Access Control Series
Installation Manual

Version: VIPACC-Q121

Thank you for purchasing this Access Control system.
This install guide covers basic setup, installation and use of your surveillance system.

For detailed technical support and software downloads, visit our Help Centre at:
help.c5k.info

help.c5k.info

Table of Contents

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:

IP/Domain Name: 192.168.0.2
User Name: admin
Password: 123456
Maintenance password: s4musvvcai

Component	Image
Access Controllers ACCON-2P22 / ACCON-2P41 / ACCON-2P42 / ACCON-2P81 • Supports up to 100,000 NFC cards & up to 150,000 events • Supports high frequency 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 & 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) & 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 Reader ACRDR-2SC • Gain access via RFID card • Connect and configure with PC via ethernet cable • RS485 protocol • Tamper switch triggers loud alarm, deterring removal • Blue backlight for low light visibility • IP65 weather rated for outdoor use	
Touch Keypad + RFID Card Reader ACENR-2SKC • Gain access via RFID card and keycode • Connect and configure with PC via ethernet cable • RS485 and Wiegand 26/34 protocol • Tamper switch triggers loud alarm, deterring removal • Blue backlight for low light visibility • IP65 weather rated for outdoor use	
Large Touch Keypad + RFID Card Reader ACRDR-2LKC • Gain access via RFID card and keycode • Connect and configure with PC via ethernet cable • RS485 and Wiegand 26/34 protocol • Tamper switch triggers loud alarm, deterring removal • Blue backlight for low light visibility • IP55 weather rated for outdoor use	

Component	Image
Vandal-Proof Keypad + RFID Card Reader ACRDR-2MKC • 12 button keys (0-9, *, #) • Connect and configure with PC via ethernet cable • RS485 and Wiegand 26/34 protocol • Tamper switch triggers loud alarm, deterring removal • Blue backlight for low light visibility • IP55 rated weather resistance • IK08 rated for vandal resistance	
Fingerprint + RFID Card Reader ACRDR-2SFC • Stores and recognises up to 3000 fingerprints • Gain access via RFID or fingerprint scan • Connect and configure with PC via ethernet cable • RS485 and Wiegand 26/34 protocol • Tamper switch triggers loud alarm, deterring removal • Blue backlight for low light visibility • Indoor use only	
RFID Card Reader ACRDR-2PC • Gain access via RFID card • Connect and configure with PC via ethernet cable • RS485 protocol • Compact, textured design • Tamper switch triggers loud alarm, deterring removal • Blue backlight for low light visibility • IP67 weather rated for outdoor use	
USB Card/Tag Enroller ACENR-2C • Required for all VIP Vision Access Control Readers • Connects to SmartPSS & powered via USB port • Support IC card (Mifare card) at 13.56MHz frequency • Confirms card registration with LED light & beep	
USB Fingerprint Enroller ACENR-2F • Required for the ACRDR-2SFC • Connects to SmartPSS & powered via USB port • Recognises dry or wet fingerprints	

1.4 Access Control Accessories Range

Component	Image
Heavy Duty Door Release Button 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 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 ACDSW102 • 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	
13.56MHz NFC Thin Proximity Cards ACKEY103 • High Frequency 13.56MHz • Mifare IK S50 IC Chip • 1024 bits memory • 0.8mm card thickness	
13.56MHz NFC Proximity Keyfobs ACKEY104 • High Frequency 13.56MHz • Read-only memory • NTAG215 • 28 x 35 x 6.2mm	

Electric Door Strikes

VIP Vision has a variety of solid, high security electronic door strikes and magnetic locks to accompany your access control systems.

Our range of electronic door strikes feature tough, steel and stainless steel, convertible fail-safe/fail-secure, multi-voltage, and door/lock monitored models.

1.5 Access Controller Dimensions

ACCON-2P22/2P42/2P41/2P81
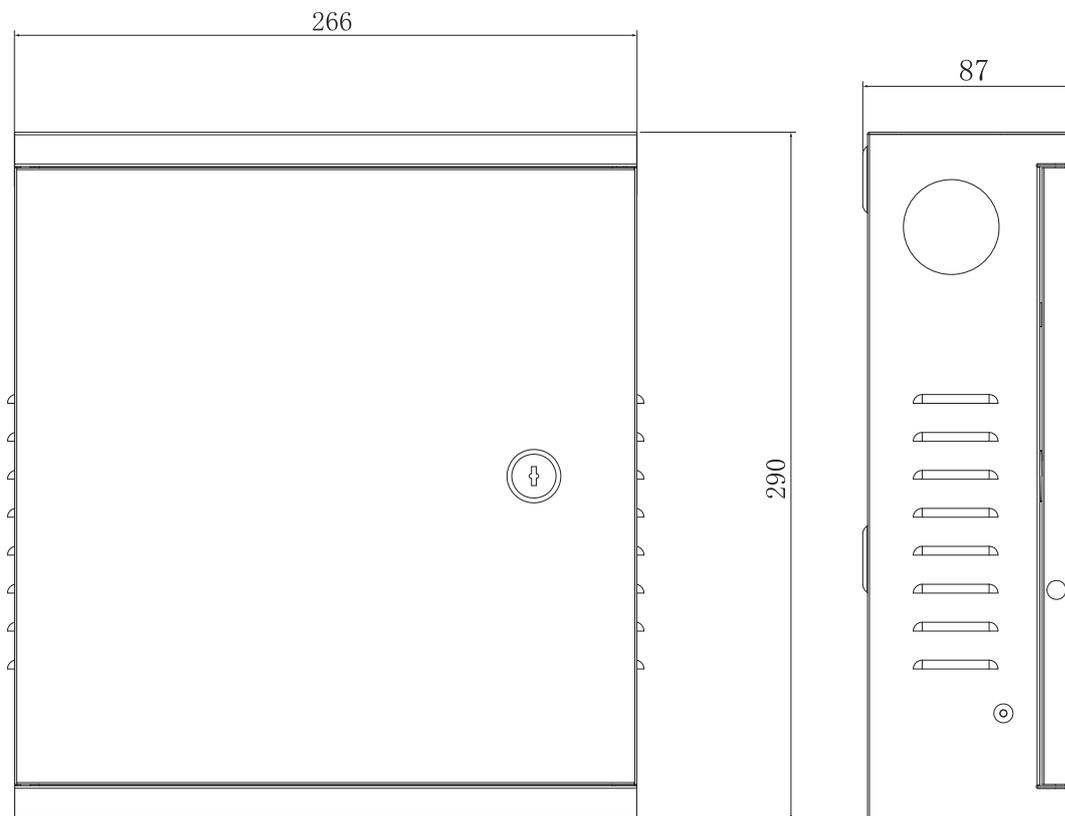
ACCON-2C41
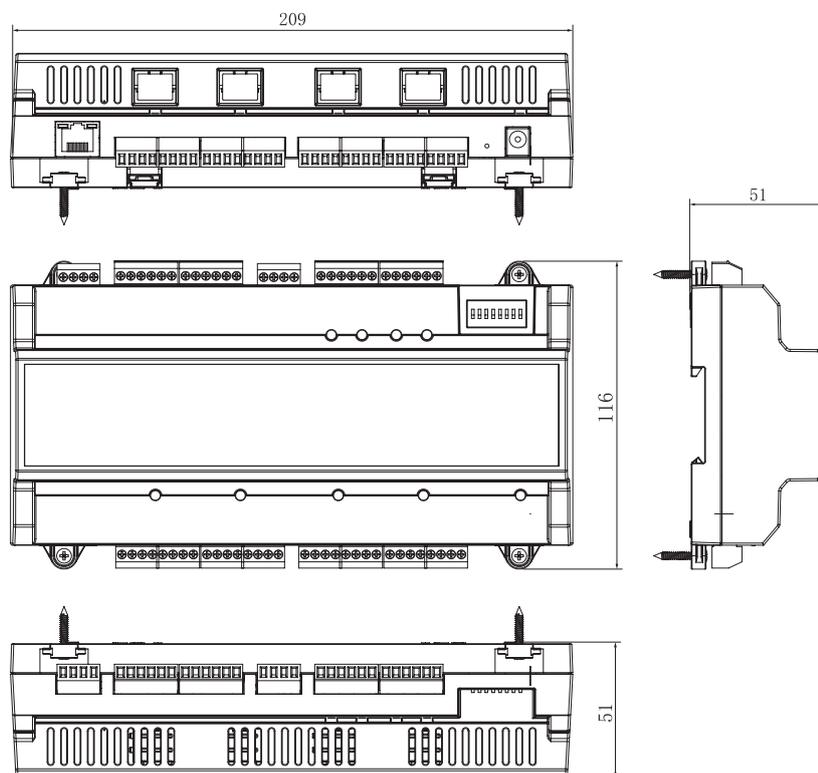
2. Access Controller Installation

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

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

Communication between access controllers, keypads and card readers requires CAT5e/CAT6 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.

Labelling all cables clearly will reduce troubleshooting time. Check wiring before power up.

2.1 System Diagram

PC with Smart PSS

Card & Fingerprint Enrollers

TCP/IP Network

Access Controller
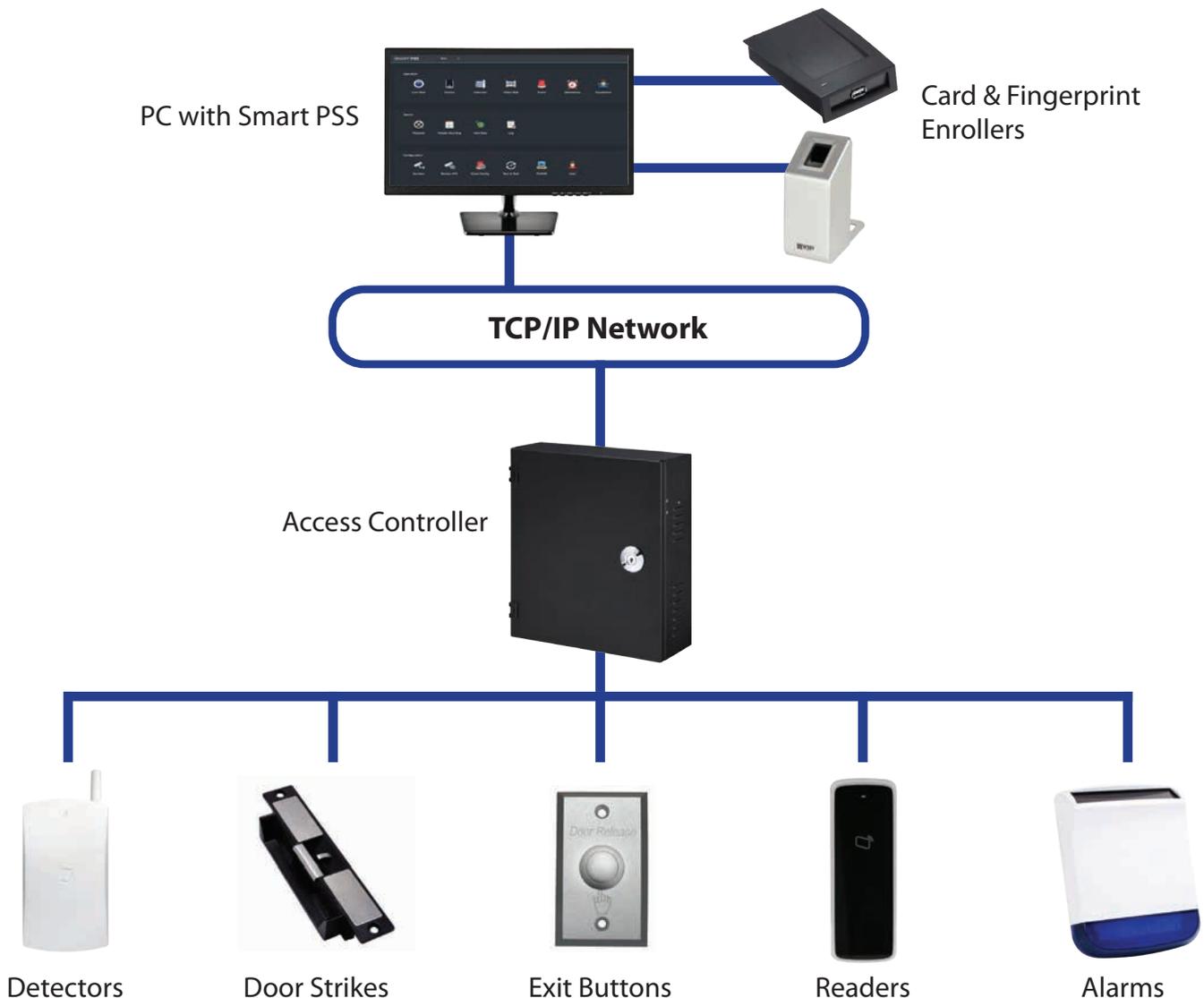
Detectors   Door Strikes   Exit Buttons   Readers   Alarms

ACCON-2C41
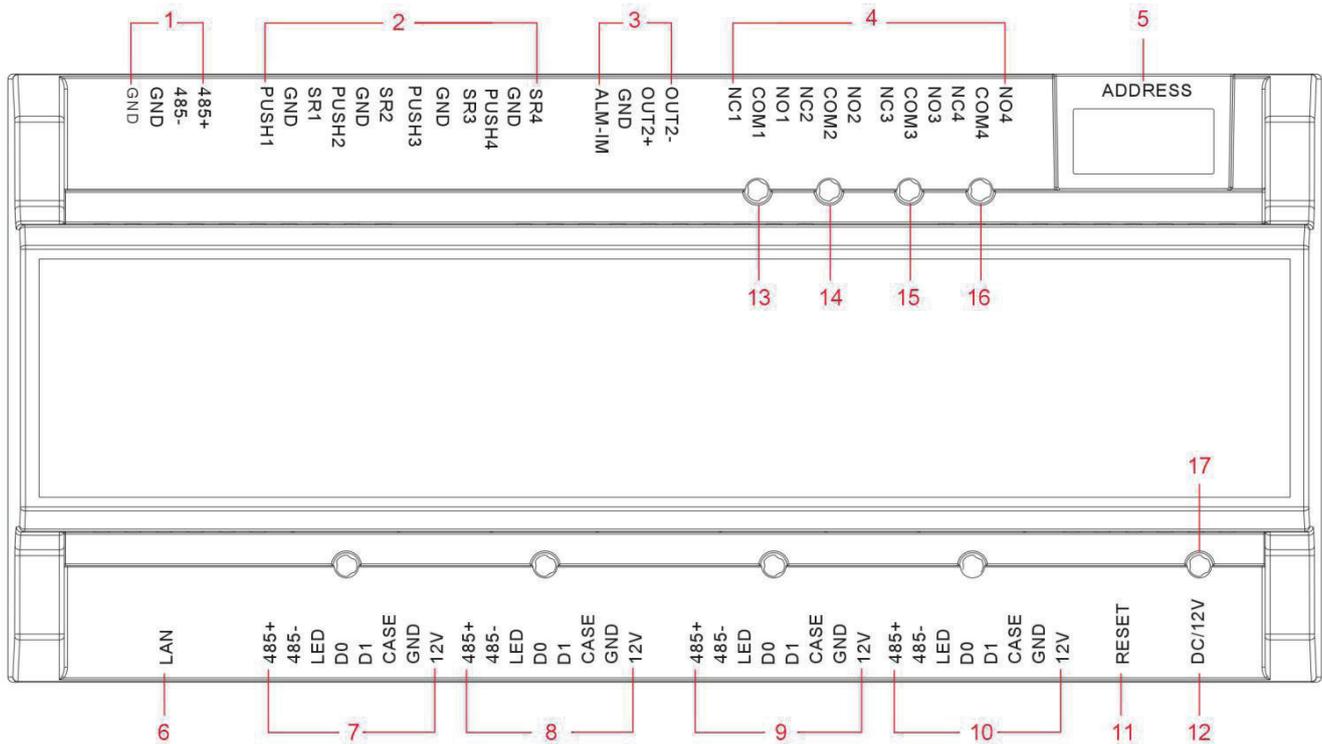
Port No.	Image	Port No.	Image
1	RS485 communication port	8	Card/fingerprint reader/keypad 2
2	Door 1 - 4 push button inputs (PB1,PB2,PB3,PB4) Door 1 - 4 sensor inputs (SR1,SR2,SR3,SR4)	9	Card/fingerprint reader/keypad 3
3	No.3, 4 doors unlock +door sensor	10	Card/fingerprint reader/keypad 4
4	External alarm input (ALM-IN) /output External alarm output (OUT2+,OUT2-)	11	Reset Button
5	DIP Switch - Use for reset to factory default settings	12	12V DC input (1A)
6	Network cable input (RJ-45)	13-16	Door lock/unlock indicators
7	Card/fingerprint reader/keypad 1	17	Power indicator

ACCON-2P41

ACCON-2P42

ACCON-2P81

Exit Reader of Door 4 — Wiegand Reader — CASE, LED, D1, D0
Entry Reader of Door 4 — Wiegand Reader — CASE, LED, D1, D0
Exit Reader of Door 3 — Wiegand Reader — CASE, LED, D1, D0
Entry Reader of Door 3 — Wiegand Reader — CASE, LED, D1, D0
Exit Reader of Door 4 — 485 Reader — 485+, 485-
Entry Reader of Door 4 — 485 Reader — 485+, 485-
Exit Reader of Door 3 — 485 Reader — 485+, 485-
Entry Reader of Door 3 — 485 Reader — 485+, 485-
Power Supply of Reader — GND, 12V, 12V

NOT USED — SPK+, SPK-
Extension Modules — 485+, 485-, GND, 485+, 485-, GND

External Alarm Outputs:
ALARM1/ALARM2 triggers alarm — OUT1+, OUT1-
ALARM3/ALARM4 triggers alarm — OUT2+, OUT2-
ALARM5/ALARM6 triggers alarm — OUT3+, OUT3-
ALARM7/ALARM8 triggers alarm — OUT4+, OUT4-

Lock/Unlock Control Outputs:
Door 1 — NO/NC1, COM1
Door 2 — NO/NC2, COM2
Door 3 — NO/NC3, COM3
Door 4 — NO/NC4, COM4
Door 5 — NO/NC5, COM5
Door 6 — NO/NC6, COM6
Door 7 — NO/NC7, COM7
Door 8 — NO/NC8, COM8

4-ch Alarm Input:
ALARM1, ALARM2, GND, ALARM3, ALARM4, GND
Door Contact of Door 5 — SR5
Door Contact of Door 6 — SR6, GND
Door Contact of Door 7 — SR7
Door Contact of Door 8 — SR8, GND

Ext. Alarm Output Relays — JK4 JK3 JK2 JK1
DIP Switch

Door Lock/Unlock Control:
J35 — ON/NC — JK5
J37 — ON/NC — JK6
J39 — ON/NC — JK7
J41 — ON/NC — JK8
J18 — ON/NC — JK9
J22 — ON/NC — JK10
J20 — ON/NC — JK11
J24 — ON/NC — JK12

Restart Button

Tamper Switch

Wiegand Reader — CASE, LED, D1, D0 — Exit Reader of Door 2
Wiegand Reader — CASE, LED, D1, D0 — Entry Reader of Door 2
Wiegand Reader — CASE, LED, D1, D0 — Exit Reader of Door 1
Wiegand Reader — CASE, LED, D1, D0 — Entry Reader of Door 1
485 Reader — 485-, 485+ — Exit Reader of Door 2
485 Reader — 485-, 485+ — Entry Reader of Door 2
485 Reader — 485-, 485+ — Exit Reader of Door 1
485 Reader — 485-, 485+ — Entry Reader of Door 1
Power Supply of Reader — GND, GND, 12V, 12V

Battery — +, -
Charge Port — +, -
Power Port DC12V — +, -

NET — LAN Cable — PC

Extended Module

Door Push Buttons — PUSH1, GND, PUSH2, PUSH3, GND, PUSH4 — Door 1 Exit Button, Door 2 Exit Button, Door 3 Exit Button, Door 4 Exit Button
Door open/close Sensors — SR1, GND, SR2, SR3, GND, SR4 — Door Contact of Door 1, Door Contact of Door 2, Door Contact of Door 3, Door Contact of Door 4
Door Lock Sensors — PUSH, GND, PUSH, PUSH, GND, PUSH — Door 5 Exit Button, Door 6 Exit Button, Door 7 Exit Button, Door 8 Exit Button

2.3 Installation

2.3.1 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.

Port No.	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
JK39		
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		

2.3.2 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).
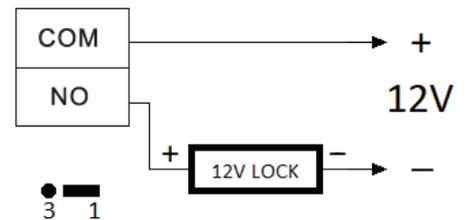
b) Fail Safe type door lock connection - Remove power to unlock.

Typical Fail Secure type door lock: Electromagnetic locks, drop bolts (fail safe type).
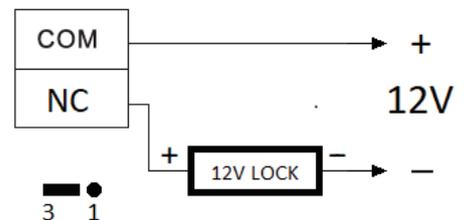
It is strongly recommended to use separate power supply for door locks if more than 4 locks are installed.

2.3.3 Connect 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 also **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).

ACCON-2C41
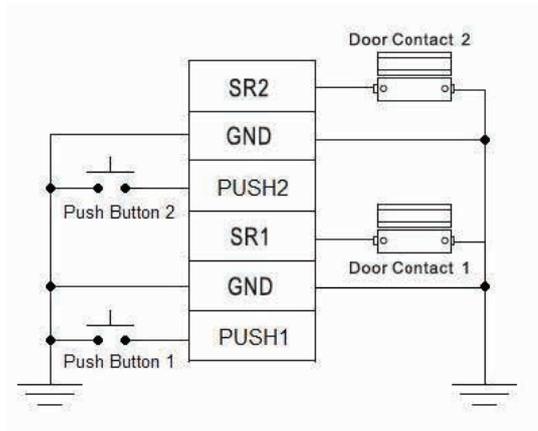
ACCON-2P22
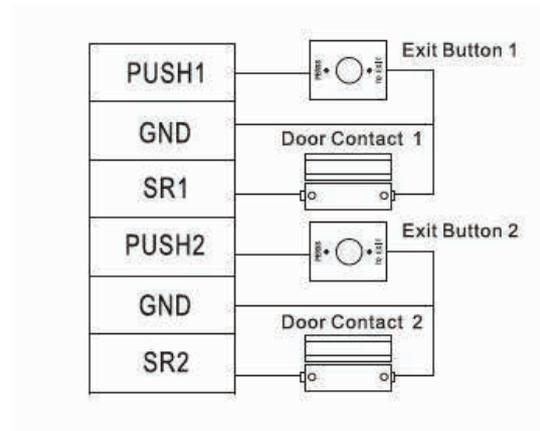
ACCON-2P41
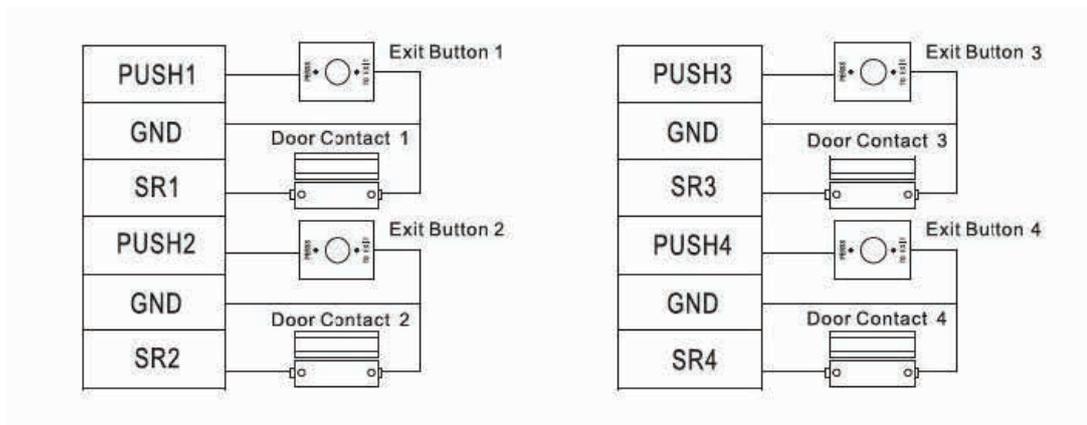
ACCON-2P42/2P81
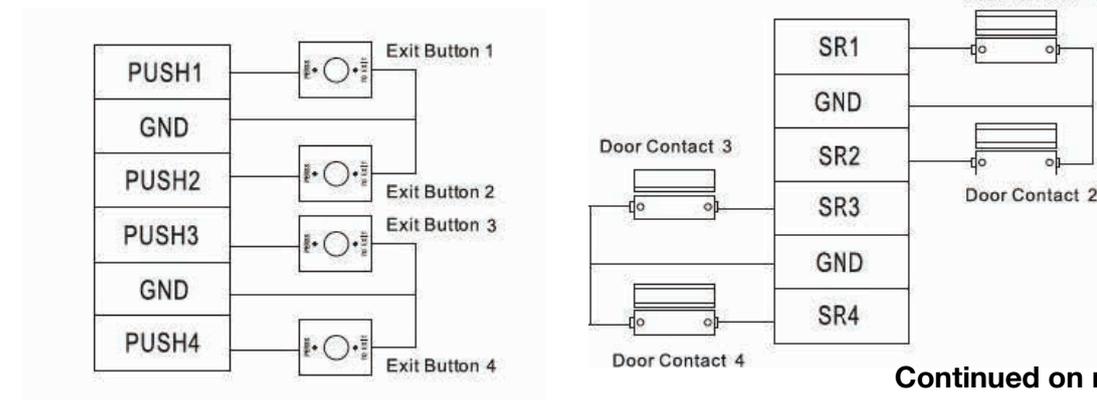
Continued on next page ⟶

ACCON-2P81 ONLY
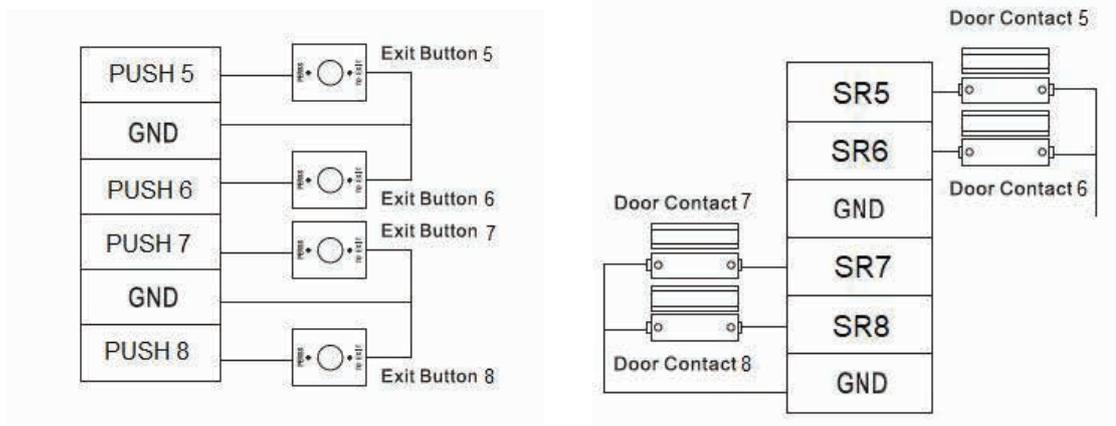
2.3.4 Connecting Card Readers, Fingerprint Readers and Keypads

You can choose to connect either a 485 bus or Wiegand bus. VIP Vision access control panels and readers support both formats. **Note:** *Must use 485 bus for Fingerprint readers. 485 and Wiegand readers connected via CAT5e/CAT6 cable up to 100.*

a) If 485 readers are used:

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

b) If Wiegand readers are used:

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

2.3.5 Connect External Alarm Inputs (optional)

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

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

Note: 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.

*Due to this, connecting ALARM1 is **not recommended if a high security level is required**.*

2.3.6 Connect External Alarm Outputs (optional)

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

The following tables are for **2P42 and 2P81 ONLY**

ACCON-2P42

For 2P42, two External Alarm inputs share one set of External Alarm 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		

ACCON-2P81

For 2P8, each External Alarm input has one External Alarm 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)
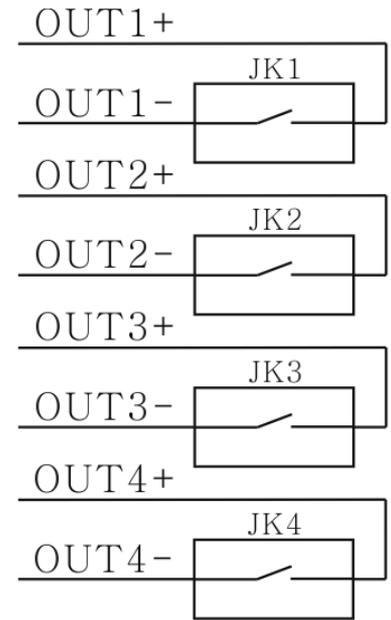
2.3.7 Connect Power Cable (2P Series) / DC Power Adaptor (2C Series)

For **2P Series**, connect the power cable located at the bottom left hand corner of the metal case.
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 while powering up. The beep sound may last for 15 seconds when power is applied for the first time.

2.3.8 Connect Network Cable

Connect a CAT5e/CAT6 LAN cable in the NET connector of the access controller panel. Connect the other side of the cable to the network port of a PC.

2.3.9 Connect Backup Battery (2P Series Only)

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

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

Be careful with the polarity of the battery; an incorrect connection will result in system damage.
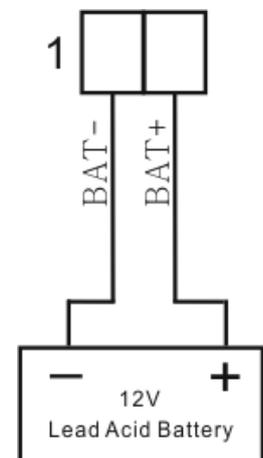
3. Configuration via Smart PSS
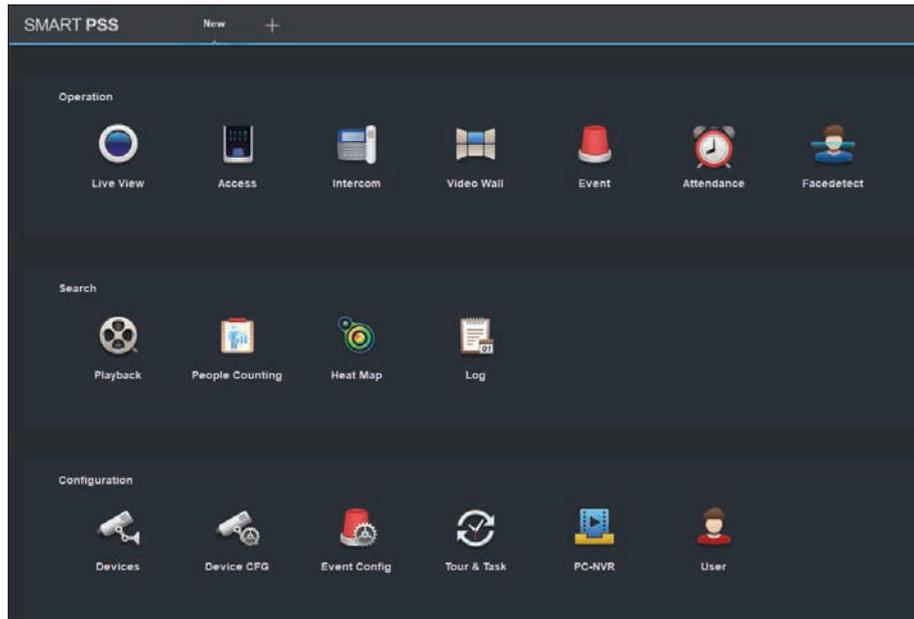
Smart PSS is an all-in-one, full-featured application for configuring access control systems, surveillance cameras, network video recorders, video walls and intercom systems. The software provides efficient device management and is user friendly.

3.1 Security Recommendations

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, it would be easy for the culprit to guess these passwords for 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 locked to prevent any unauthorised 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 requires in order to function properly.

3.2 Smart PSS Installation

3.2.1 Install the Smart PSS Software

Download the latest version of Smart PSS from the VIP Vision website at: **www.vip-vision.com/support/downloads**

Must check the "accept agreement" box.
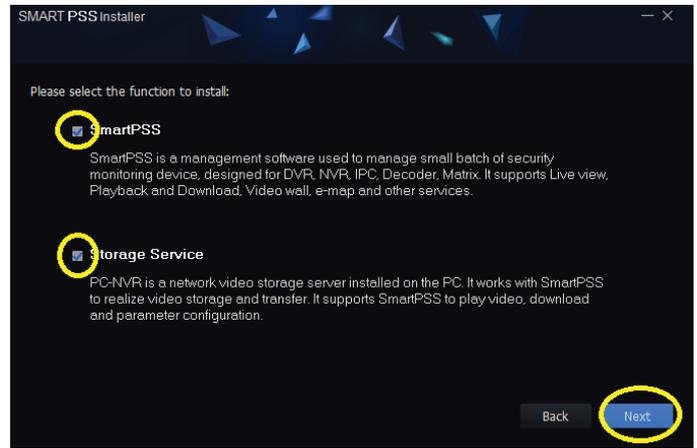
Check both boxes for complete software installation.
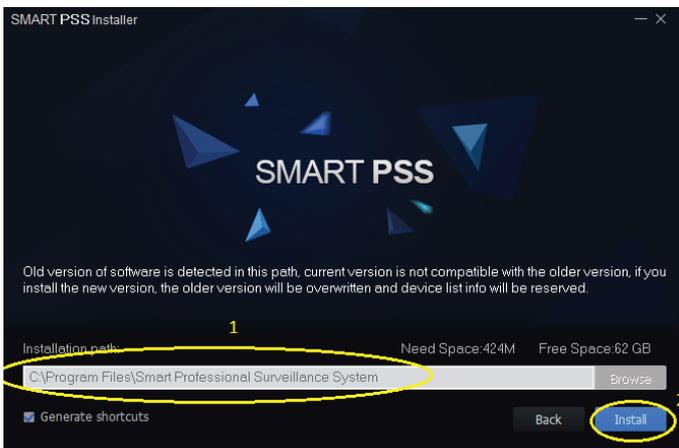
Change the installation folder if necessary and click "Next".
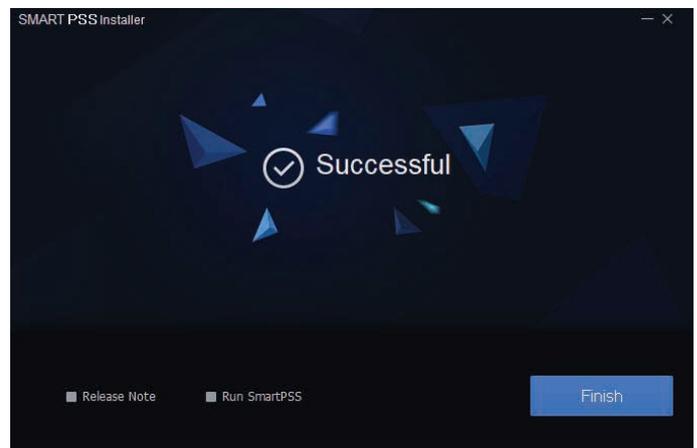
Wait until "Successful" is shown on the screen. Check "Run SmartPSS" and click "Finish" to launch.

3.2 Smart PSS Installation (continued)

3.2.2 Set Password for Smart PSS

When the program launches for the first time, it will begin Initialisation and prompt the user to set a password. Enter a password, then check "Auto Login after Registration" and click "Next".
Note: The password must be 8 digits with and contain both numbers and letters.

Next, you will be required to set security questions to be used for password resets. Set three security questions that you will remember the answers to, and click "Finish".
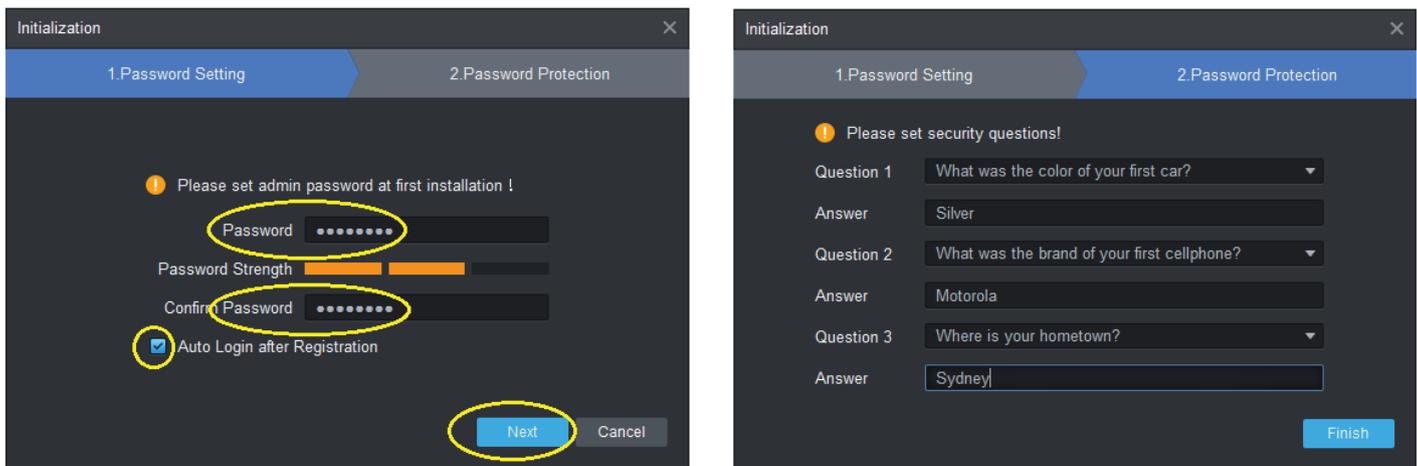
3.2.3 Configure the PC Network Card (Ethernet Card)

The default IP address of the 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. We recommend setting **xx** to a larger number to reduce the possibility of conflicting with other devices.
In this example, we'll set the IP of the network card to **192.168.0.199**

1. Press the **Windows key + R** to open Run. Type "ncpa.cpl" and click "OK" to access Network Communications.
2. Right click on the Ethernet icon and click Properties.
3. Double click the item "Internet Protocol Version 4 (TCP/IPv4)"
4. Select "Use the following IP address" and enter:
    IP address: **192.168.0.199**
    Subnet mask: **255.255.255.0**
5. Click "OK" to confirm.
6. Click "OK" again to finish.

3.2.4 Add the Access Controller to Smart PSS

1. Open Smart PSS and log in.
2. The program will open to the Devices menu. Click the "+ Add" button.
3. In Manual Add, enter:
   IP\Domain Name: **192.168.0.2**
   User Name: **admin** (default)
   Password: **123456** (default)
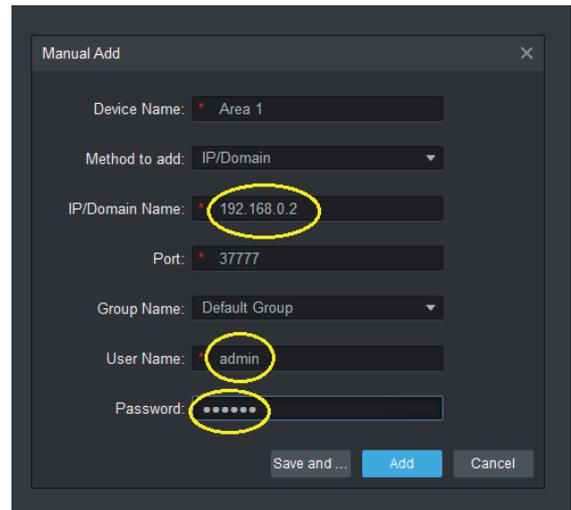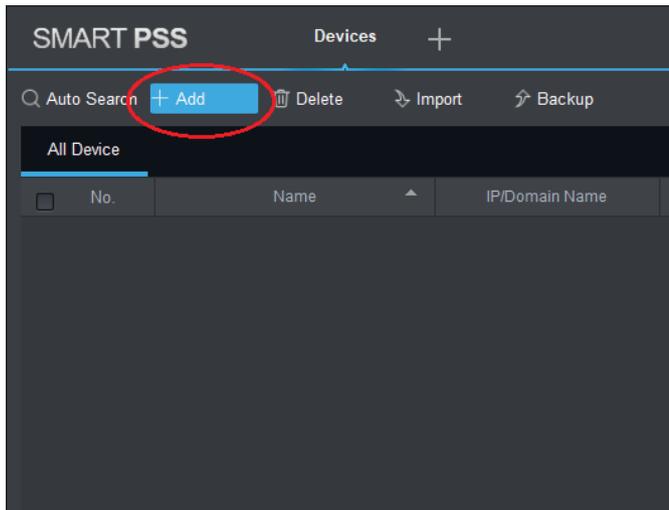
4. If the device is successfully added, you can see the device type and a green circle indicating the online status.

3.2.5 Synchronise Time with PC

It is important that you synchronise the time/date of the access controller with the PC. Otherwise, the access controller's clock may not match up with the actual time.

1. 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 Menu.
2. Click the Device CFG icon to enter the Device Configuration menu.
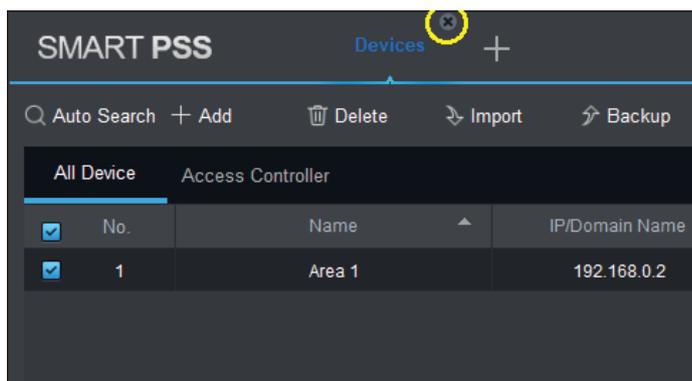
3. Click the access controller name defined earlier.
4. Click "System" and then "General".
5. Select the correct time zone and click "Sync PC" to synchronize the time with PC. After that, click "Save" to finish synchronizing the time with PC.
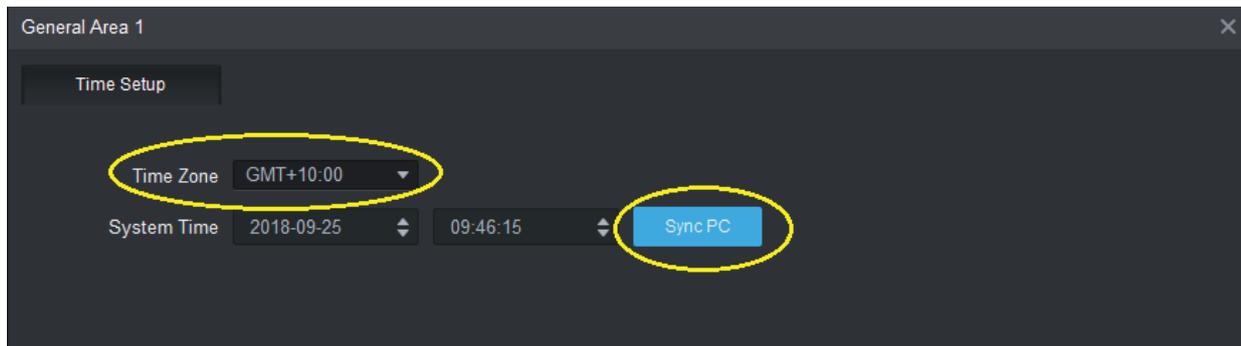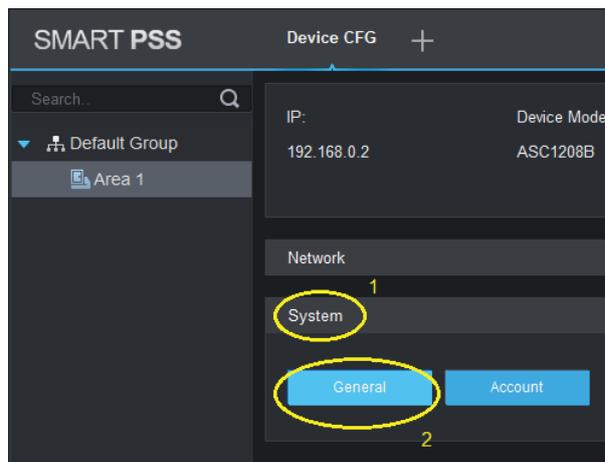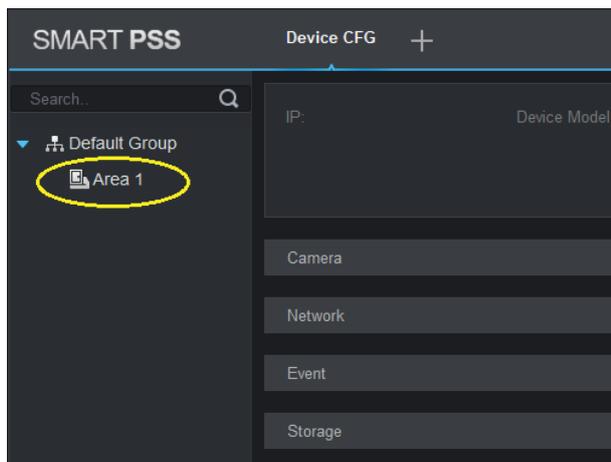
3.2.6 Add Users

1. From the Main Menu, click the "Access" icon to enter the Access Controller menu.
2. 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.
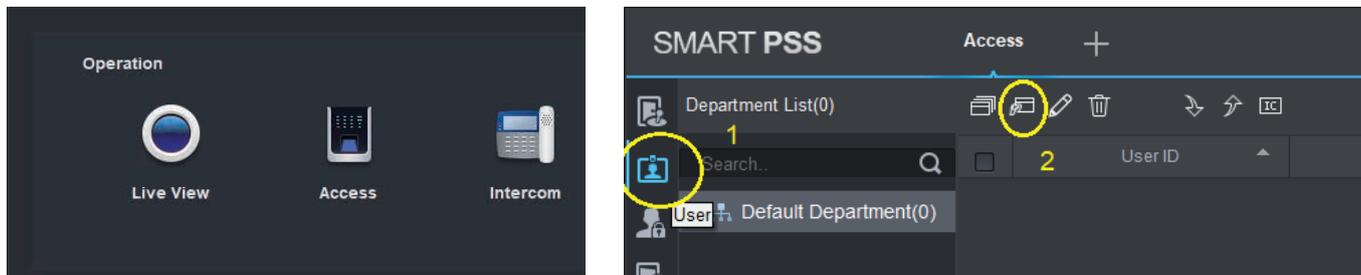
3. Enter all user information in the box.

   User ID: Maximum 10 digits with no leading zero

   Name: Name of the user

   Card No.: Put a IC card on the USB enroller, 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: Not applicable

   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 using the Remote Verification function. Refer to 3.3.5 Remote Verification for more.*

You can now press "Finish" to add the user, or continue on to **3.2.7 Add Fingerprints** to add the user's fingerprints.

3.2.7 Add Fingerprints (optional)

Continuing from **3.2.6 Add the Access Controller to Smart PSS**:

1. Plug the USB Fingerprint Enronner to the PC USB port.
2. In the Add User menu, click the Fingerprint info tab.
3. Make sure "USB Fingerprint Reader" is selected in the Fingerprint Device section.
4. Place the user's finger on the fingerprint reader and click the "Collect" button. For the most accuracy, ensure that the scanned finger is clean and not too dry or wet. When the blue fingerprint icon on the left appears, it means the scan is complete.
5. For accuracy, the reader needs to scan 3 times. Repeat until the process is complete, then press "Finish".
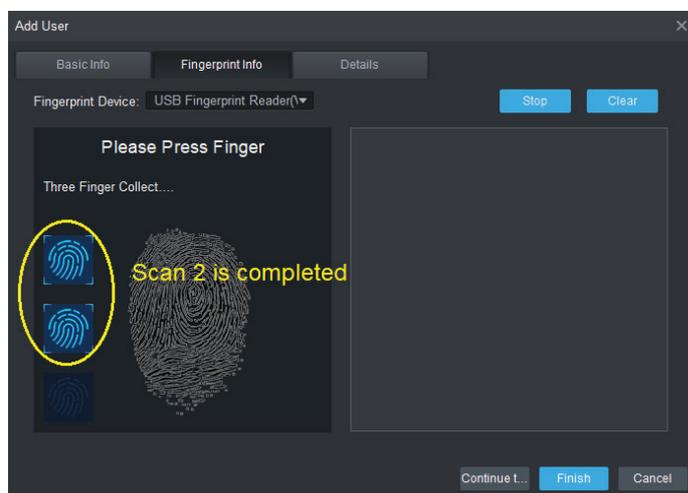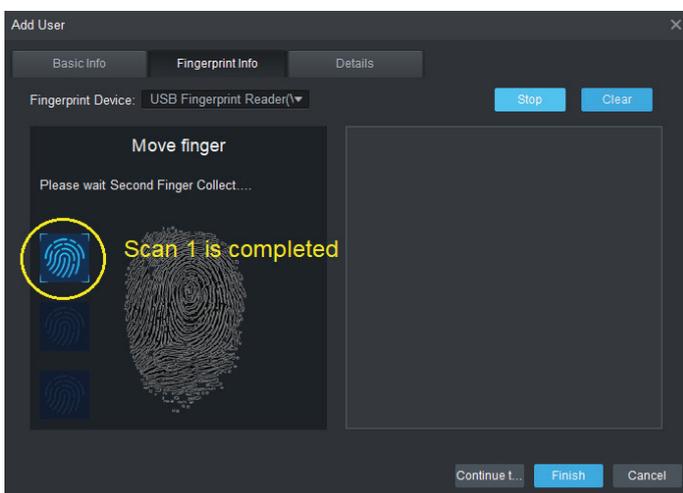
You will now see the user(s) added on the User Screen.
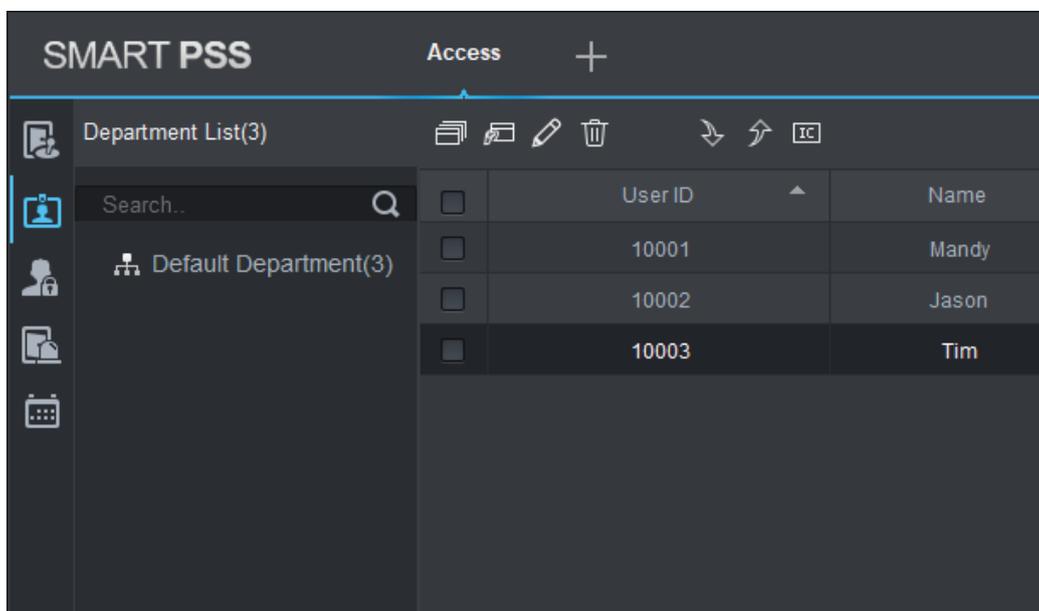
3.2.8 Set Door Groups

1. From the Access Controller menu, click the "Upload User to Device" icon and then "Access Level" to enter the Access Level screen.

2. Click the "Add" button.
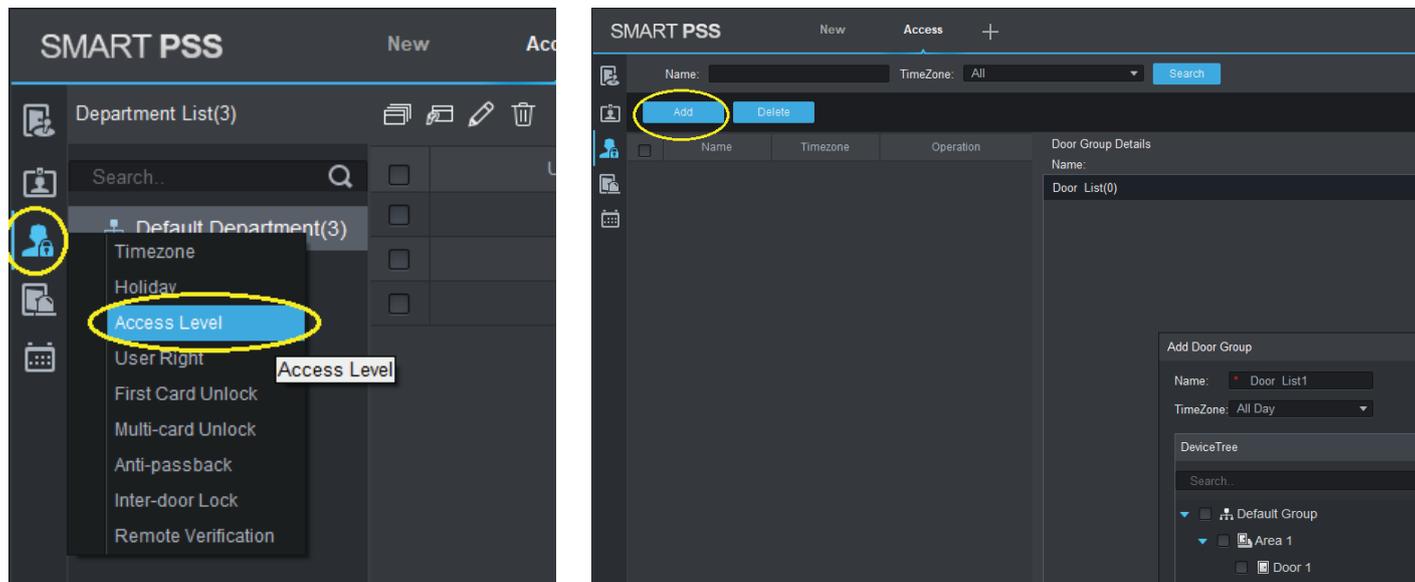
3. Enter the name for the Door group, the time zone and the doors that the users belonging to this group can gain access to.

    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.
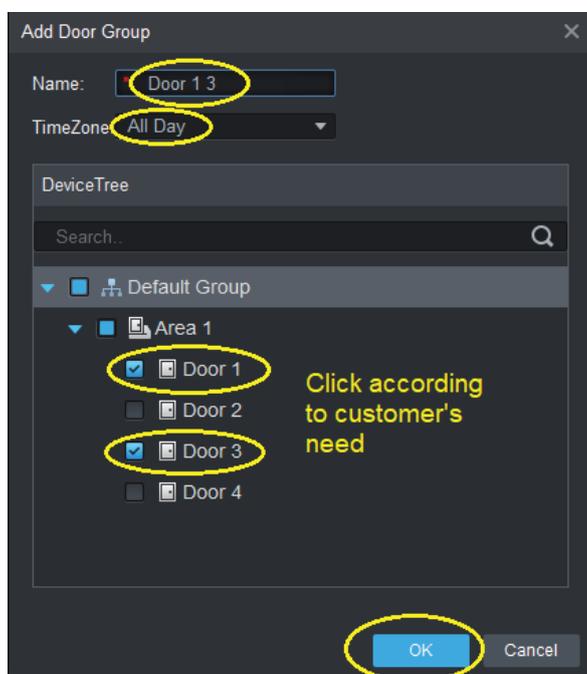
4. Repeat this process until every required door group is created.

3.2.9 Set Time Schedules

1. From the Access Controller menu, click the "Upload User to Device" icon and then "Timezone" to enter the Time Zone Setup screen.
2. Click the "Add" button, then enter the name of the time schedule. Press the Settings button on the right to set the time schedule.
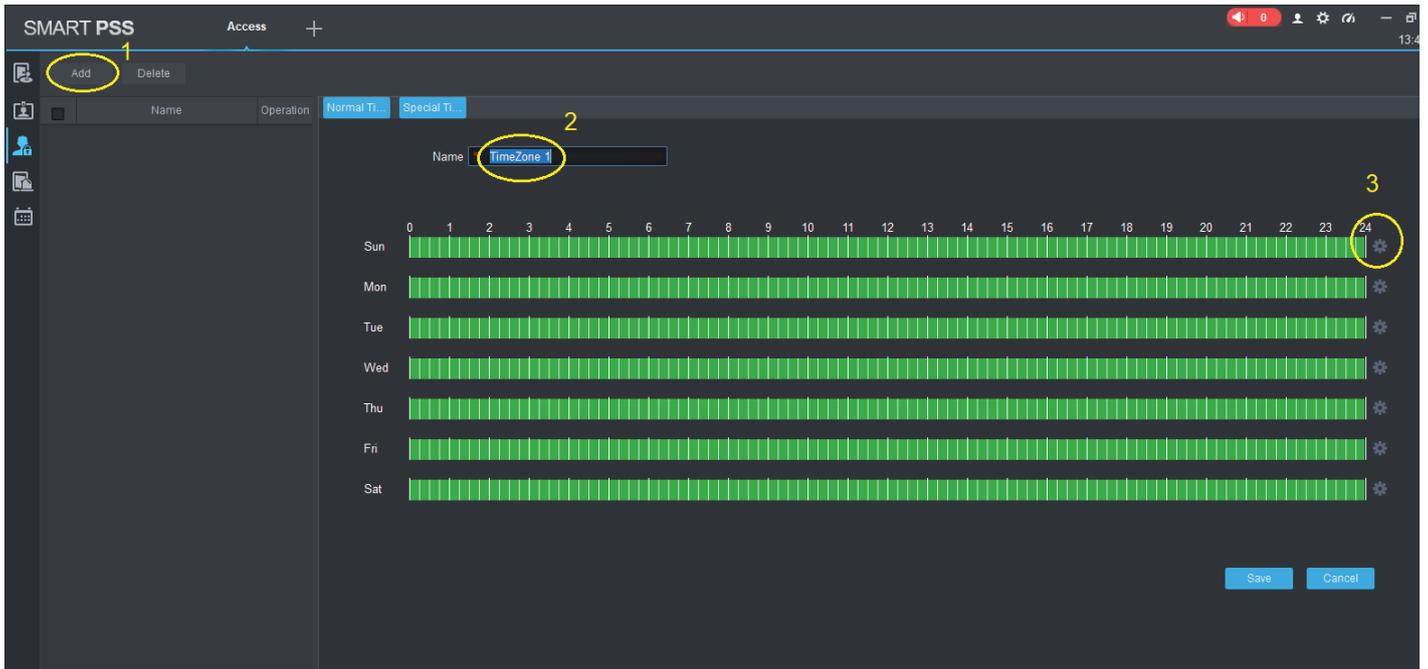
3. Set the time(s) and the days(s) of week when the doors are allowed to be accessed.
4. Press "OK" when done.
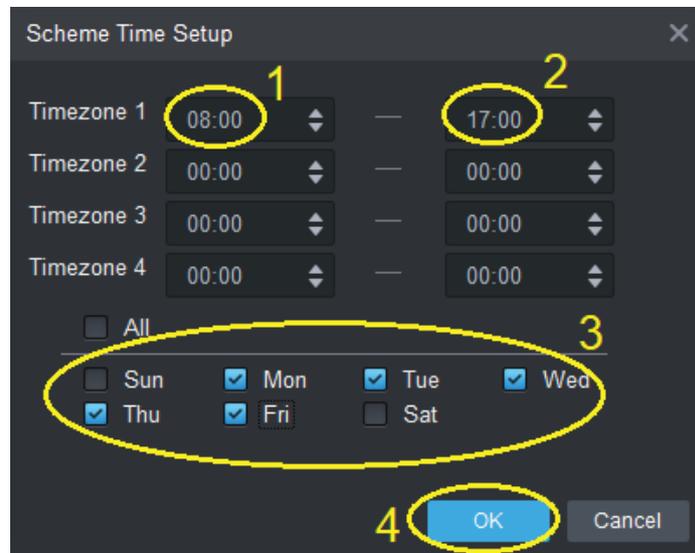
5. Press "Save" to finish.

3.2.10 Set Holiday Schedules

1. From the Access Controller menu, click the "Upload User to Device" icon and then "Holiday" to enter the Holiday Schedule Setup screen.

2. Click "Add", then enter the name of the holiday schedule. Select the date and click "Save" when finished.
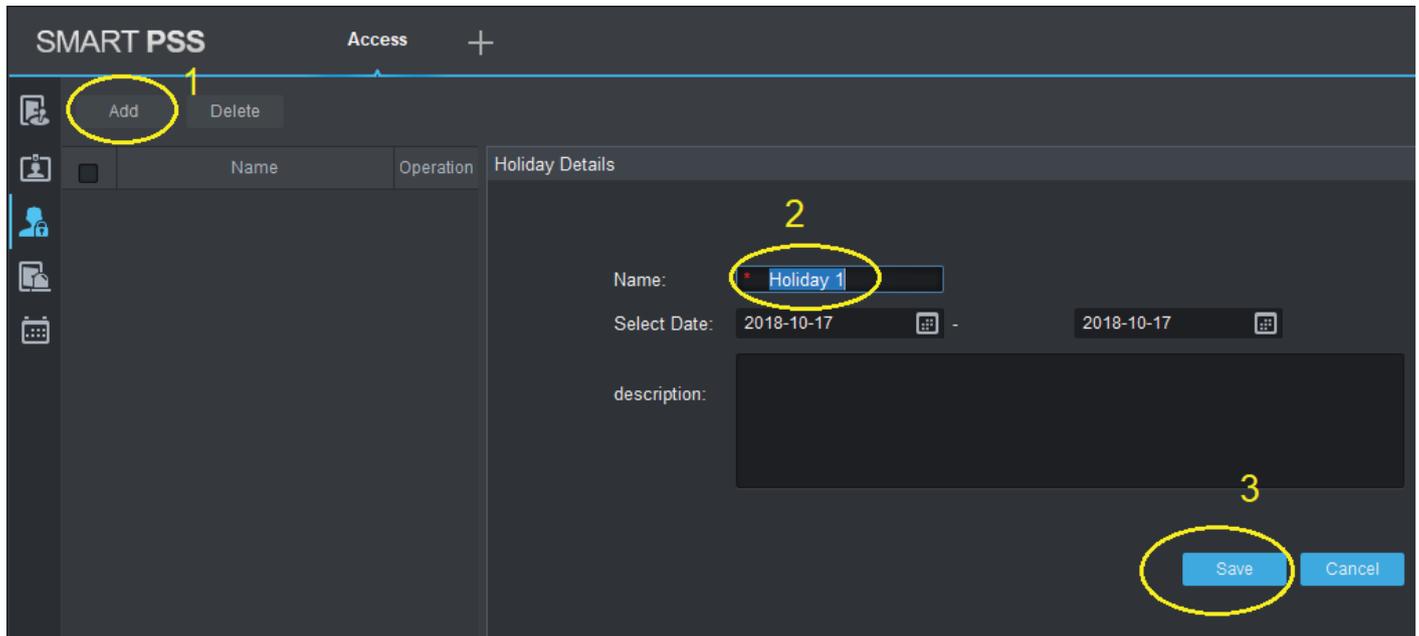
3. Set the holiday time schedule to restrict the time when users can get access.
    In this example, authorized users can get access at 08:00-10:00 during holiday.
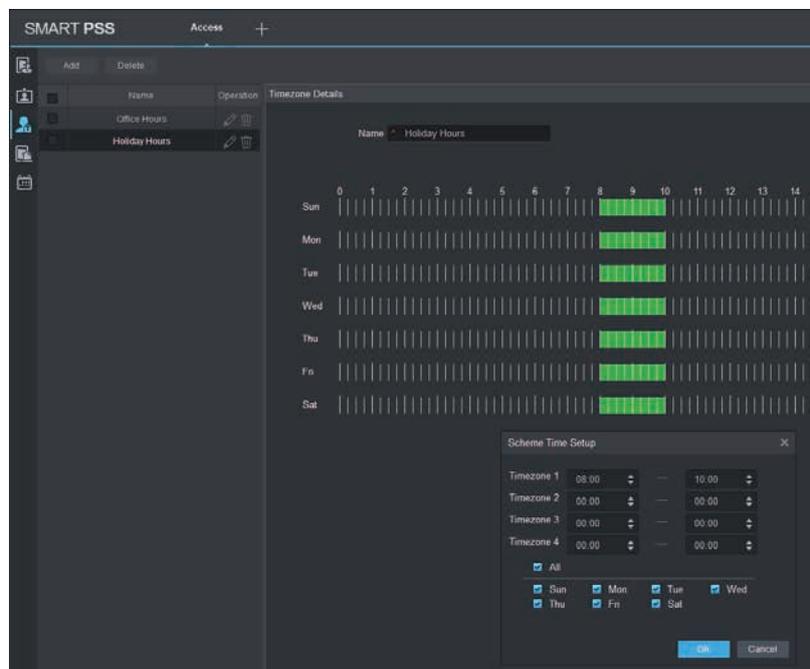
Continued on next page ⟶

3.2.10 Set Holiday Schedules (continued)

4. Select which doors to restrict access to through "Door Configuration".
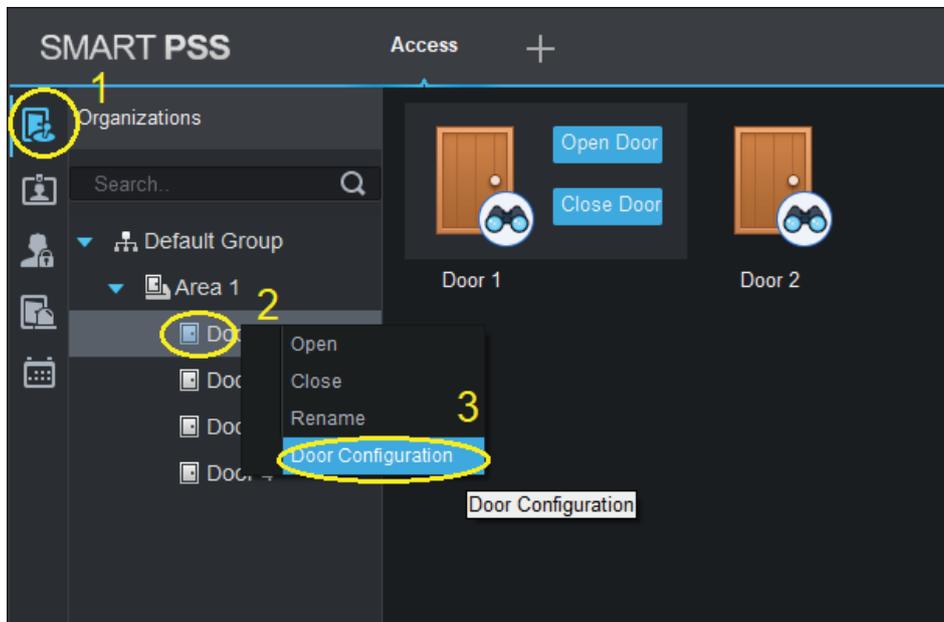
4. Select the Holiday Timezone, then click "OK" when done.
    In this example, on 2018-10-17 (Holiday), users can get access between 08:00-10:00 at Door 1 only.
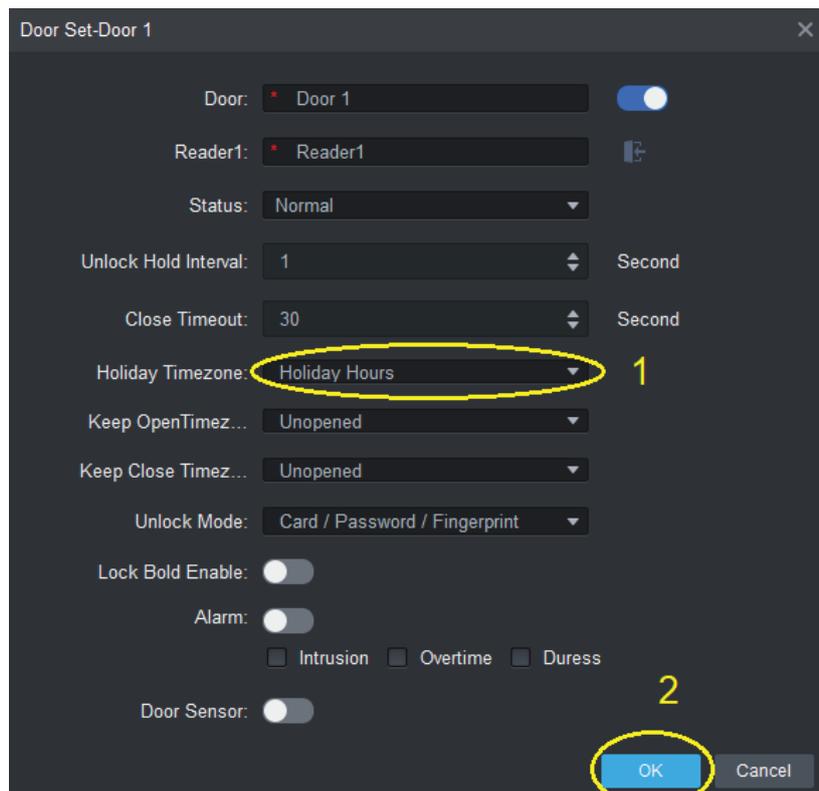
3.2.11 Assign User Access Levels

1. From the Access Controller menu, click the "Upload User to Device" icon and then "Access Level" to enter the Access Level screen.
2. Click the "Add User" icon.
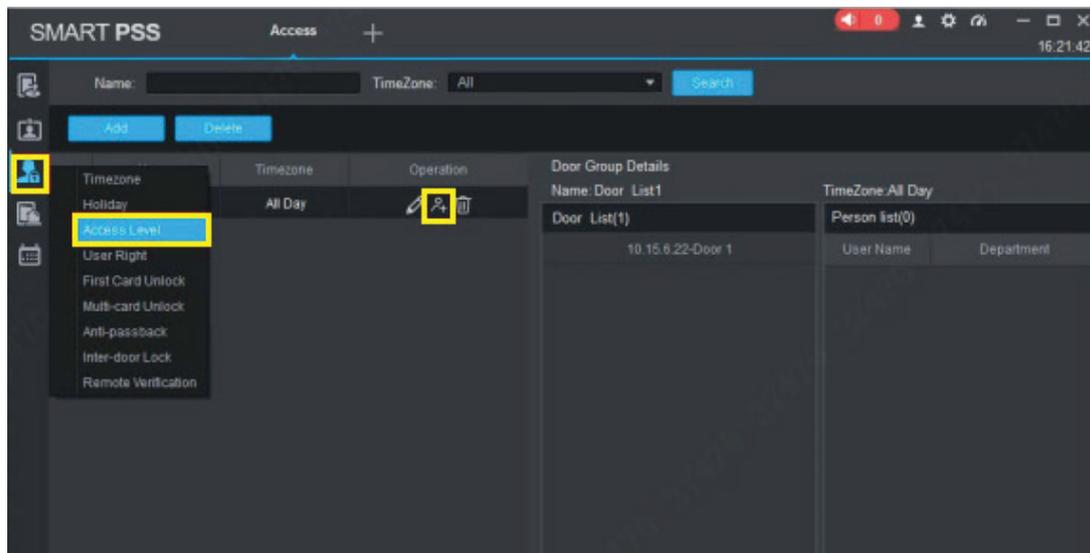
3. When the "User Select" dialog box pops up, select the user's department from the drop down list and click OR enter the user's ID or name directly. You may also click the magnifier icon to list all users.
4. Select the users to be assigned to this door group, then click the "OK" button.

   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.
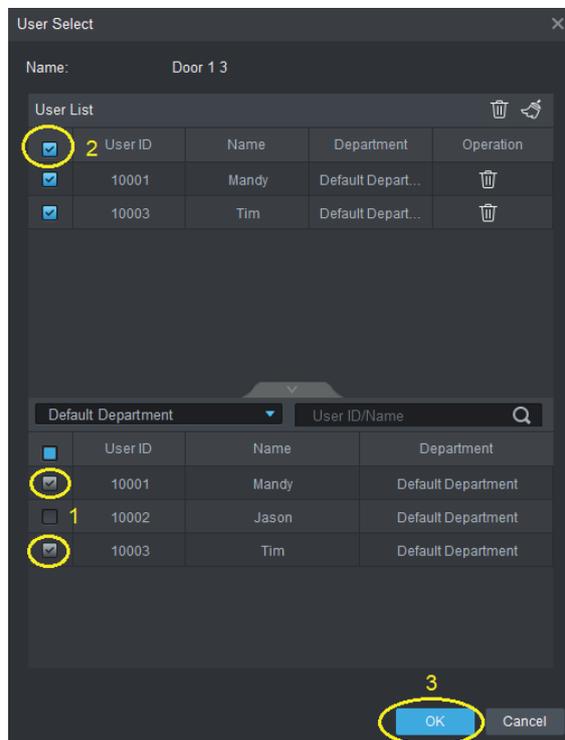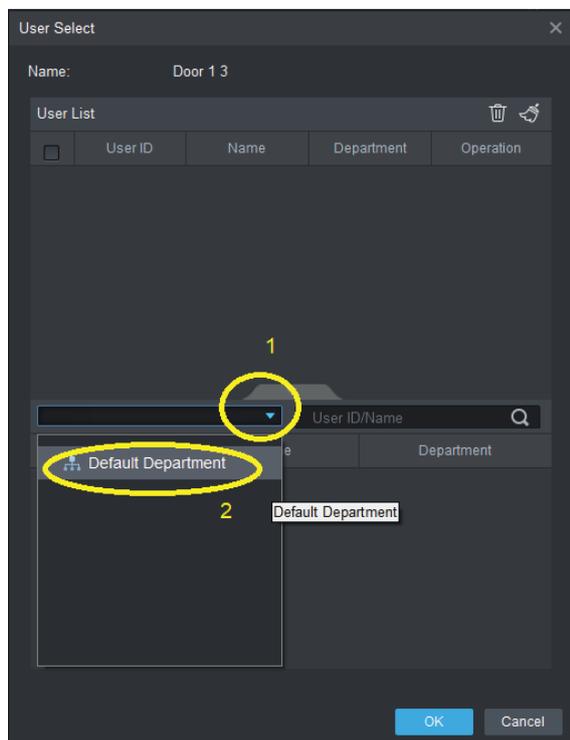
3.2.12 Configure Doors

1. Click the Console icon.
2. Choose the door to be configured by right clicking the door name and clicking Door Configuration.
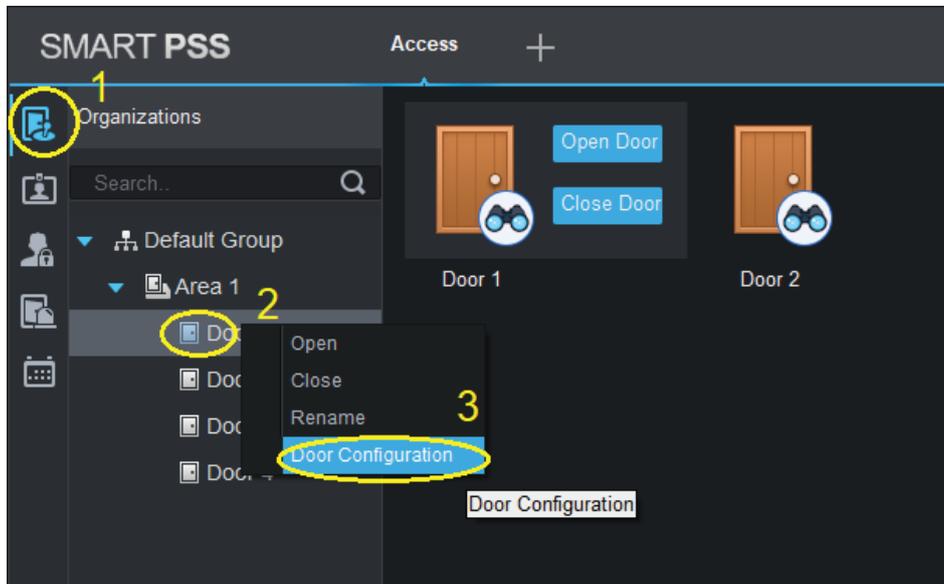
3. Enter all user information in the box.

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 unlocked.

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.
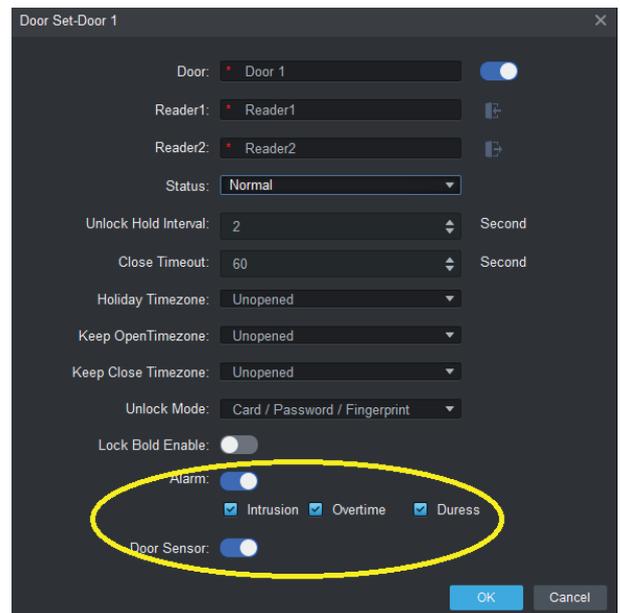
If the alarm is triggered, the Access Control console will display the alarm event time and change the icon on the door.
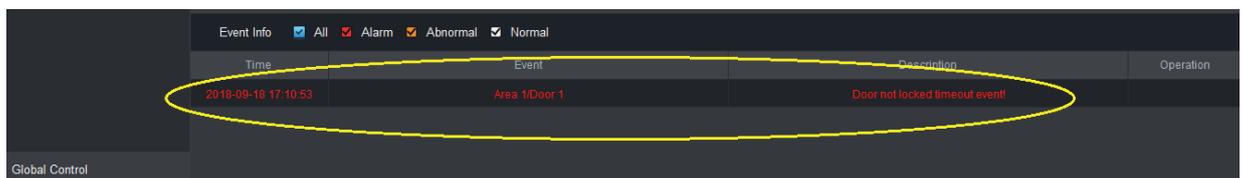
3.2.13 Log Records and Log Files

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

1. Click the "Log" icon on the side menu then click the "Export" button. A dialog box will be shown.
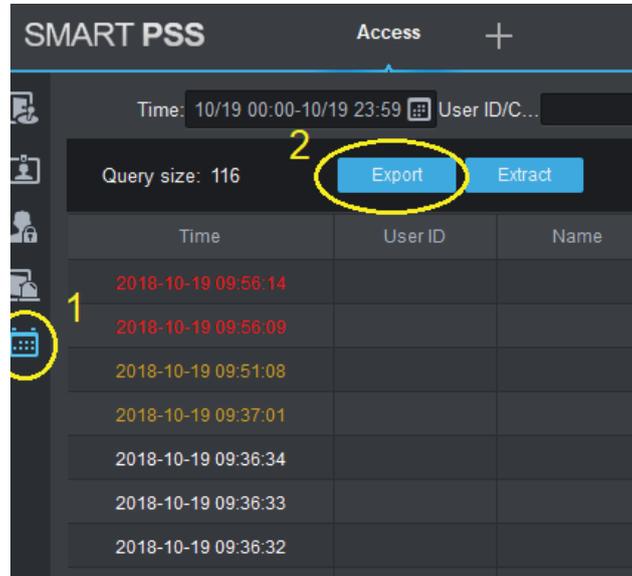
2. Choose the folder and the name of the log file and click "Save". The file format is Microsoft Excel compatible.
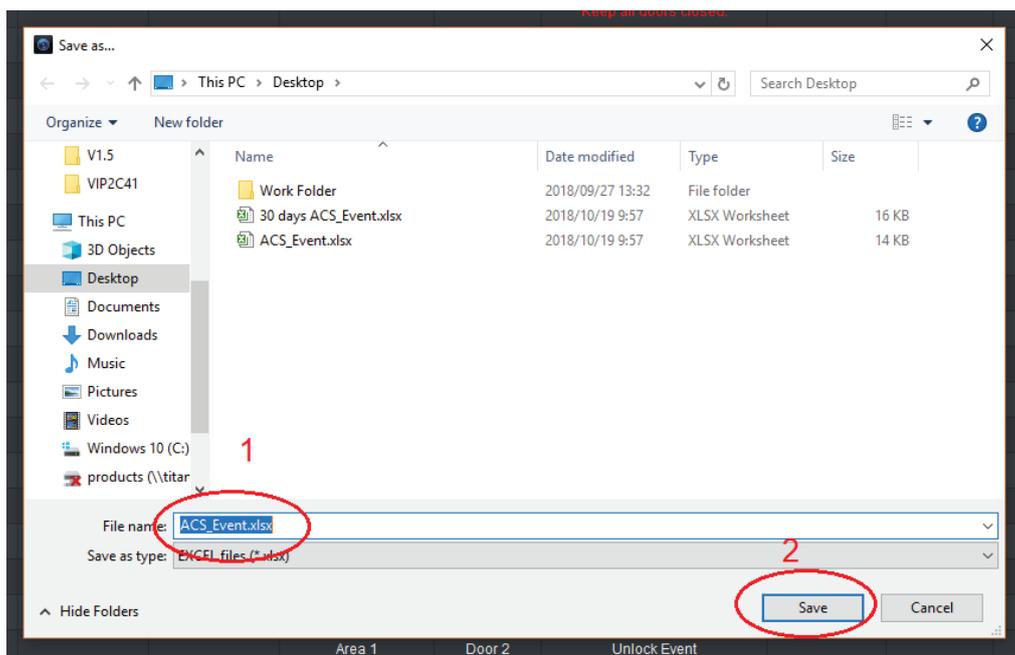
3.3 Advanced Functions

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

3.3.1 First Card Unlock

The specified doors must be unlocked by appointed users first, then other users can open the door afterward. This function ensures that the door must always opened by appointed users before other users with lower access rights can. 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.

1. Click the "Upload User to Device" icon, then select "First Card Unlock".
2. Click the "Add" button and select which door is to be "First Card Unlocked".
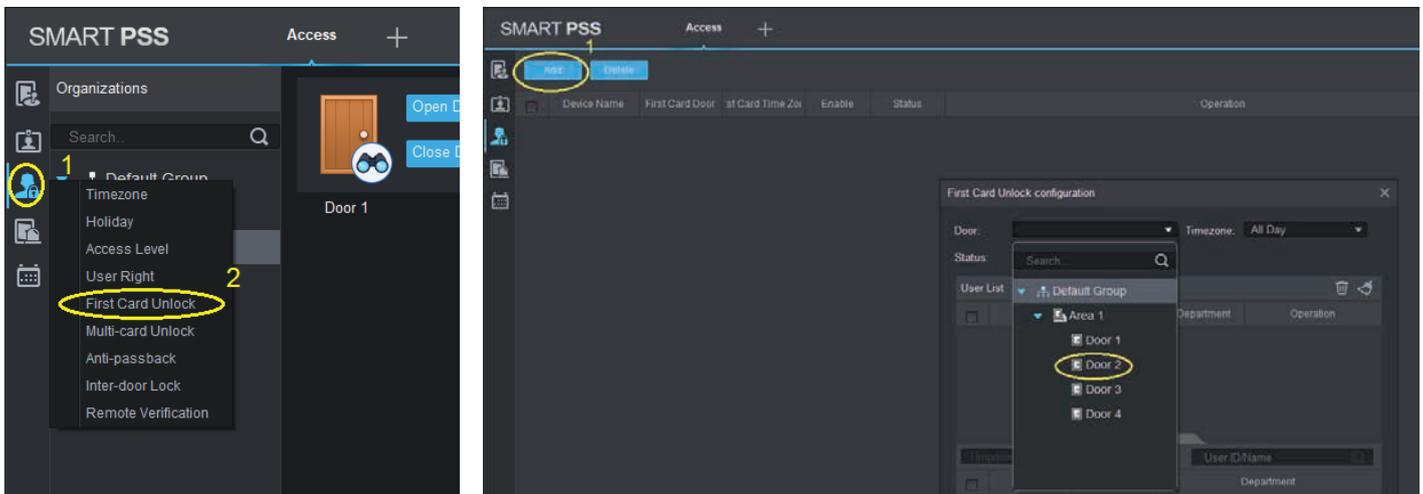
3. Enter the user ID or user name to be the "First Card Unlock" holder. The name will be displayed automatically if the information is correct
4. Click "Save" when done. The door information to be "First card unlocked" is shown.

   In this example, Mandy is the supervisor to "First Card Unlock". She must open Door2 before anyone else can.

VIP Vision Access Control Installation Manual - Version: VIPACC-Q121
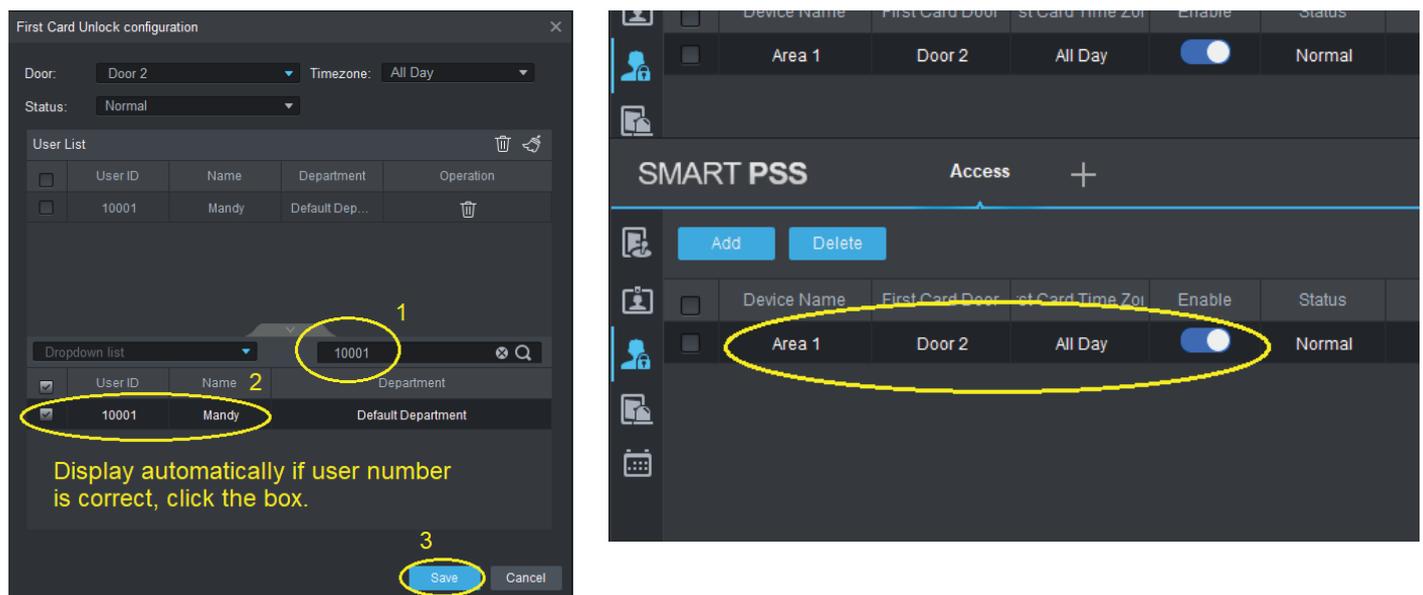
3.3.2 Multi-card Unlock

The door is to be unlocked by **TWO** groups of user in a specified order. This is similar to First Card Unlock, but also allows unlocking by multiple specified/all group members.

1. Click the "Upload User to Device" icon, then select "Multi-card Unlock".
2. A user group must be added first. Click "User Group" to create one.
3. Click the "+" symbol to add a user group.
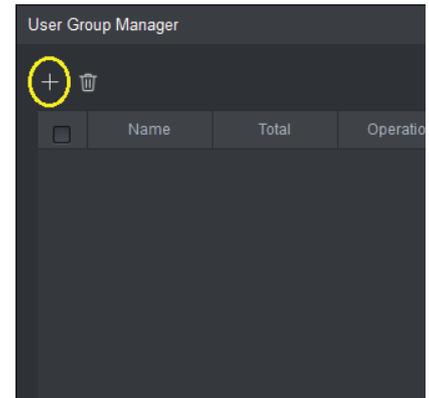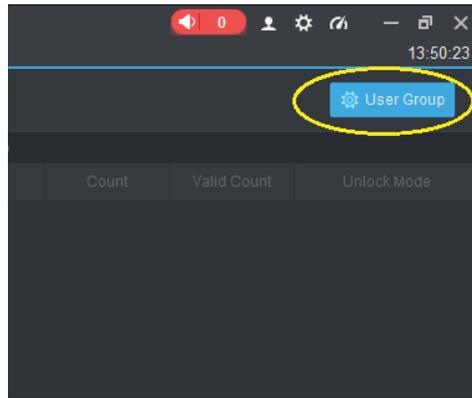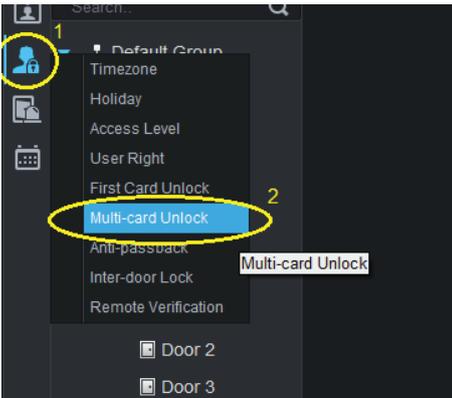
4. Name the user group
5. Click the magnifier icon to search for users to be added. Select each user to be added to this group.
6. Click "Save" to finish.
7. Repeat Steps 3 to 7 until all necessary groups have been added.
    In this example, Mandy and Jason are in Group 1 & Tim and Isabella is in Group 2.
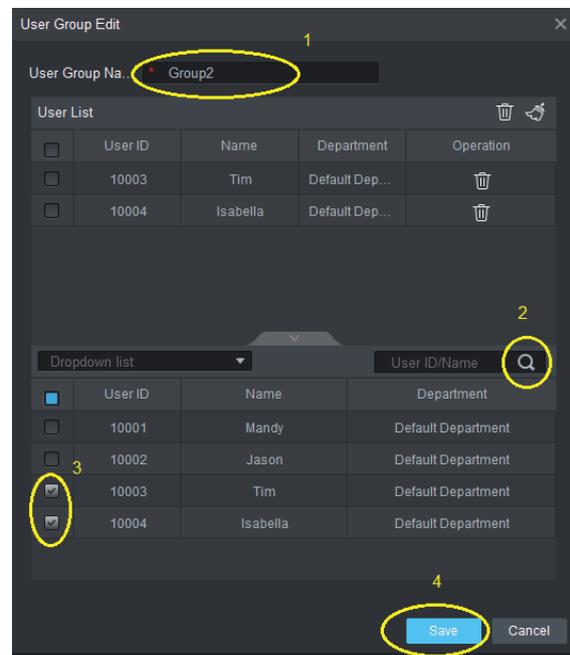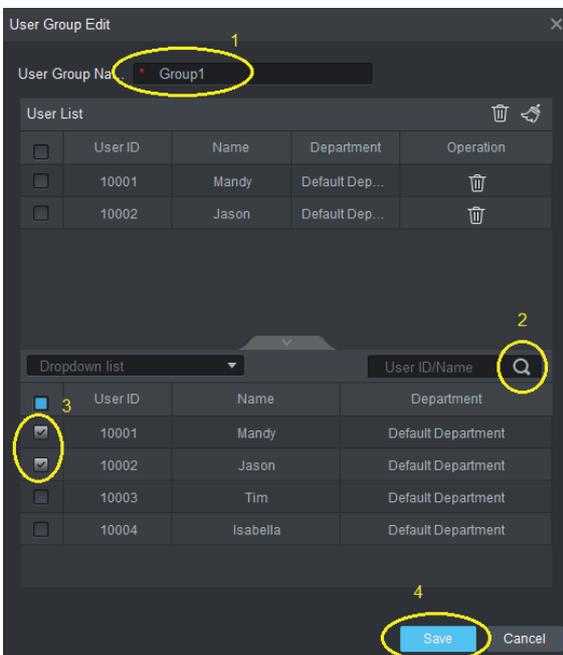
3.3.2 Multi-card Unlock (continued)

8. Close the User Group Manager window.
9. Click the "Add" button.
10. Select the door to be "Multi-unlocked".
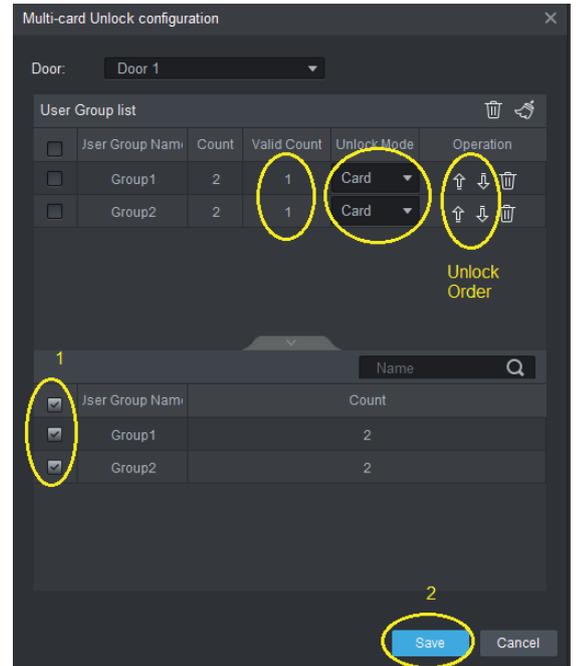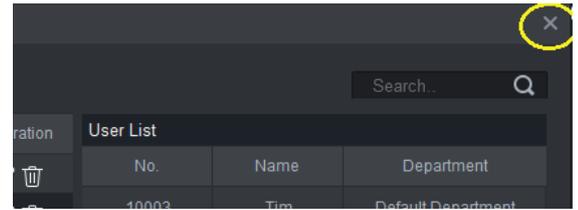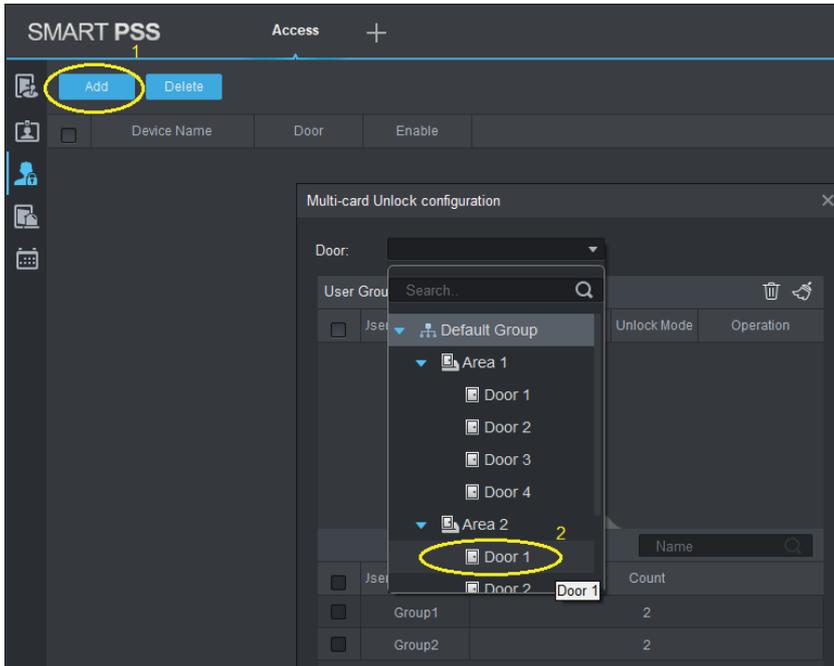
11. Click the door groups and click "Save" to finish.
    Note: You can select different unlock modes for each user to unlock: Card, Fingerprint or Password.
    Valid Count: Number of users per group requires to Multi-Unlock; in our example, one user per group.
12. Once set up is finished, you will see the following screen. You can enable or disable this function with the switch.
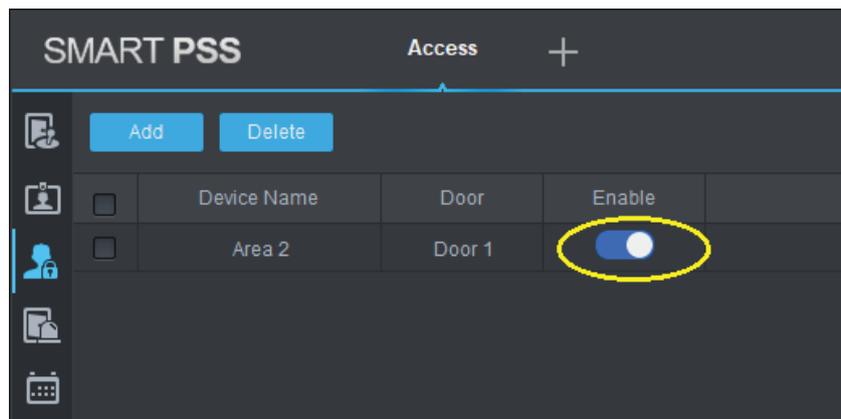
In this example, Group 1: Mandy and Jason, Group 2 : Tim and Isabella.

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 unlock, (4 users total to unlock). The order is: Group 1 Mandy + Jason, then Group 2: Tim + Isabella. Unlock order within the same group is not important.

3.3.3 Anti-passback

The anti-passback function is useful if there are two different doors intended for entrance and exit. Once an user enters via the entrance door, they cannot open the entrance door again. If the user wants to leave, they must use the exit door. An example for this application is a car park.

1. First click the "Upload User to Device" icon, then select "Anti-passback".
2. Click the "Add" button
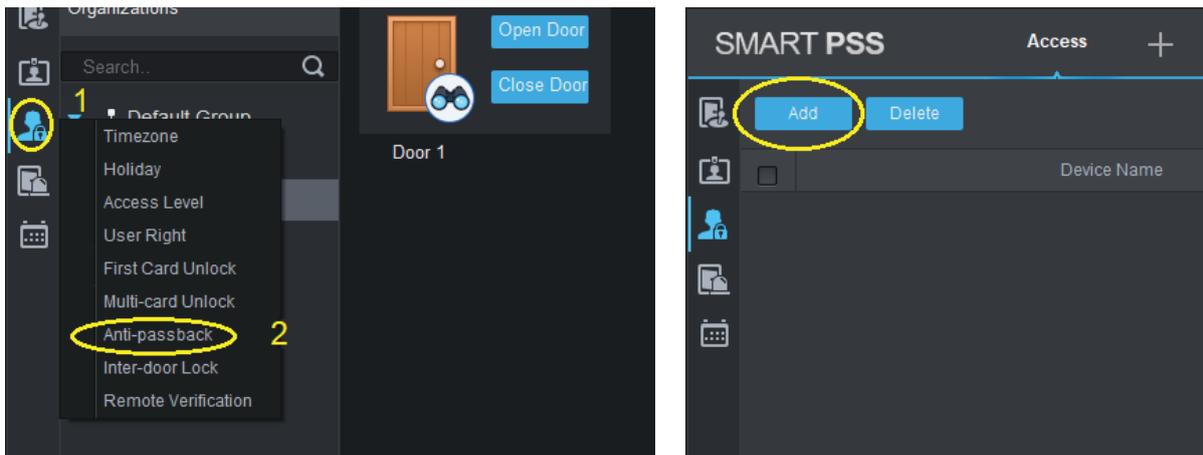
3. Select a Device (the name of the access controller) with the drop down list.
4. Name the Anti-passback rule.
5. Select the doors to use with Anti-passback.
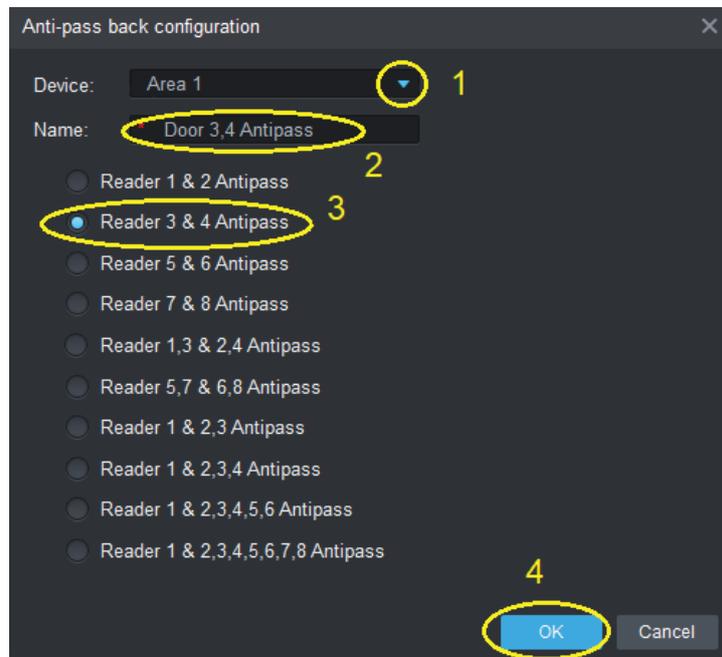
In this example, Area 1 access controller door 3 and 4 are "anti-passback".

i.e. Users must enter from door 3 and leave from door 4. Once they have entered through door 3, they cannot open door 3 again and must leave from door 4.

3.3.4 Inter-door Lock

With inter-door locking, Door B cannot be opened if Door A is still open. Typical application: Bank security doors. To use this function, door open/close status sensors must be installed
Important: For this function to work properly, Door Sensors must be enabled in the "Door Configure" menu.

1. Click the "Upload User to Device" icon, then select "Inter-door Lock".
2. Click the "Add" button.
3. Select a Device (the name of the access controller) with the drop down list.
4. Name the Inter-lock rule.
5. Select the doors to be Inter-locked.
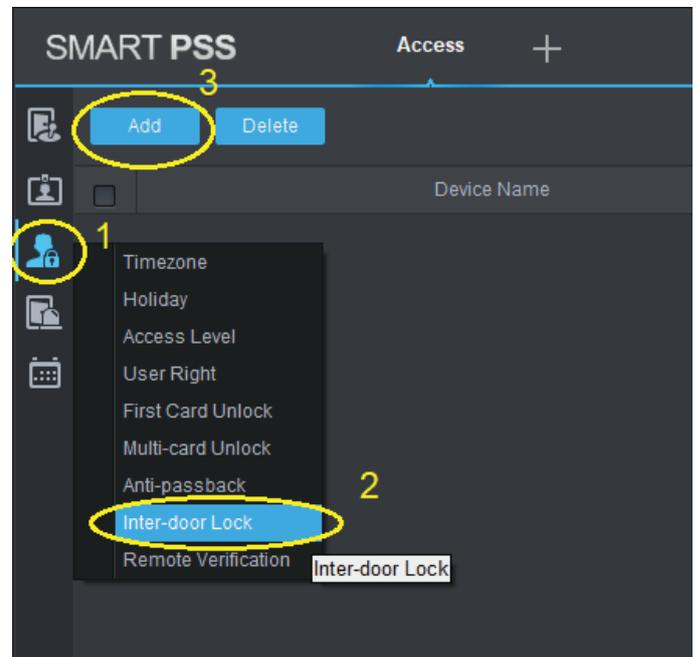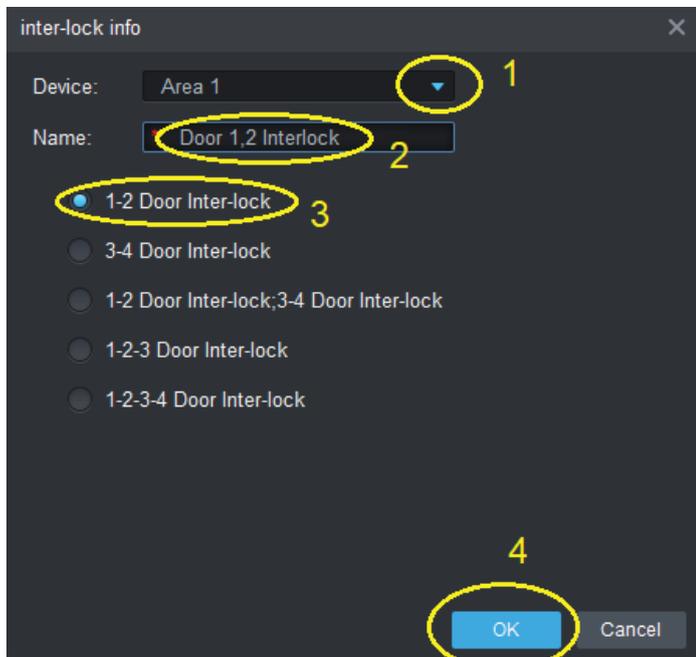
In this example, Area 1 access controller door 1 and 2 are inter-locked.
i.e. If Door 1 is not closed, users cannot open Door 2. Similarly, Door 1 cannot be opened if Door 2 is not closed.

3.3.5 Remote Verification

When enabled, every user with access rights to enter a door will be verified by a photo stored 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 pops up so the operator can verify the user's identity. The operator then opens the door **manually** by clicking the "Open" button.

This function is useful if human verification is required in areas where high security is needed.

*Important: Once this function is activated, **the door must be opened MANUALLY** after verification. Entering the keypad password or tapping card on the card reader will no longer open the door automatically without verification.*

1. Click the "Upload User to Device" icon, then select "Remote Verification".
2. Click the "Add" button.
3. Click to select the door and time need Remote Verification to be enabled and click the "Save" button.
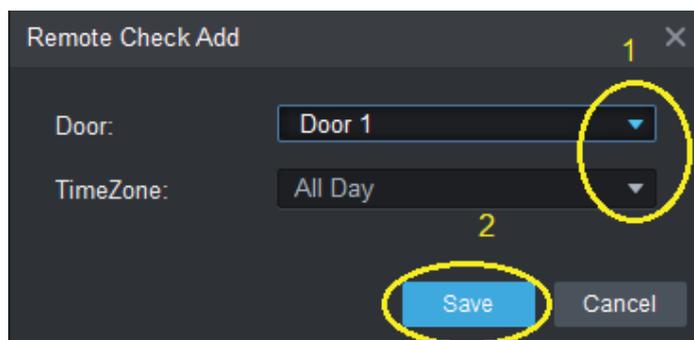
4. Once the set up is finished, you will see the following screen.You can enable or disable this function with the switch.
5. Click the event icon, double click Access Controller (Area 1) and the door to be "remote verified".
    In this example, Door 1 of Area 1 is selected.
6. At the bottom of the screen, click "Normal Event". A new window will open.
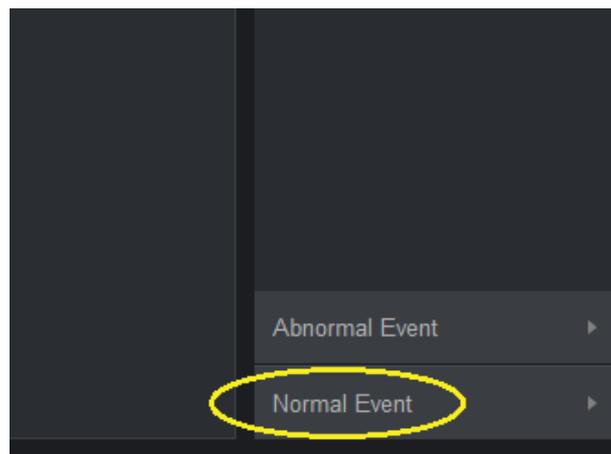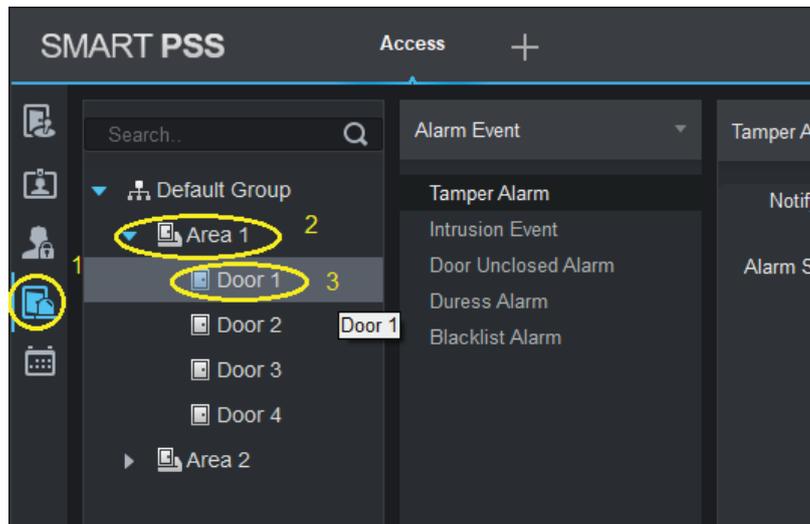
3.3.5 Remote Verification (continued)

7. Select the "Enable remote verification" and turn enable the switch. 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).

8. Double click the IP Cam controller (Network Video Recorder - IP CAM in this case) and select the camera to be displayed.
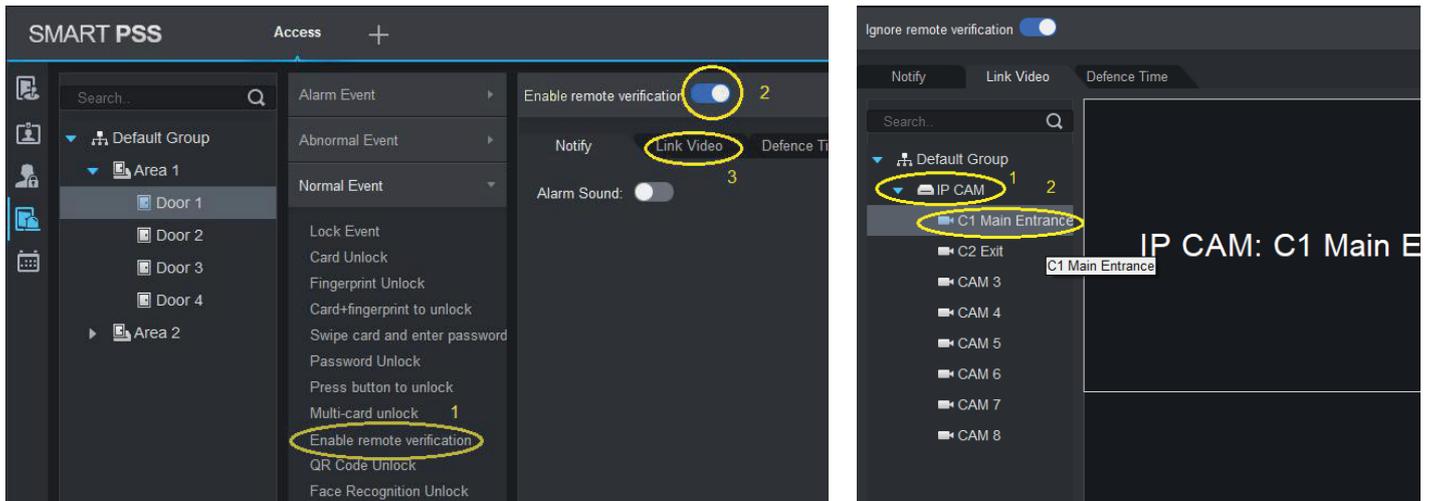
9. Make sure the switch "Auto Open Video" is on (Blue colour) and click the "Save" button to finish.

Remote verification setup is now complete.

In this example, 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.
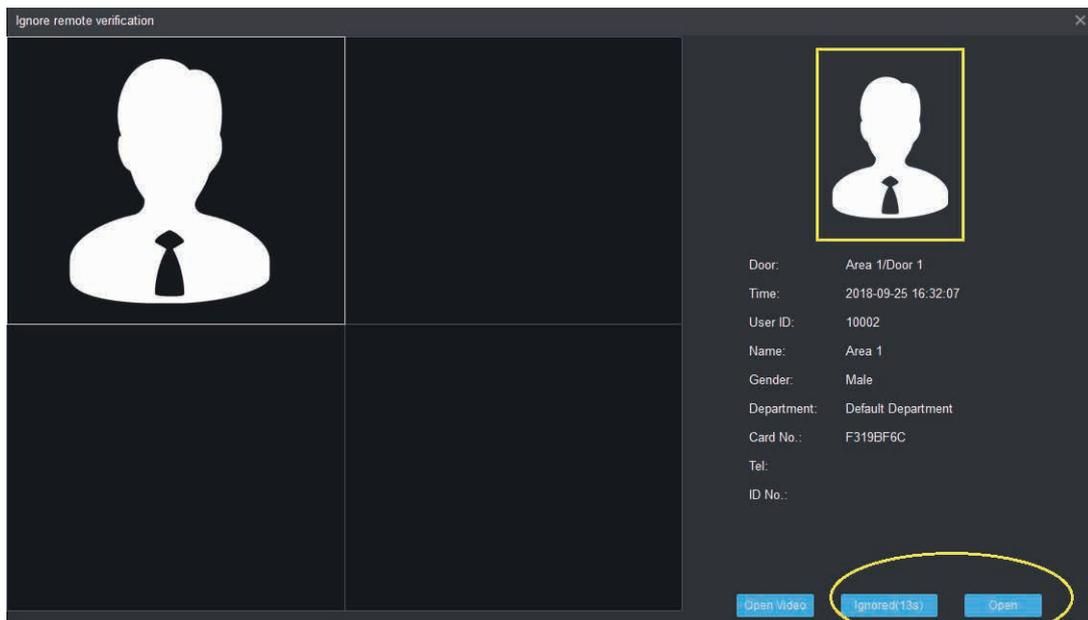
3.3.6 Door Open Timeout

The VIP Vision access controller is able to notify the operator when a door is opened for a duration 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.

1. Click the Console icon.
2. Choose the door to be configured by right clicking the door name and clicking Door Configuration.
3. Following the image below, turn on the Door, Alarm and Door Sensor switches, set a Close Timeout time (example: 10 seconds) and select the Overtime check box.
4. Click "OK" to save.
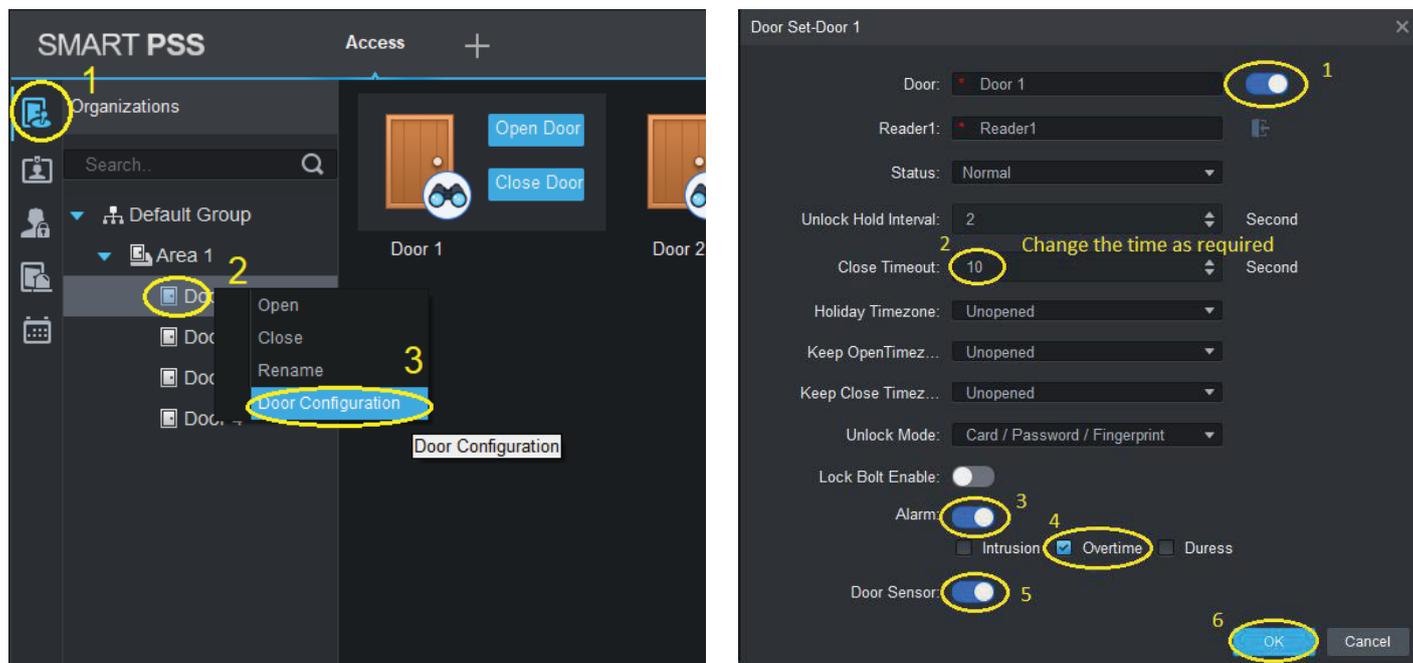
5. Click the Alarm button, then select the door being configured and click Door Unclosed Alarm.
6. Switch on "Door Unclosed Alarm" and "Alarm Sound". Click "Save" to finish.
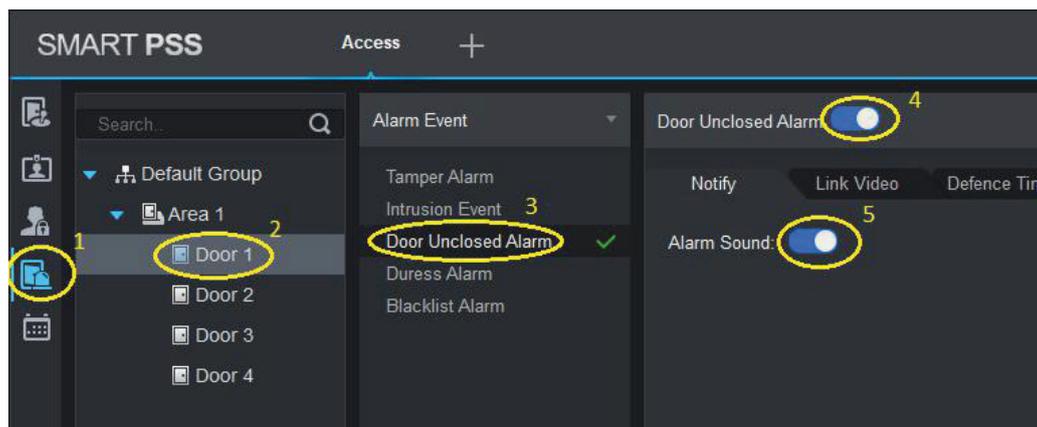
When finished, the PC speak will sound if the door is opened for a period longer than the preset period. Note:

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.

3.3.7 Backup and Restore Smart PSS Settings

Once you have finished configuring Smart PSS settings, it is recommended that you backup the PC settings. This will benefit you when re-installing or changing the Smart PSS setup to a new PC, as you won't need to input all saved settings and information (such as user information, access level, schedule etc) again.

Backup settings:

1. Click the System Config symbol.
2. Click 'Local Path' on the left panel then click 'Backup' button.
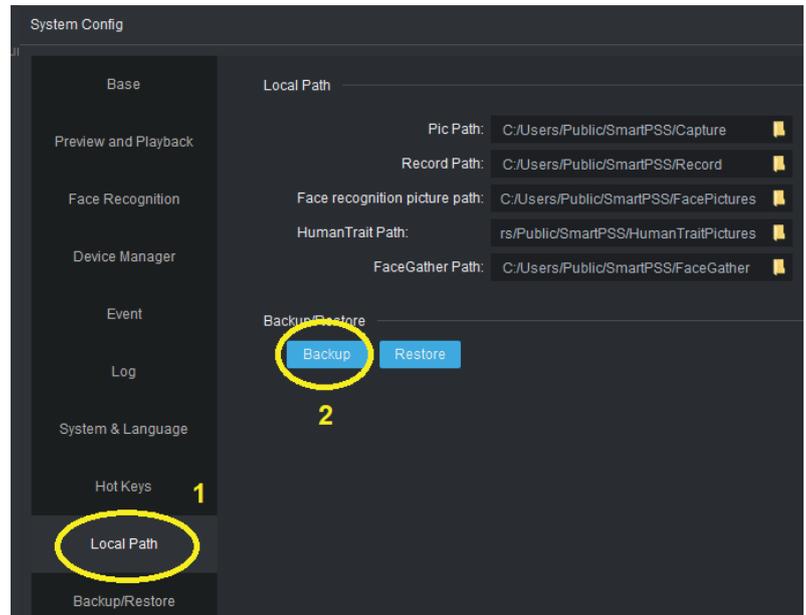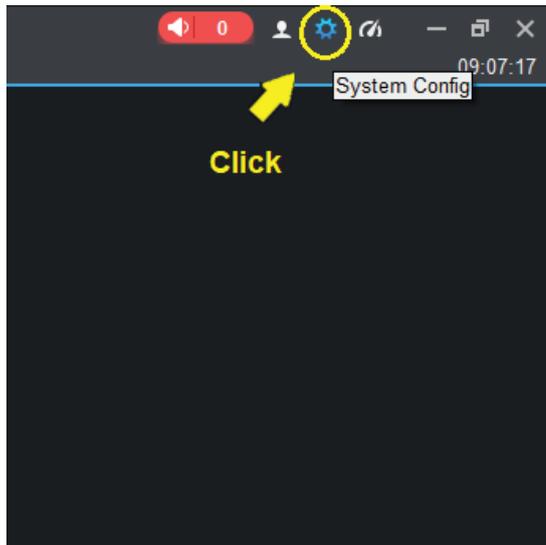
1. Enter the filename for the backup file and click "Save"
2. Wait for about 10 seconds. You'll see the the prompt "Export of system setting is done." in the lower right corner of the screen.
3. After that, click "Save" button to exit the System Config menu. Backup is completed.
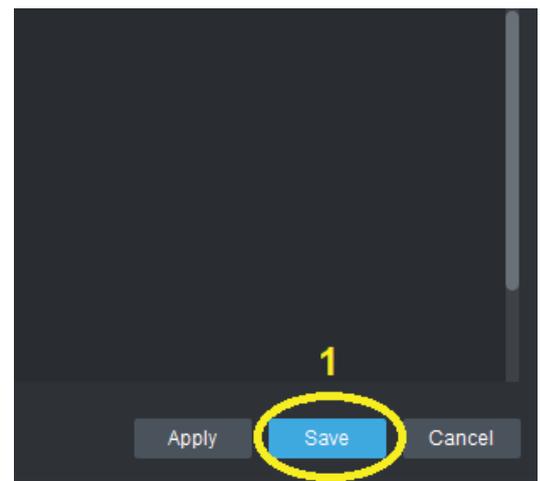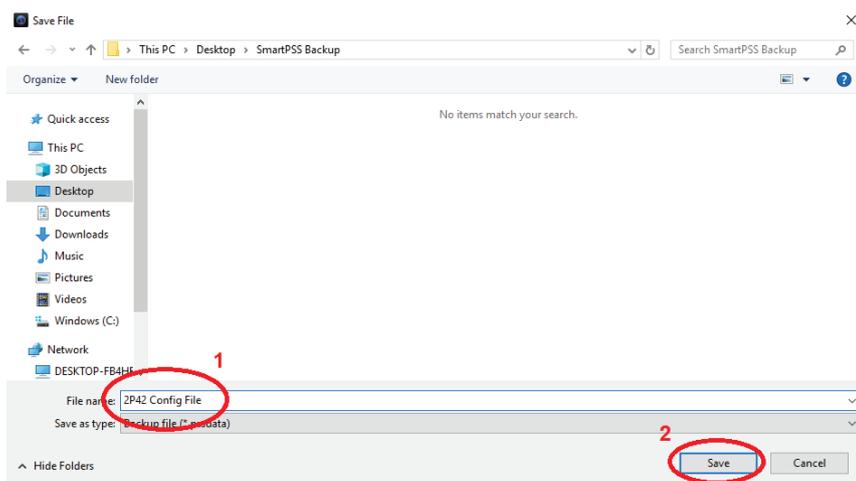
Backup settings:

1. Click the System Config symbol.
2. Click 'Local Path' on the left panel then click 'Restore' button.
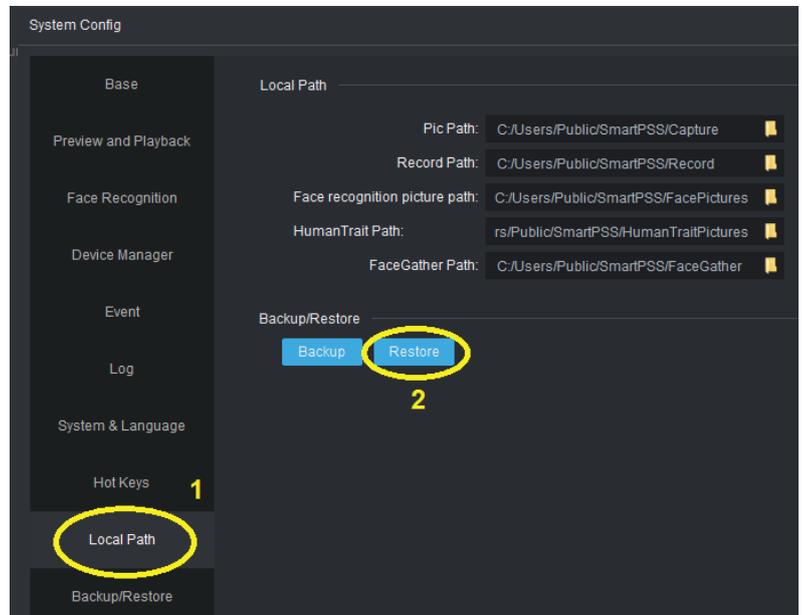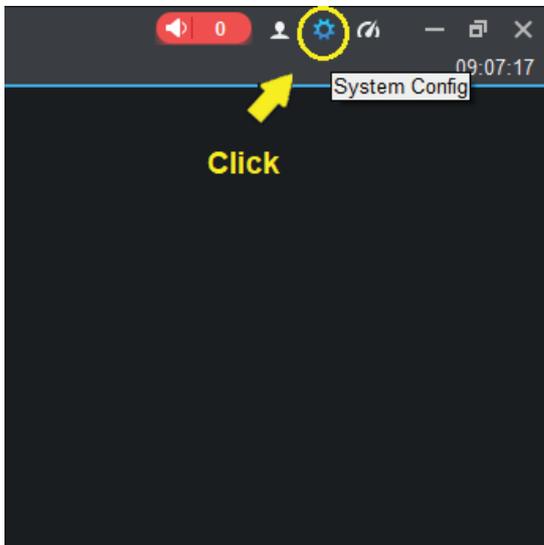
3. Select the file ot be restored and then click "Open".
4. Click 'OK' button. The restore process will begin.
5. The system will restart after the restore is finished.
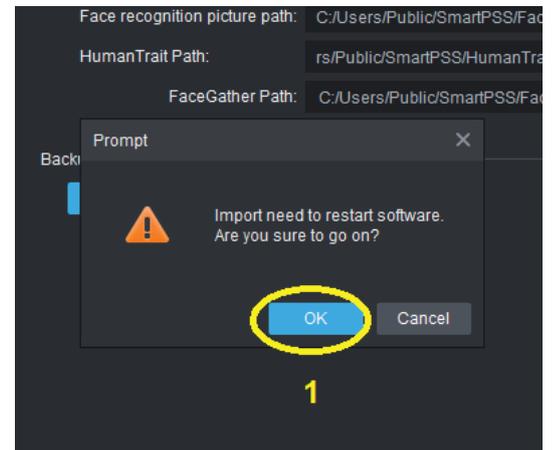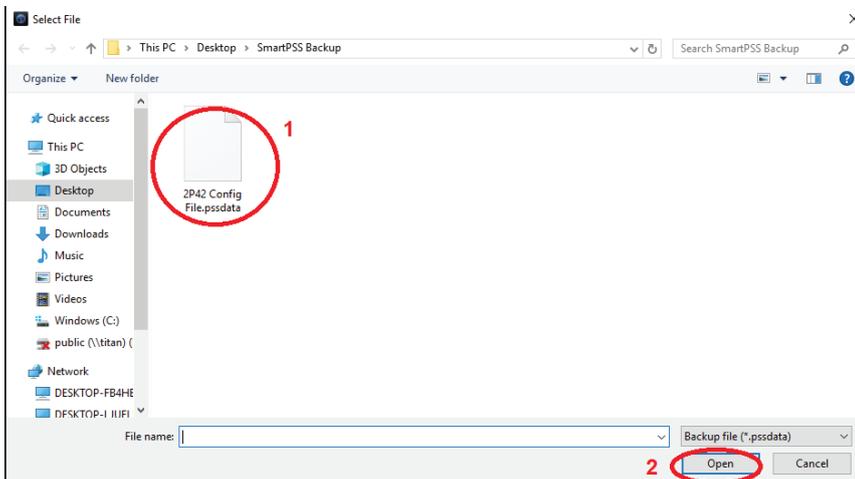
3.4 Events

In simple terms, an event is an action taken (B) after an incident occurs (A). "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 to take when an event is triggered (refer to full list on next page).

VIP Vision Access Control Installation Manual - Version: VIPACC-Q121
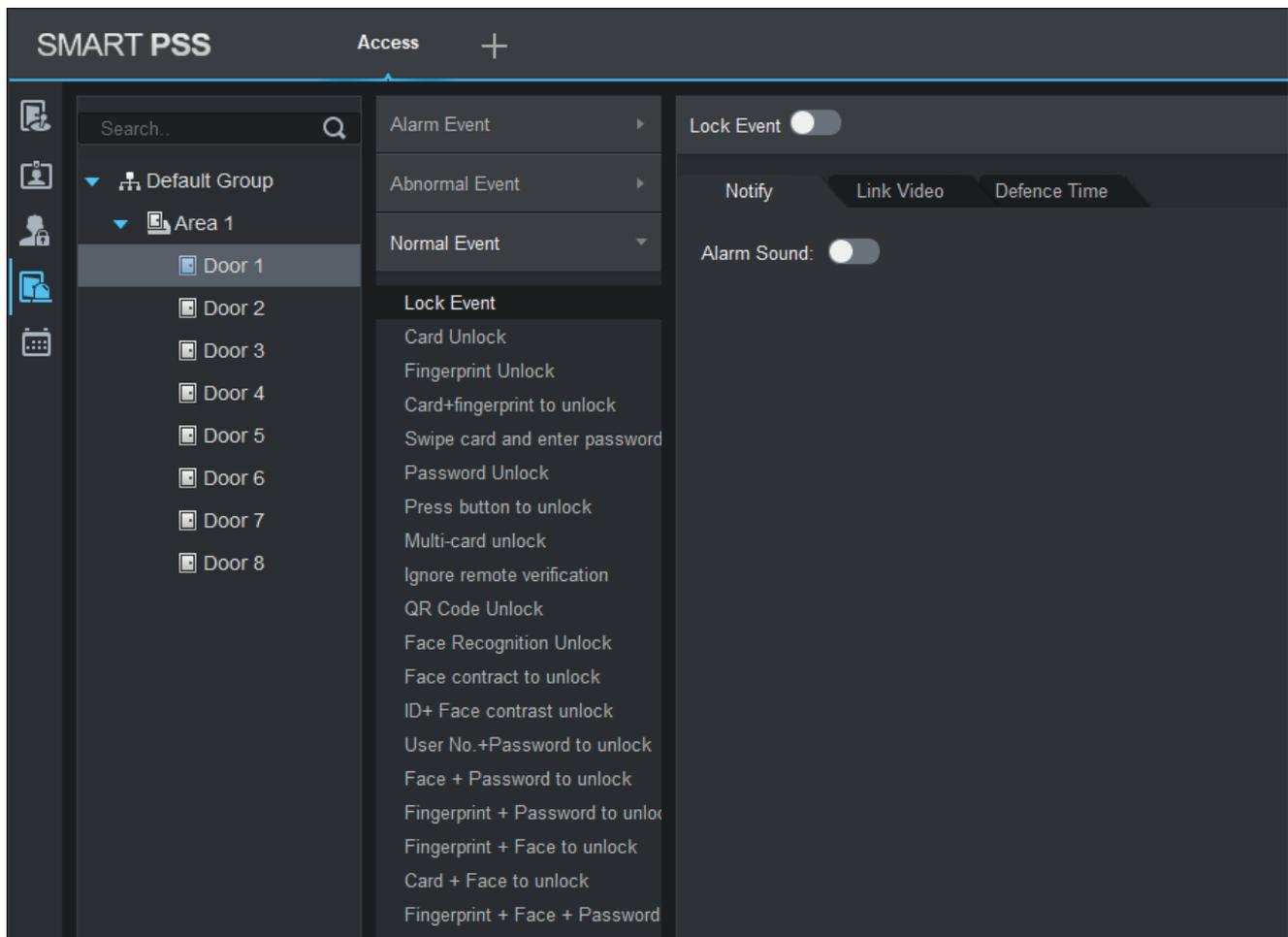
Event Type	Description
Alarm Event	**Tamper alarm:** Alarm is triggered when the card reader is un-installed.
	Intrusion alarm: Alarm is triggered when a door is opened abnormally.
	Duress alarm: Alarm is triggered when a door is opened by duress card.
	Door Unclosed alarm: Door remains opening and exceeds 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 while 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.
	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.

4. Troubleshooting

4.1 Troubleshooting Issues

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
Can't connect to PC console	• Ensure that you are connecting to the correct Access Point, with the correct password. • Ensure DHCP is turned on before you attempt to connect to the Access Point.
No power	• Ensure that power switch is switched on. • Check power cord connection. • Confirm that there is power from the outlet. • Ensure the power supply meets or exceeds the current rating for the device you are powering.
Fingerprint reader is not working	• Make sure the fingerprint reader is connected on
Some cards cannot be used	• Ensure that RFID IC cards with frequency of 13.56MHz are used. • 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. • Check the wiring between the door electric strikes/bolts and the access controller. • Ensure that jumpers on the access controller main board are set correctly • Check door lock power.
User added but cannot gain access	• Ensure that the user has assigned access level to entry particular doors. • Ensure the user enter the door at correct time. • 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. • Ensure that the electric strikes/bolts are using separate power supply.
Can't open the door by door push button	• Check door push button wiring, make sure it is wired to the correct door. • 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. • 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.

VIP Vision Access Control Installation Manual - Version: VIPACC-Q121

4.2 Frequently Asked Questions

I have enabled the Intrusion and "Door unclose" (overtime) warnings but they are not working. Why?

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.

How do I access the "Door Configuration" menu?

Click the "Console" icon on the top left corner of the screen. Select the door you want to configure and RIGHT click the mouse. Click "Door Configuration".

How do I reset the system to factory settings?

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.

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.

Unfortunately, you <u>must</u> 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 <u>must</u> 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.

Fingerprint verification is only working intermittently. Why?

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.

Fingerprint reader can read cards but cannot read fingerprints. Why?

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.

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

Technically yes, but it's redundant. We strongly recommend that for a single reader, only one connection method should be used.

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

Yes, the access controller accepts mix connections.

On the "Add user" or "Edit user" screen, what is "Card Password" and "Unlock Password"?

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.

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

Suggested password length is 6 digits. Do not use simple passwords such as "123456", "000000" etc, as they can be easily guessed.

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".

Can I use ID cards instead of IC cards?

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.

Can I Inter-lock/Anti-passback doors connected to different access controllers that are in the same network?

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

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

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.

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

1. First, unplug the network cable for the one already installed.

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

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

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

5. Power off both controllers and power on again.

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

Yes, you can. But it is **not recommended**, as you will lose 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 settings do not match, you cannot access the controller anymore. You will have no choice but to reset to factory settings, resetting the IP address back to 192.168.0.2.

1. Click the Device CFG icon on the main menu.
2. Click the access controller's name.
3. Click Network and then TCP/IP.
4. Enter the **NEW** IP address. Must be 192.168.0.xx, where xx is 0-255 and does not conflict with other devices on the same network.
5. Click "Save" button below this dialogue box.

The access controller will generate a long beep and restart.
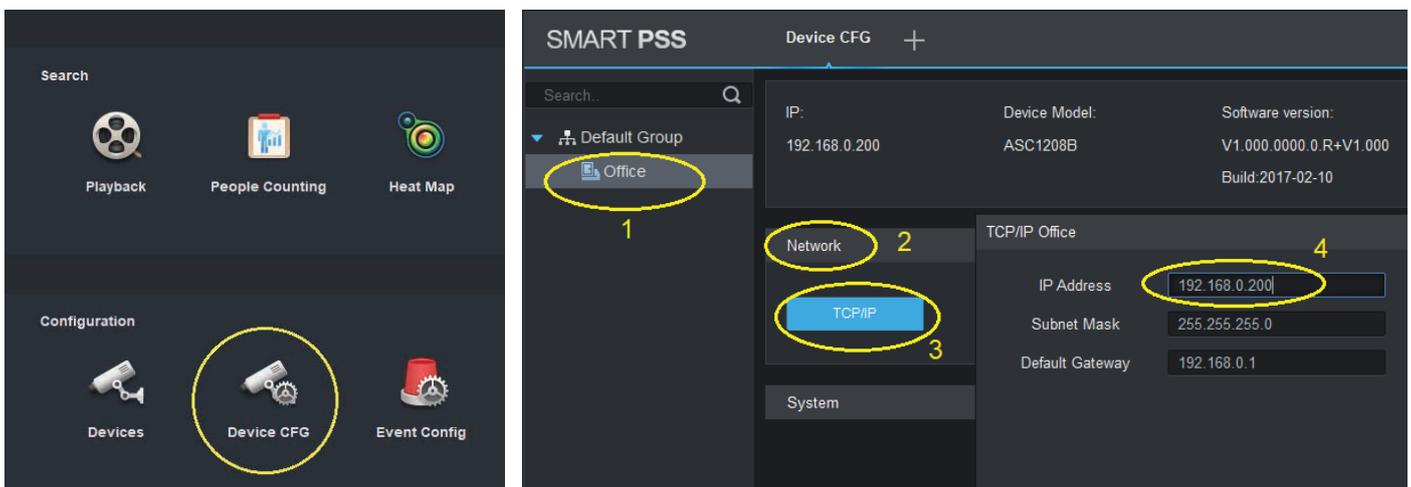
1. Go back to the main menu and click the Devices icon.
2. Click the modify icon.
3. Enter the new IP address. Must match the two IP addresses.
4. Click the Save button.
5. If the modification is successful, the Online Status indicator will turn green.
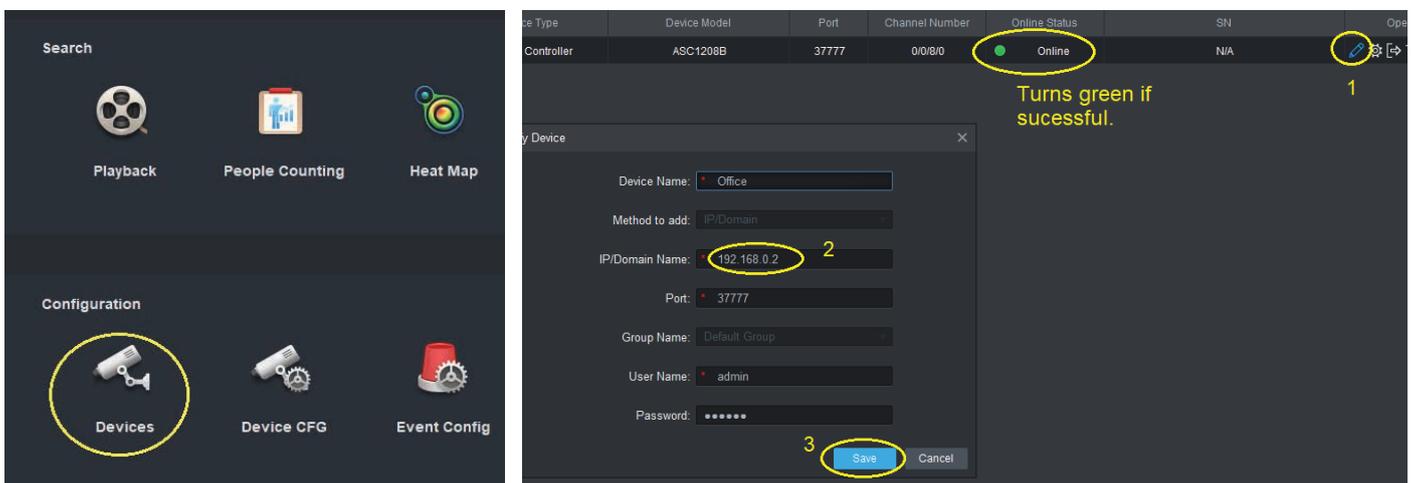
Version: VIPACC-Q121

Note:

All products, designs and software here are subject to change without prior written notice.