taps the card at Door 1 ( incident A) , the Main Entrance Network Camera will display the user who taps the cards at Door 1.

The actions when an event occurs are to “Link Video” and generate alarm sound in **PC speakers**. To enable the event, you must enable that event by sliding the slide switch to right hand side.

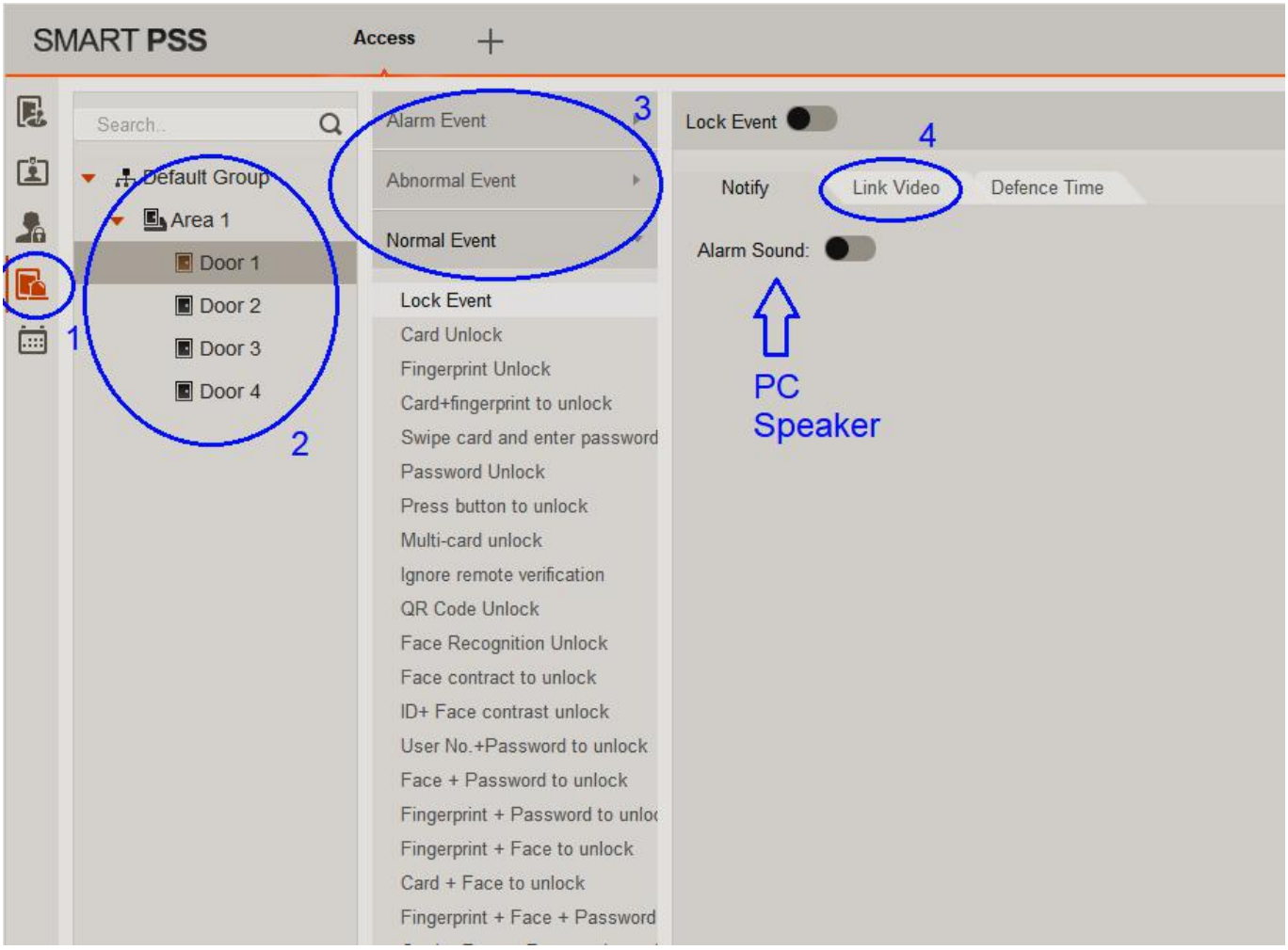
To configure an event:

1) Click the Event icon 

2) Select the door where you want to monitor.

3) Select event type: Normal, Abnormal or Alarm.

4) Select the action when an event is triggered.



## Summary of available events

| Event Type | Description |
|---|---|
| Alarm Event | Tamper alarm：Alarm is triggered when the card reader is un-installed. |
| | Intrusion alarm：Alarm is triggered when a door is opened abnormally. |
| | Duress alarm：Alarm is triggered when a door is opened by duress card. |
| | Door Unclosed alarm：door remains opening and exceeds the set time |
| | Blacklist alarm：Alarm is triggered when door is opened via blacklisted card. |
| Abnormal Event | Card unregistered: Alarm is triggered when the card is un-registered or it has been reported lost. |
| | Card suspended：Alarm is triggered when the card is suspended/freeze. |
| | Unlock mode error：Alarm is triggered when the door is not unlocked by specific unlock method. |
| | Card Validity error：Alarm is triggered when current time is not within card validity. |
| | Timezone error：Alarm is triggered when a user try to enter the door at unauthorized time. |
| | Holiday unlock Timezone error：Alarm is triggered when verification of current period is not in holiday period. |
| | Incorrect first card：Alarm is triggered when a door is not unlocked by the first card user first. |
| | Inter-lock mode：Alarm is triggered if a user tries to open the second door when the first door is opened. |
| | Anti-pass Back Mode: When one enters via verification but exits without verification, alarm is triggered at his/her next |
| Normal Event | Lock event：Alarm is triggered when the door is initially open and then closed |
| | Card unlock：Alarm is triggered when the door is unlocked by tapping cards. |
| | Fingerprint unlock：Alarm is triggered when the door is unlocked by fingerprints. |
| | Card + fingerprint to unlock：Alarm is triggered when the door is unlocked by first tapping cards and pass fingerprints verification. |
| | Card +password unlock：Alarm is triggered when the door is unlocked by first tapping cards and pass password verification. |
| | Password Unlock：Alarm is triggered when door is unlocked by entering password. |
| | Press Button to Unlock：Alarm is triggered when door is unlocked via button. |
| | Multi-card unlock：Alarm is triggered when the first card in multi-card unlock mode passes verification. |
| | Enable remote verification：Alarm is triggered when a user passes remote verification. |

# 5 Troubleshooting

Please refer to the table below for easy troubleshooting. The table below describes some typical problems and their solutions. Please consult these guides before contacting your place of purchase.

| Problem | Solution |
|---|---|
| Cannot connect to PC console | • Ensure that you changed the PC network card IP address to 192.168.0.xx where xx is 0-255 (except 2)<br>• Ensure that network cable is plugged in the PC and the LAN port of the access controller.<br>• the Access Point. |
| No power | • Ensure that power switch is switched on.<br>• Check power cord connection.<br>• Confirm that there is power from the outlet.<br>• Ensure the power supply meets or exceeds the current rating<br>• for the device you are powering. |
| Fingerprint reader is not working | • Make sure the fingerprint reader is connected on 485 bus. |
| Some cards cannot be used | • Ensure that RFID IC cards with frequency of 13.56MHz are used.<br>• Low frequency RFID ID cards (125kHz) are not supported for higher security. |
| Unable to unlock door | • Check the wiring between keypads, card readers, fingerprint readers to the access controller.<br>• Check the wiring between the door electric strikes/bolts and the access controller.<br>• Ensure that jumpers on the access controller main board are set correctly<br>• Check door lock power. |
| User added but cannot get entry | • Ensure that the user has assigned access level to entry particular doors.<br>• Ensure the user enter the door at correct time.<br>• Ensures that the card is not frozen or reported lost. |
| Internal alarms: Intrusion, Door open timeout and tamper not working | • Ensure that door sensor is installed and Alarm and Door Sensor slide button is switched on in the door configuration menu. |
| Card readers, keypads and fingerprint readers are working intermittently | • Ensure that Cat 5e cables are used.<br>• Ensure that the electric strikes/bolts are using separate power supply. |
| Cannot open the door by door push button | • Check door push button wiring, make sure it is wired to the correct door.<br>• Disable Remote Verification for the door to be opened by push button. |

| | |
|---|---|
| No video image for remote verification | • Only VIP series of Network Video Recorder System is supported.<br>• Ensure that Remote Verification is enabled and video is linked to the specified camera. |
| The access controller does not open doors at correct time | • Ensure that the time on the PC console is synchronized with the access controller. Make sure time is adjusted when Daylight Saving starts and ends. |
| Cannot capture user pictures using USB camera | • Only VIP series of USB camera is supported. |

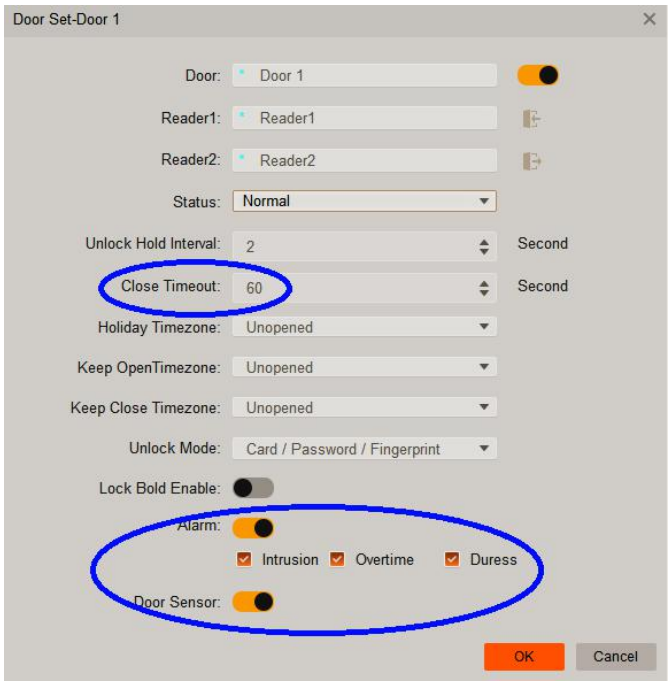
# 6 FAQs

**Q:** I have enabled the Intrusion and “Door unclose” (overtime) warnings but they are not working, why?

**A:** First, you must wire up the door status sensors for the doors to be monitored.

Second, you must enable “ALARM” and “Door Sensor” and check on the “Intrusion” and “Overtime” box in the “Door Configuration”.

Change the timeout period if you need.



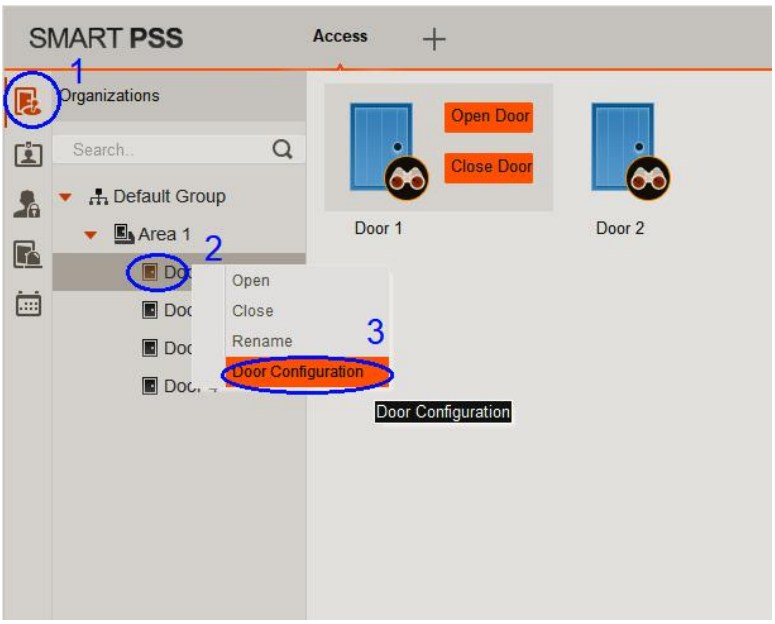

**Q:** How do I access the “Door Configuration” menu?

**A:**

a) Click the “Console” icon on the top left corner of the screen.

b) Select the door you want to configure and **RIGHT** click the mouse.

c) Click “Door Configuration”.



Q: How to reset the system to factory settings?

A: First power off the controller then switch DIP switch 1,3,5,7 to ON position and power ON. After a few seconds, a repeating beep sound will be heard every 2 seconds. Turn off the controller and switch and switch DIP switch 1,3,5,7 to OFF position. Power on again and the system is reset to factory settings.

Q: Do I have to set up User rights and Access Levels etc again after reset to factory settings? I can see the information is still in the PC console?

A: Unfortunately, you **must** set up User rights and Access Levels etc again after reset to factory settings. Although you can see the user information and access levels on the PC, these information has not downloaded to the controller. You **must** clear all information previously added to the PC console before you start setting up the PC console again, so it is strongly suggested that not to reset to factory settings easily.

Q: Fingerprint verification is working intermittently, why?

A: Make sure the finger is registered. Finger to be recognized must be clean, not too wet or not too dry. Make sure the finger covers most of the the fingerprint scanner window.

Q: Fingerprint reader can read cards but cannot read fingerprints, why?

A: Fingerprint readers **must** be wired up on 485 bus, i.e. use the wires 458+ and 485- for the Fingerprint readers. Disconnect the Wiegand signal connections before you connect the 485 bus.

Q: Can I connect the Wiegand and 485 wires from the same reader to the control panel at the same time?

A: Technically, yes but why ? We strongly recommend that for a single reader, only one connection method should be used.

Q: Can I use Wiegand connection for some readers and 485 connection for other readers?

A: Yes, the access controller accepts mix connection.

Q: On the “Add user” or “Edit user” screen, what is “Card Password” and “Unlock Password”?

A: Card password can be ignored, not used because no password is needed when you tap the card.

Unlock password is the password for the keypad. Password can be from 1-6 digits. Suggested password length is 6 digits for more security.

Q: What do I need to pay attention when setting the password?

A: Do not use simple password such as “123456”, “000000”,”111111” etc…

Do not use “0” as the first digit for the password. The access control ignores leading zeros.
For example, if you entered “012345” as the password, you can access the door by entering “012345” or “12345”.
Suggested password length is 6 digits.

Q: Can I use ID cards instead of IC cards?

A: No, IC cards are much more secure than ID cards. VIP access controller gives you the best security options so we do not use IC cards in our new designs and products.

Q: Can I Inter-lock/Anti-passback doors connected to different access controllers but are in the network.

A: No, Inter-lock/Anti-passback locks must be in the same access controller.

Q: I cannot open the door by tapping cards, inputting passwords or clicking “Open Door” on the PC console. Why?

A: Make sure Remote Verification of that door is disabled. If it is enabled, the door can **ONLY** be opened manually after verified by the PC console operator.

Q: I want to add another access controller, but the IP address is the same as the one already installed (192.168.0.2), so what should I do?

A: a) First unplug the network cable for the one already installed.

c) Plug another network cable to the new access controller. (Need 2 network cables for 2 controllers)

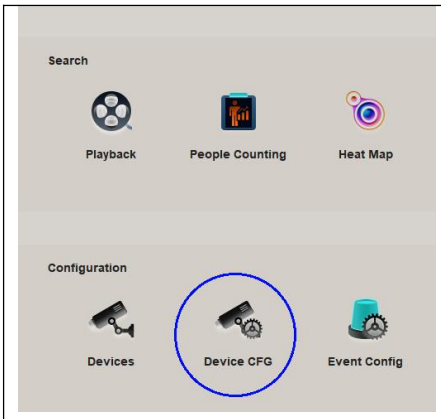
d) Change the IP address of the new access controller, e.g. 192.168.0.3 (See the last question of FAQs)

e) Plug the network cable back to the old access controller. (Now 2 network cables should be connected)

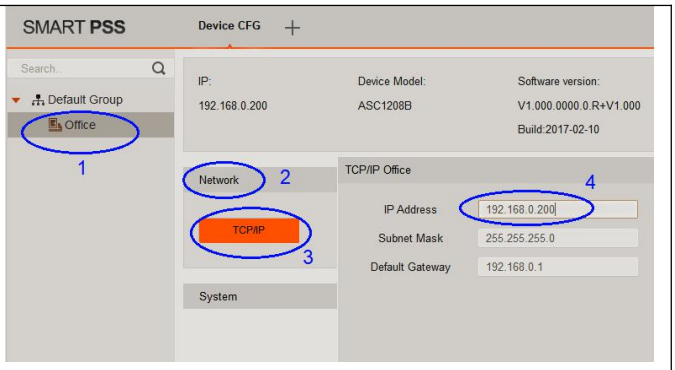
f) Power off both controllers and power on again.

**Q:** Can I change to other IP for the access controller after I finished setting up the system?

**A:** Yes, you can. But we suggest not to do it as you will lost control of the access controller if you set up improperly or you forget the new IP address. If the access controller's IP address and your setting do not match, you cannot access the controller anymore. You have no choice but to reset to factory settings which will reset the IP address back to 192.168.0.2.

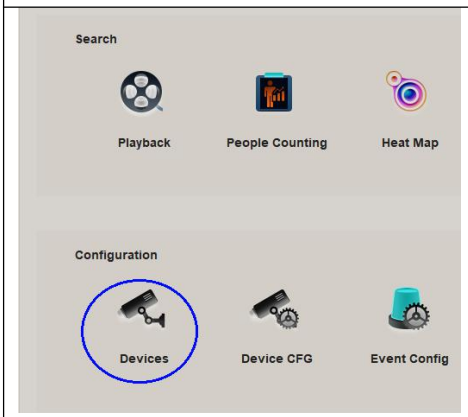



Click the Device CFG icon on the main menu.

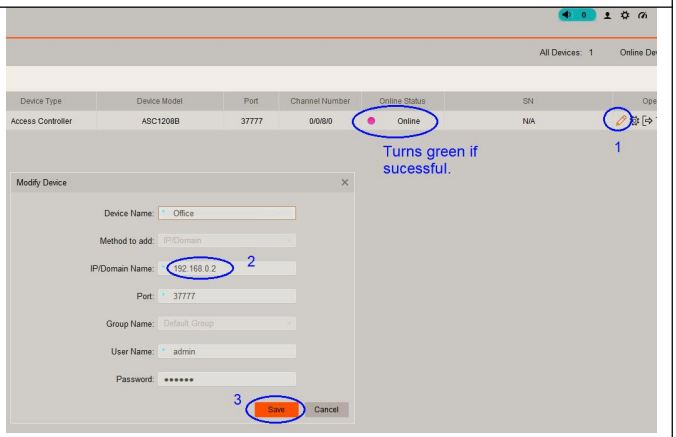



1) Click the access controller's name.
2) Click Network and then TCP/IP.
3) Enter the NEW IP address. Must be 192.168.0.xx where xx is 0-255 and has no conflicts with other devices on the network switch.
4) Click "Save" button below this dialogue box.

The access controller will generate a long beep and restart.



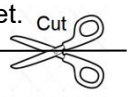

1) Close the Device CFG menu and go back to the main menu.
2) Click the Devices icon on the main menu.




1) Click the modify icon. 
2) Enter the new IP address. Must match the two IP addresses.
3) Click Save button.
4) If the modification is successful, the Online Status indicator will turn green.

# 7 After Installation

Its is always a good practice to write down the installation details so that the installer or the user can see the installation summary for ease of system maintenance. Cut this table and stick it inside the access controller cabinet.




## Installation Summary

**Model:** _____ **Installation date:** _____

**IP Address:** _____ **Installed by:** _____

### Function Summary

| Function / Door | Door 1 | Door 2 | Door 3 | Door 4 | Door 5 | Door 6 | Door 7 | Door 8 |
|---|---|---|---|---|---|---|---|---|
| First Card Unlock | | | | | | | | |
| Multi-Card Unlock | | | | | | | | |
| Anti-Passback | | | | | | | | |
| Inter-door Lock | | | | | | | | |
| Remote Verification | | | | | | | | |
| Intrusion Alarm | | | | | | | | |
| Door Timeout | | | | | | | | |
| Duress Alarm | | | | | | | | |

### External Alarms

| Terminal | Device | Enabled | Disabled | Output Device |
|---|---|---|---|---|
| Alarm 1 | | | | |
| Alarm 2 | | | | |
| Alarm 3 | | | | |
| Alarm 4 | | | | |
| Alarm 5 | | | | |
| Alarm 6 | | | | |
| Alarm 7 | | | | |
| Alarm 8 | | | | |

***Note: The number of external alarm inputs is different by different models.***

# 8 Limited Warranty

Cornick Pty Ltd (Seller) warrants its products to be in conformance with its own plans and specifications and to be free from defects in materials and workmanship under normal use and service for forty-eight months from the date of original purchase. Sellers obligation shall be limited to repairing or replacing, at its option, free of charge for materials or labour, any part which is proved not in compliance with Sellers specifications or proves defective in materials or workmanship under normal use and service. Seller shall have no obligation under this Limited Warranty or otherwise if the product is altered or improperly repaired or serviced by anyone other than Seller.

For Warranty Service: Return transportation prepaid with a copy of your purchase receipt and contact details to:

Cornick, Unit 1/9 Hannabus Place, Mulgrave, NSW 2756 Australia.

Seller has no obligation to attend the buyer's location to retrieve the goods or make repairs on site.

- There are no warranties, expressed or implied, of merchant ability, or fitness for a particular purpose or otherwise, which extend beyond the description on the face hereof. In no case shall seller be liable to anyone for any consequential or incidental damages for breach of this or any other warranty, express or implied, or upon any other basis of liability whatsoever, even the loss or damage is caused by its own negligence or fault.

- Seller does not represent that the products it sells may not be compromised or circumvented; that the products will prevent any personal injury or property loss by burglary, robbery, fire or otherwise; or that the products will in all cases provide adequate warning or protection. Customer understands that a properly installed and maintained alarm system or video surveillance system may only reduce the risk of a burglary, robbery, or fire without warning, but it is not insurance or a guarantee that such will not occur or that there will be no personal injury or property loss as a result.

- Consequently, seller shall have no liability for any personal injury; property damage or other loss based on a claim the product failed to give any warning. However, if seller is held liable, whether directly or indirectly, for any loss or damage arising under this limited warranty or otherwise, regard less of cause or origin, seller's maximum liability shall not in any case exceed the purchase price of the product, which shall be the complete and exclusive remedy against seller.

- This warranty replaces any previous warranties and is the only warranty made by the Seller on this product. No increase or alteration, written or verbal, of the obligations of this Limited Warranty is authorized.

Please refer to the website (www.vip-vision.com) for a full list of trading terms.