V1

Official UK distribution partner

ACCESS CONTROL QUICK INSTALL GUIDE

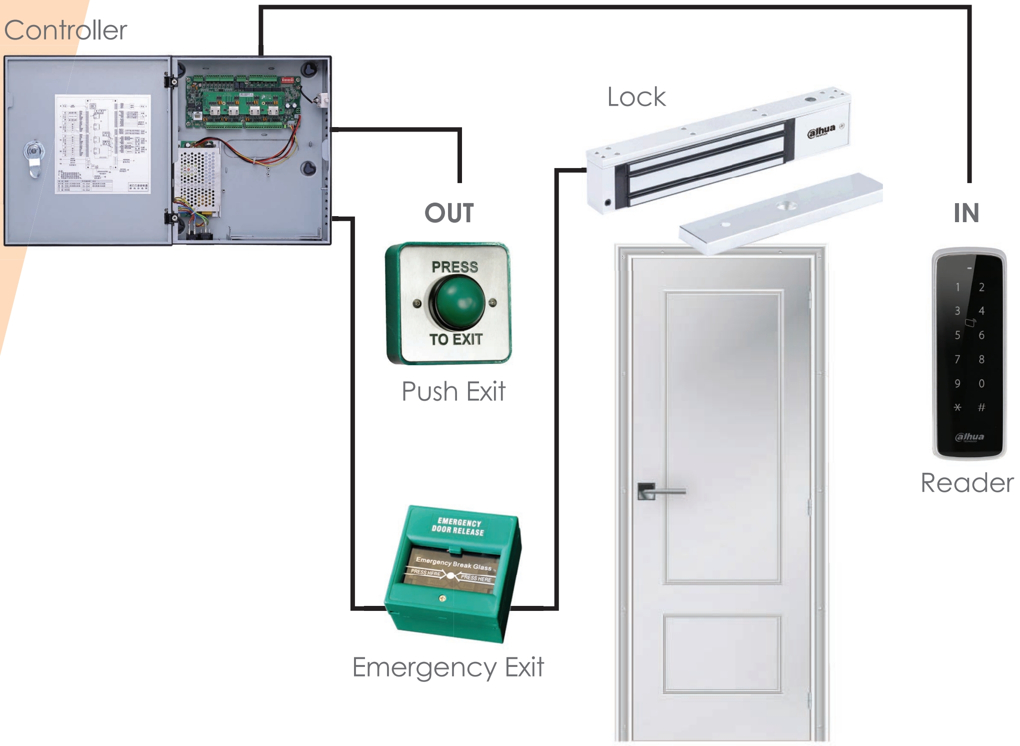
Please read this document before installation

WIRING CONFIGURATION - ACS CONTROLLERS

Dahua access controllers can be used in multiple installations scenarios with options for one door, two door or four door controllers and one way or two way access.

The example below is based on a one door one way system.

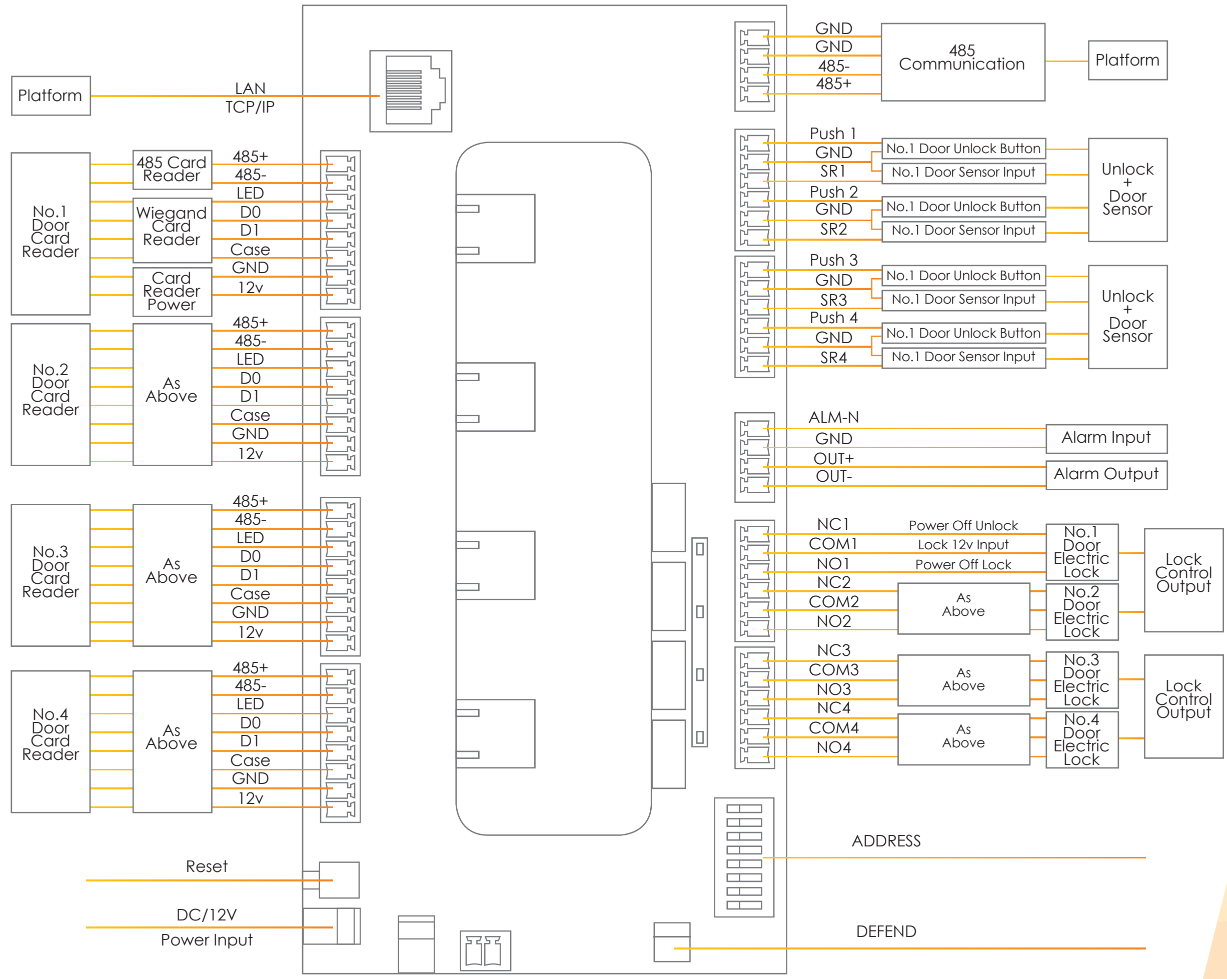
One Way Access Example



Connections

The number of connections available varies between controller models but all controllers have the same basic configuration. Each controller can support at least one reader per door. Each door can also support push to exit, door sensor, lock output or an additional reader for two way systems.

When connecting Dahua readers to Dahua controllers, Wiegand connections are not required if RS485 is used.



Reader Connections

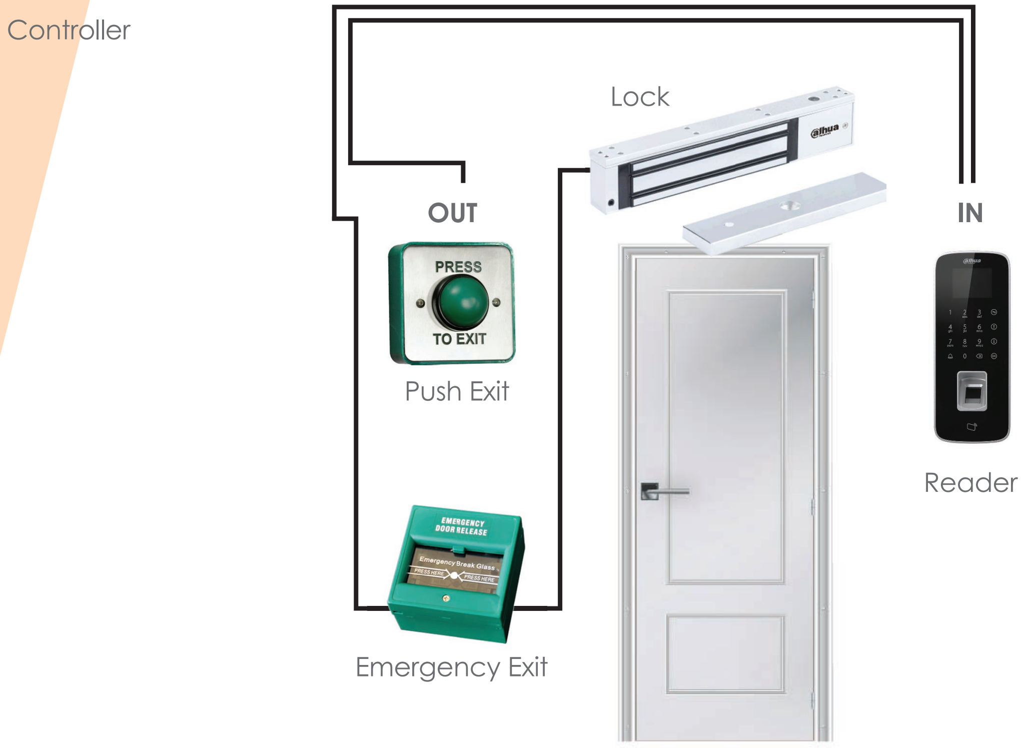
Purple Cable	RS485+ connection to controller
Yellow Cable	RS485- connection to controller
Brown Cable	Wiegand LED connection to controller
Green Cable	Wiegand D0 connection to controller
White Cable	Wiegand D1 connection to controller
Blue Cable	Wiegand case/tamper connection to controller
Black Cable	Reader ground connection to controller
Red Cable	Reader 12v positive connection to controller

WIRING CONFIGURATION - ASI1212D

The ASI1212D is a standalone two way controller with built in keypad, card & fingerprint readers. This unit supports a single door with the option to add an external reader for use as a two way system.

The example below is based on a one way system.

Stand Alone Access Example



Connections

Connector 1	**Purple Cable**	Push to Exit
	Yellow Cable	Ground (Push to Exit / Door Sensor)
	Brown Cable	Door Sensor
	Green Cable	Lock Output Normally Open
	White Cable	Lock Output Normally Closed
	Blue Cable	Lock Output Common
	Black Cable	12v - Power Input
	Red Cable	12v + Power Input

Connector 2 (for external reader)

Purple Cable	RS485+
Yellow Cable	RS485-
Brown Cable	Wiegand LED
Green Cable	Wiegand D0
White Cable	Wiegand D1
Blue Cable	Wiegand Tamper
Black Cable	12v - Power Output
Red Cable	12v + Power Output

When connecting Dahua readers to Dahua controllers, Wiegand connections are not required if RS485 is used.

Connector 3	**Purple Cable**	RS485+
	Yellow Cable	RS485-
	Brown Cable	Alarm Input Ground
	Green Cable	Alarm Input
	White Cable	Alarm Output
	Blue Cable	Alarm Output Ground
	Black Cable	Bell-
	Red Cable	Bell+

Connector 4	**RJ45 Connector**	Network Connection

ACS NETWORK CONFIGURATION

Default Settings
Username: admin
Password: 123456
IP Address: 192.168.0.2

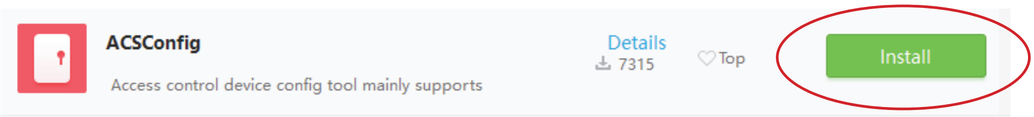
Configuring the access control system requires a computer with the ACS tool installed.

To install the ACS tool on a PC follow the steps listed below.

1. Go to www.cop-eu.com
2. Click on the Access Control category
3. Go to Controllers > click on your model of controller
4. Select the Downloads tab from underneath the product picture, then click on Dahua toolbox and run the installer

Once the Toolbox has been installed an account must be registered before the configuration tools can be installed.

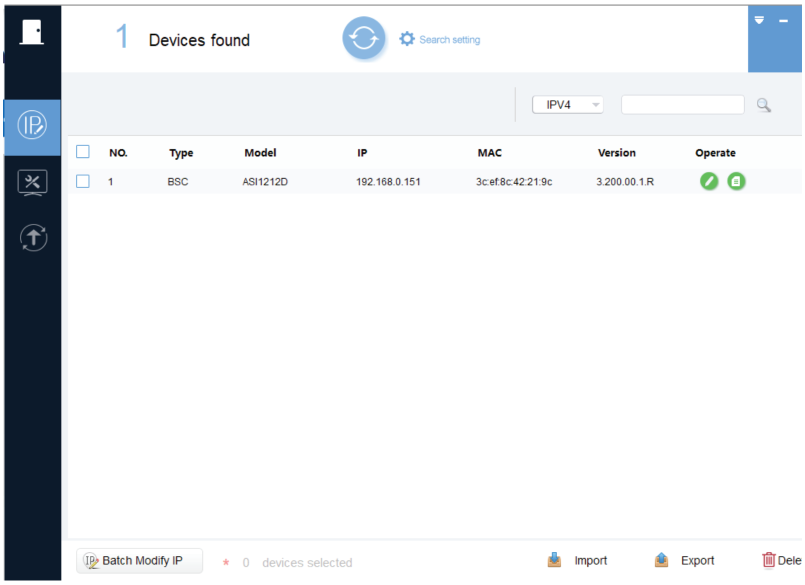
After installing and registering an account on Dahua toolbox, scroll down the list of applications and find **ACSConfig**. Click the install buttton to install the tool on your computer.



Once the Toolbox has been installed an account must be registered before the configuration tools can be installed.

After installing and registering an account on Dahua toolbox, scroll down the list of applications and find **ACSConfig**. Click the install buttton to install the tool on your computer, once installed click open to launch the tool.

Note: Make sure the computer running the tool is connected to the same LAN network as the ACS controller.



□	NO.	Type	Model	IP	MAC	Version	Operate
□	1	BSC	ASI1212D	192.168.0.151	3c:ef:8c:42:21:9c	3.200.00.1.R	✎

Any ACS controllers discoverable on the network will now be displayed within the search results, to modify the network configuration of the ACS controller, click ✎ to enter the new network configuration. Click **OK** to save the setting.

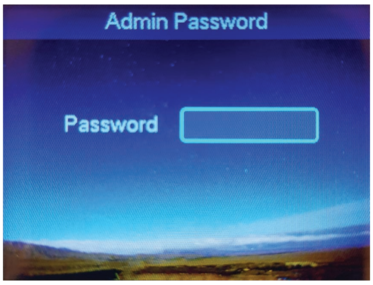
ASI1212D NETWORK CONFIGURATION

The ASI1212D features a screen interface that can be used to configure basic settings including network configuration.

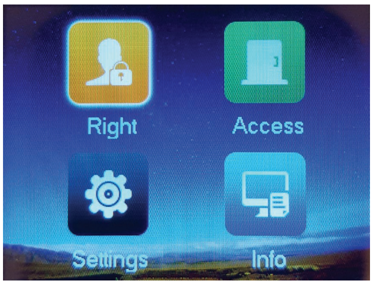
To adjust the network configuration of the unit, follow the steps below.

Default Settings
Username: admin
Password: 88888888
IP Address: 192.168.1.108

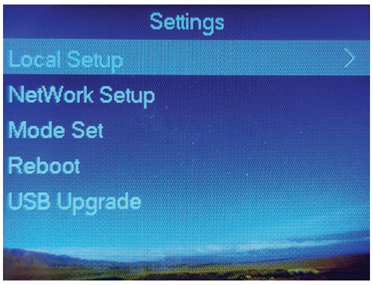
1. Press **OK** to display the admin login screen. Enter the admin password followed by **OK**.



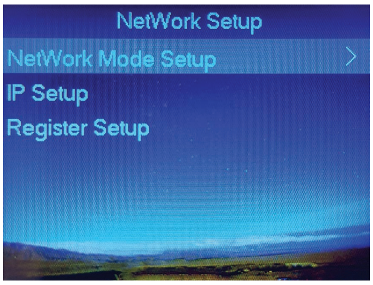
2. Press the Up/Down arrows to cycle through the menu options. Highlight Settings and press **OK**.



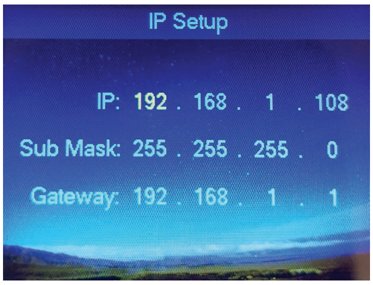
3. Select Network Setup and press **OK**.



4. Select IP Setup and press **OK**.



5. Modify the network settings accordingly and press **OK** to save the changes.


IP Setup

IP: 192 . 168 . 1 . 108
Sub Mask: 255 . 255 . 255 . 0
Gateway: 192 . 168 . 1 . 1

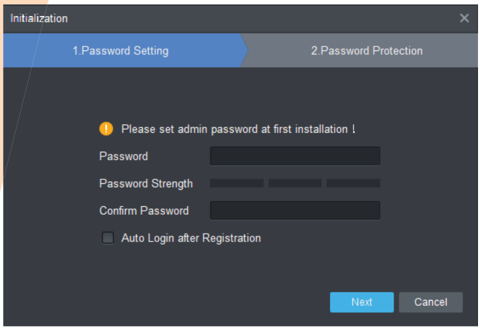
CONFIGURATION VIA SMART PSS

Smart PSS Initialisation

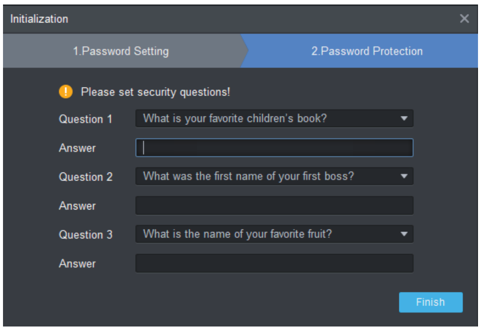
Both ACS controllers and the ASI1212D can be programmed via the Smart PSS software. If Smart PSS is not currently installed on the PC then this can be installed using Dahua Toolbox.

When first opening SmartPSS, the software will prompt for a password to be created, this password is used for logging into the software only and is not the password of the controller.

It is important to keep this password safe as failure to remember the password will result in not being able to run the SmartPSS software. The second step is to fill out the security questions and answers, they are used to reset the password if it is forgotten.



Please set admin password at first installation！



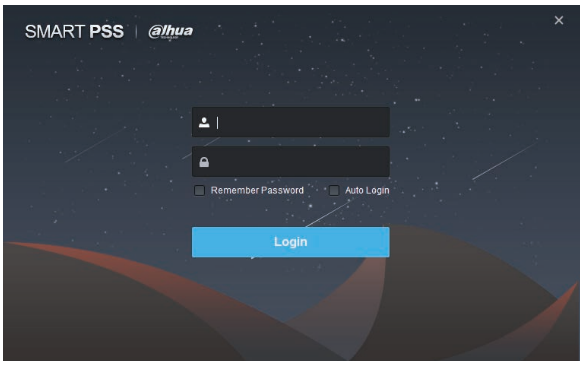
Please set security questions!

Question 1 What is your favorite children's book?

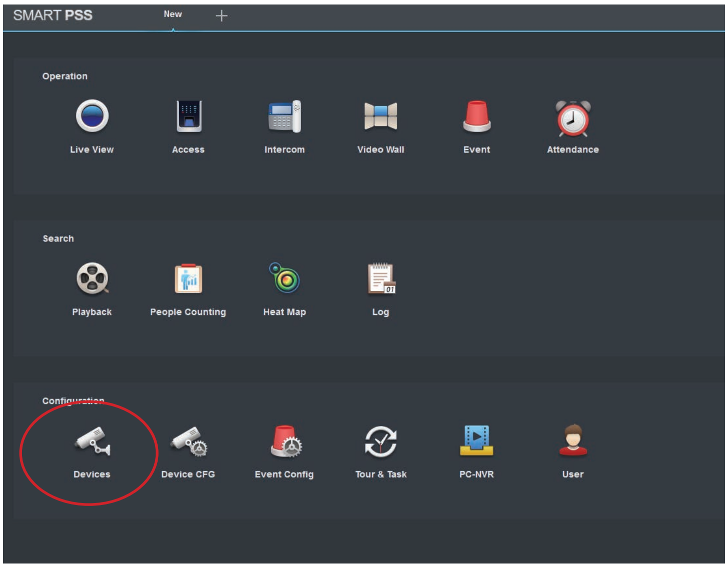
Question 2 What was the first name of your first boss?

Question 3 What is the name of your favorite fruit?

Once a password has been configured, login using the chosen password, the default username is **admin.**

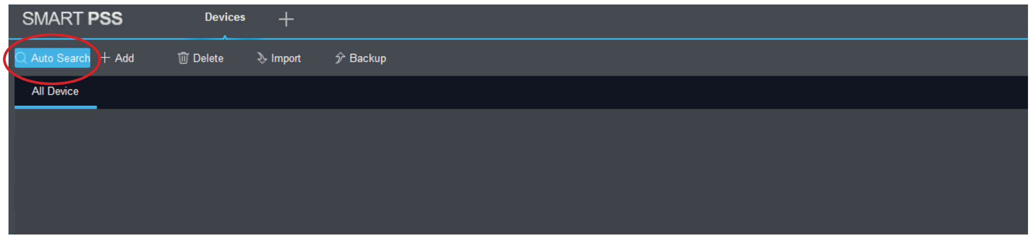


From the home screen select the **Devices** option.

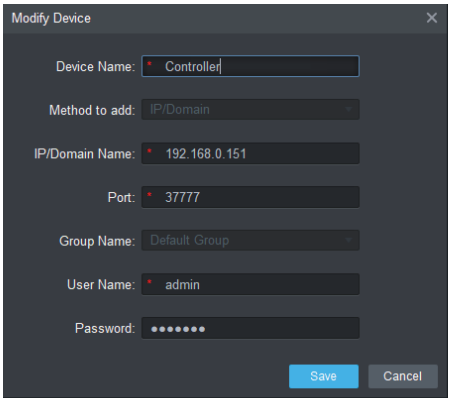


Adding a Controller

To add a controller, click the **Add** button.



Enter the connection details for the controller such as IP address, Username & Password, the default port number is 37777, click **Save** to store the connection details.


Modify Device

Device Name: * Controller

Method to add: IP/Domain

IP/Domain Name: * 192.168.0.151

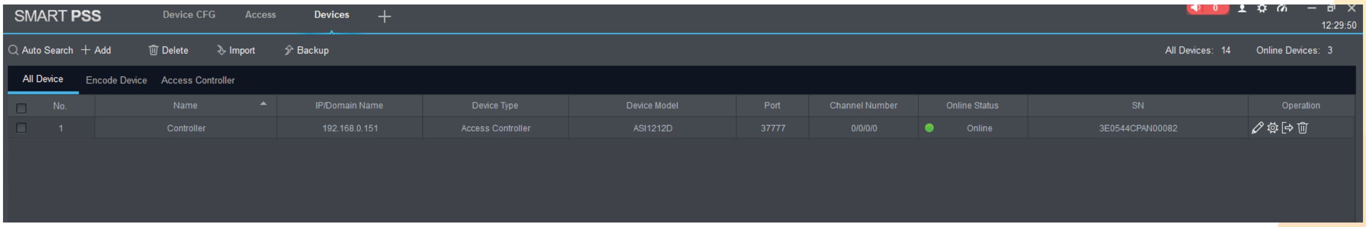
Port: * 37777

Group Name: Default Group

User Name: * admin

Password: •••••••

The added controller should now show in the device list with the current status as online.



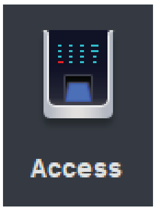
All Devices: 14 Online Devices: 3

□	No.	Name	IP/Domain Name	Device Type	Device Model	Port	Channel Number	Online Status	SN	Operation
□	1	Controller	192.168.0.151	Access Controller	ASI1212D	37777	0/0/0/0	● Online	3E0544CPAN00082	

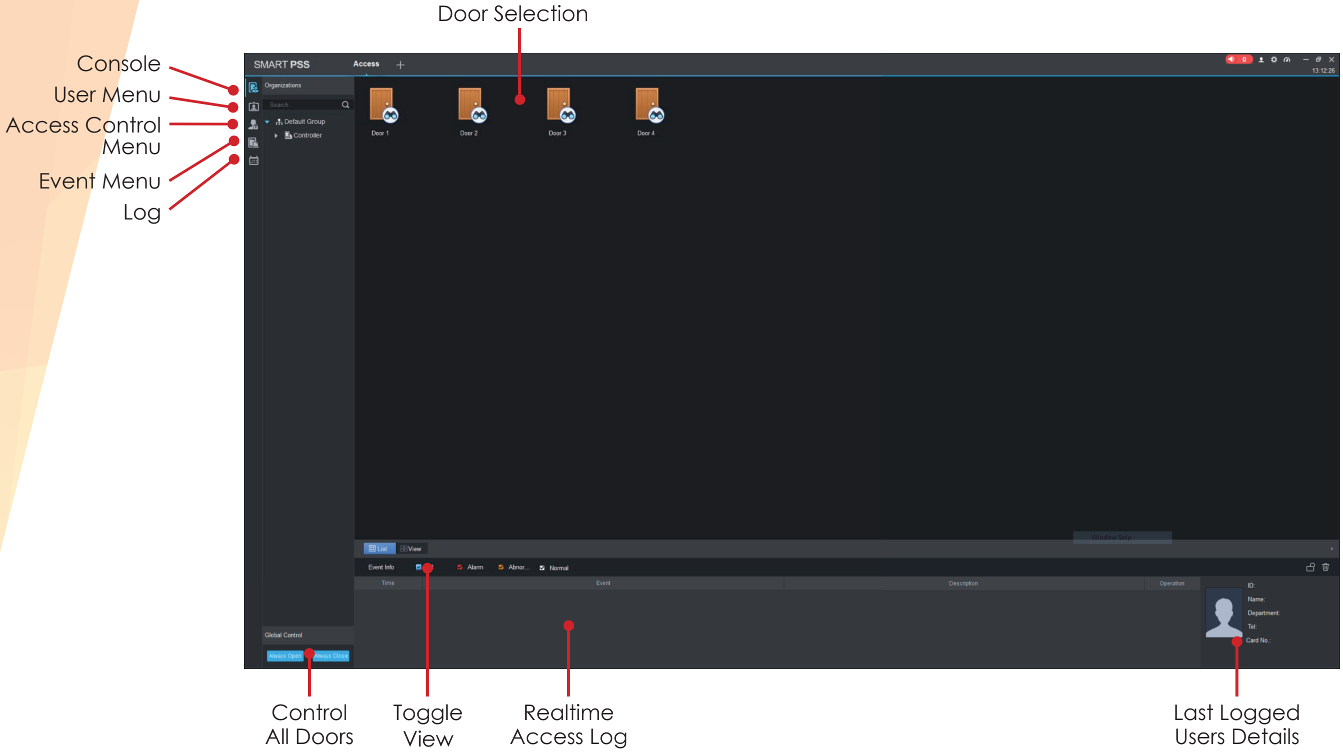
Note: If the device is not found, please refer to page 6.

Access Menu

All access control features are located within the Access section of the Smart PSS software. To enter this section, select the Access icon from the Smart PSS home screen.



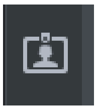
Once the access section has been opened the following screen will be shown. The number of doors displayed depends on the controller type, if a four door controller has been added then four doors will be displayed.



Adding Users

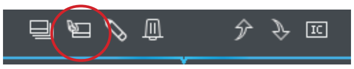
Users can be added to the system and access levels assigned with the Access section of the SmartPSS software. To add a new user follow the steps below.

Enter the user menu by clicking on the **User Menu** icon .

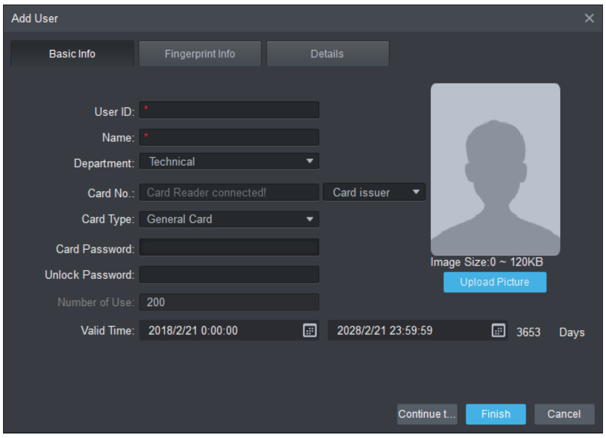


Users can be organised by department, to add a new department right click the area in the left window pane and select **Add Department**. Enter a name for the department and click **Save.**

To add a user click the new user button at the top of the SmartPSS interface.



Input the users details including ID, name, department, password and valid date range. The ID field is a unique ID given to each user, no two users can share the same ID.



Add User

User ID: *

Name: *

Department: Technical

Card No.: Card Reader connected! Card issuer

Card Type: General Card

Card Password:

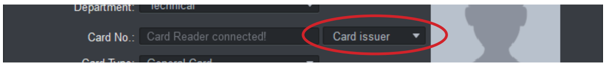
Unlock Password:

Number of Use: 200

Valid Time: 2018/2/21 0:00:00 2028/2/21 23:59:59 3653 Days

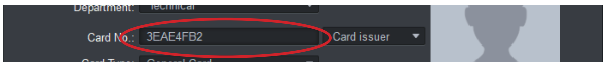
Image Size:0 ~ 120KB

When adding a Mifare card or fob to a user, first connect the ASM100 enrolment reader to the computer via USB. Alternatively, any card readers connected to the controller can be used to scan a user card for enrolment purposes. To choose the type of reader to be used, select a reader device from the **Card Issuer** dropdown box.



Card No.: Card Reader connected! Card issuer

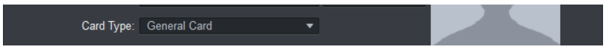
Once the **Card No** field shows the message: “Card Reader Ready”, the users card can be scanned which will assign the unique card ID to the user. Left click the **Card No** field, an audilble tone can be heard. Place the card over the reader, another audible tone can be heard which confirms the reader has scanned the card successfully. The unique card ID is now displayed in the **Card No** field.



Card No.: 3EAE4FB2 Card issuer

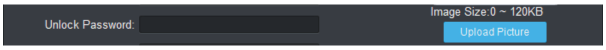
Select the card type from the dropdown box, there are multiple types available:

General	Standard User
VIP	VIP User
Guest	Temporary User, when used a limit can be set to how many times the card can be used
Patrol	Used for patrol logging without unlocking doors
Blacklist	Used to alert when a specific user accesses an area
Duress	A secondary card given to a user in case of duress. When scanned an alert can be triggered



Card Type: General Card

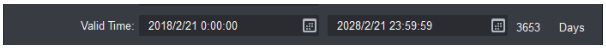
If using keypad entry, enter an unlock password for the new user. Passwords must be numerical and a maximum of 6 digits.



Unlock Password:

Image Size:0 ~ 120KB

Enter how long the new user is required access. A permanent user could be given a number of years, whereas an agency or temporary contract user could only be given a period of months or weeks.



Valid Time: 2018/2/21 0:00:00 2028/2/21 23:59:59 3653 Days

If required an image of the user can be uploaded to the Smart PSS software. This image will then appear along with the user details in the access console when the user accesses a given area.

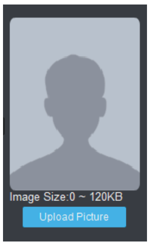
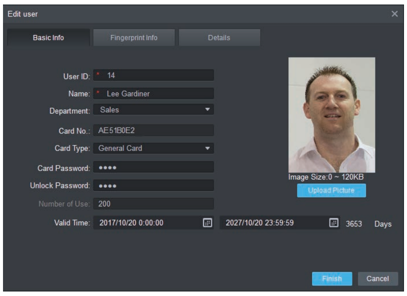


Image Size:0 ~ 120KB



Edit user

User ID: * 14

Name: * Lee Gardiner

Department: Sales

Card No.: AE51B0E2

Card Type: General Card

Card Password: ••••

Unlock Password: ••••

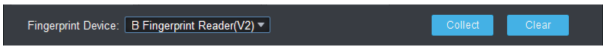
Number of Use: 200

Valid Time: 2017/10/20 0:00:00 2027/10/20 23:59:59 3653 Days

Image Size:0 ~ 120KB

If using biometric fingerprint readers, select the **Fingerprint Info** tab to add a user fingerprint.

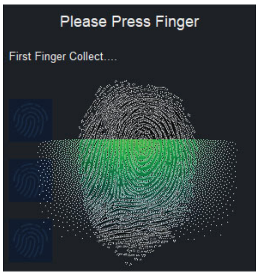
In the **Fingerprint Device** dropdown box, select the fingerprint reader that will be used to add the users fingerprint. This can be the ASM102-V2 USB reader or a fingerprint reader that is part of the system.



Fingerprint Device: B Fingerprint Reader(V2)

Click the Collect button to start recording the users fingerprint and follow the onscreen prompts.

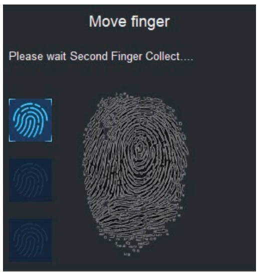
1. Place finger on fingerprint sensor



Please Press Finger

First Finger Collect....

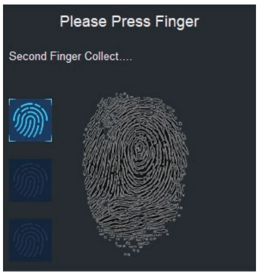
2. Remove finger



Move finger

Please wait Second Finger Collect....

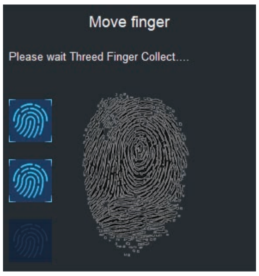
3. Place finger on fingerprint sensor



Please Press Finger

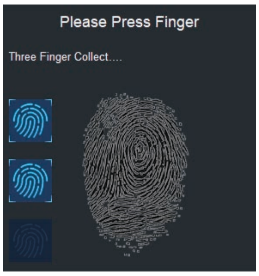
Second Finger Collect....

4. Remove finger


Move finger

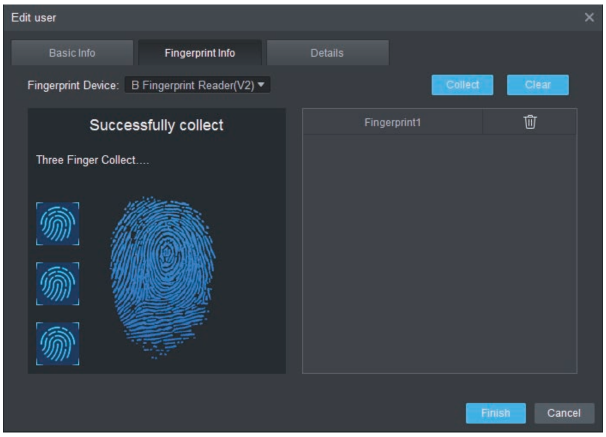
Please wait Threed Finger Collect....

5. Place finger on fingerprint sensor


Please Press Finger

Three Finger Collect....

The fingerprint should have now been recorded successfully, if the fingerprint recording fails, run through the process again making sure that the user places their finger tip over the sensor flat & central to the sensor.


Edit user

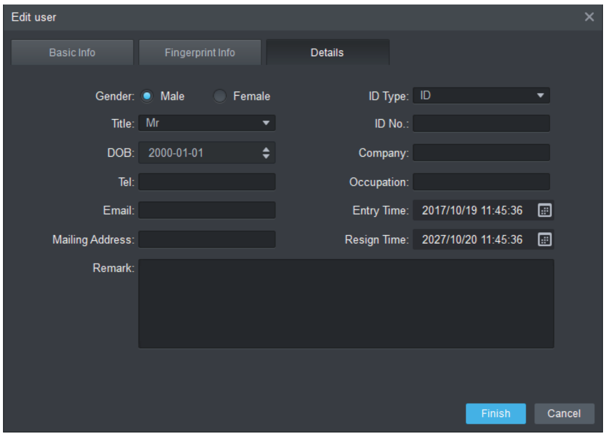
Fingerprint Device: B Fingerprint Reader(V2)

Successfully collect

Three Finger Collect....

Fingerprint1

Select the details tab to enter additional user information such as Gender, Title, DOB & contact information. It is also possible to enter specific times that the user can access areas.


Edit user

Gender: ● Male ○ Female

Title: Mr

DOB: 2000-01-01

Tel:

Email:

Mailing Address:

Remark:

ID Type: ID

ID No.:

Company:

Occupation:

Entry Time: 2017/10/19 11:45:36

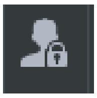
Resign Time: 2027/10/20 11:45:36

Once all the relevant user information has been entered, select the **Finish** button to save the user.

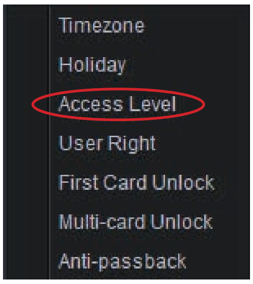
Access Levels

Before assigning user access, all doors must be added to a door list. The door list groups doors together so users can be granted access to a single door list or multiple lists.

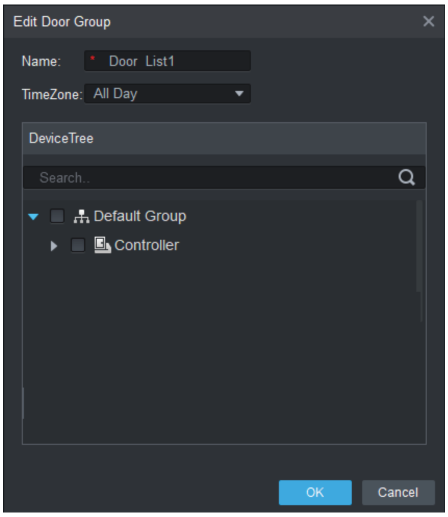
Select the access menu icon.



From the dropdown menu, select Access Level.



Click the add button to create a new door list.
Enter a name for the doorlist, a timezone can also be selected to limit access to specific times. Timezones must first be configured by selecting **Timezone** from the access menu.



Edit Door Group

Name: * Door List1

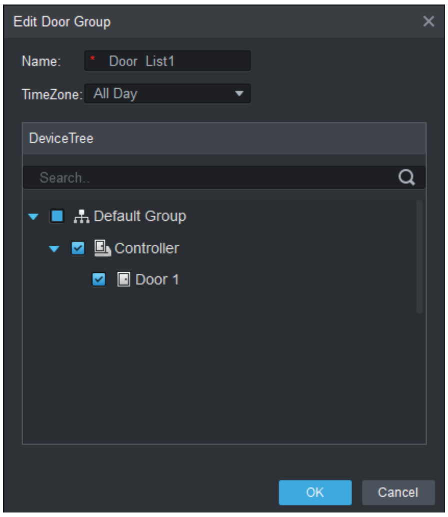
TimeZone: All Day

DeviceTree

Search..

- □ Default Group
  - □ Controller

Select the controllers and doors that are to be added to the list, click **OK** to save the list.



Edit Door Group

Name: * Door List1

TimeZone: All Day

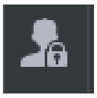
DeviceTree

Search..

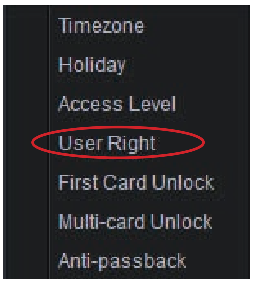
- ■ Default Group
  - ☑ Controller
    - ☑ Door 1

Now that the doors have been assigned to a list, it is possible to assign user access.

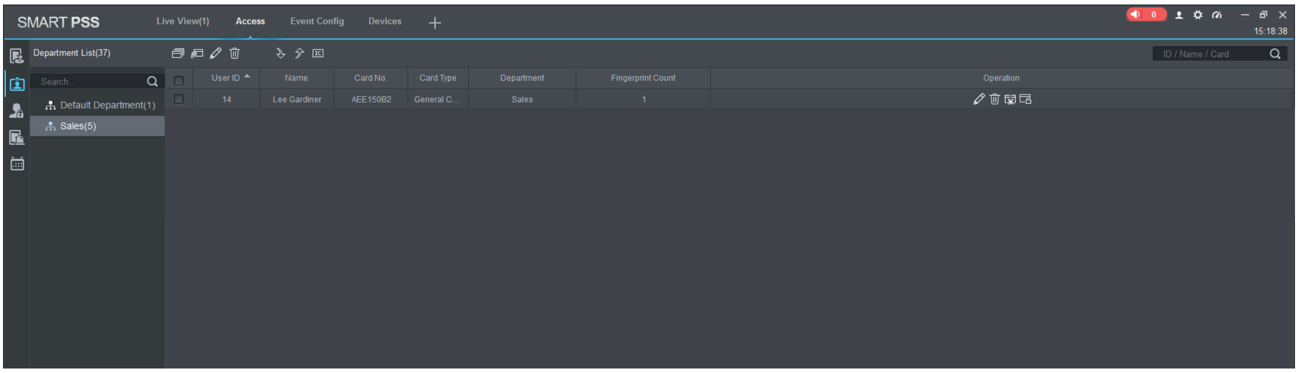
Select the access menu icon.



From the dropdown menu, select **User Right.**

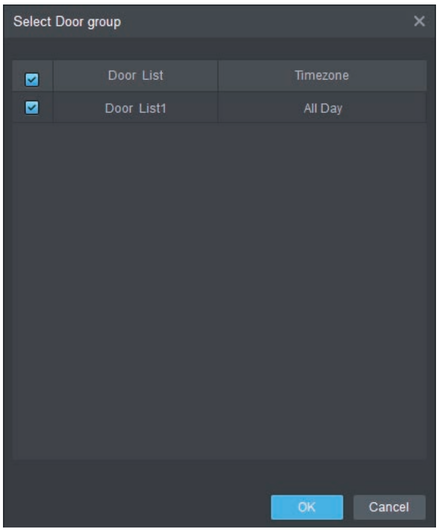


Select a department from the left window pane to display the users from that department, click on the ✎ icon to adjust the users access rights.



□	User ID	Name	Card No.	Card Type	Department	Fingerprint Count	Operation
□	14	Lee Gardiner	AEE150B2	General C...	Sales	1	✎

Select which doors the user shall have access to by select the applicable door lists. Click **OK** to save the setting.



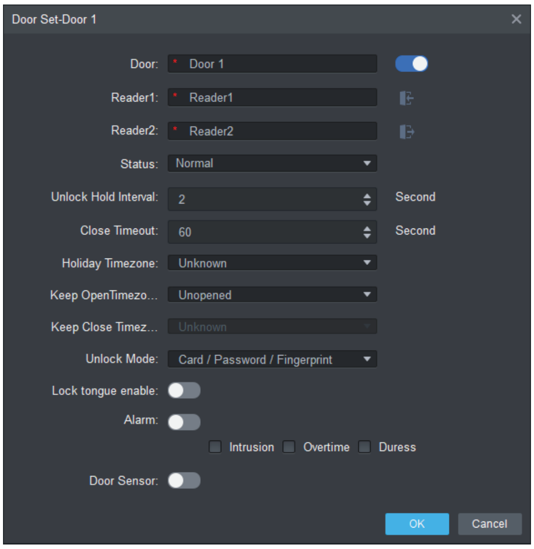
☑	Door List	Timezone
☑	Door List1	All Day

Door Configuration

There are multiple parameters that can be adjusted when configuring the operating mode of each door.

Select the console icon.

From the left window pane, right click the door to configure and select **Door Configuration**



Door Set-Door 1

Door: * Door 1

Reader1: * Reader1

Reader2: * Reader2

Status: Normal

Unlock Hold Interval: 2 Second

Close Timeout: 60 Second

Holiday Timezone: Unknown

Keep OpenTimezo... Unopened

Keep Close Timez... Unknown

Unlock Mode: Card / Password / Fingerprint

Lock tongue enable:

Alarm:

□ Intrusion □ Overtime □ Duress

Door Sensor:

Door Door name.

Reader 1 First readers name and direction. Click direction icon to toggle between enter or exit.

Reader 2 Second readers name and direction. Click direction icon to toggle between enter or exit.

Status Change operating mode, options are Normal, Always Open, Always Closed.

Unlock Hold Interval The amount of time in seconds that the relay output will trigger for.

Close Timeout When a door sensor is installed, this is the amount of time the door must be left open before an overtime event occurrs.

Holiday Timezone A timezone can be configured and selected here to create a specific time period where the door will remain locked such as weekends.

Keep Open Timezone A timezone can be configured and selected here to create a specific time period where the door will remain unlocked.

Keep Closed Timezone A timezone can be configured and selected here to create a specific time period where the door will remain locked.

Unlock Mode Select the operating mode of the door readers. It is possible to select a single authentication method supported by the reader or multiple.

Unlock Mode Examples

- Card/Password/Fingerprint would require only one of these methods be used to unlock the door.
- Card + Password would require that the user first scans their card, then enters their password before the door would unlock.

Alarm When a door sensor is installed, events can be configured to alert the operator of Smart PSS.

Intrusion Event that occurs if the door is forced open.

Overtime Event that occurs if the door is left open.

Duress Event that occurs if a user is under duress.

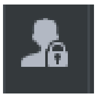
Door Sensor Select whether a door sensor is installed.

Anti-Passback

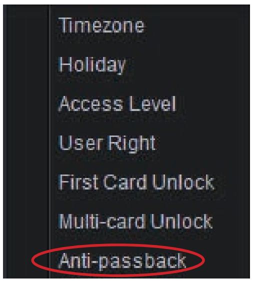
Anti-passback can be used to prevent users from passing their card back to a second user or tailgating behing another user when exiting an area (if tailgating, the user will be unable to regain access through the entrance as they will still be logged as in the area by the system).

To configure anti-passback follow the steps below:

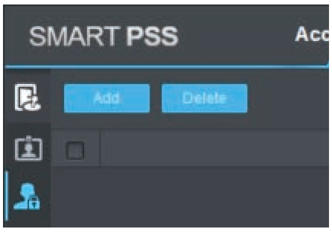
Select the access menu icon.



From the dropdown menu, select **Anti Passback.**



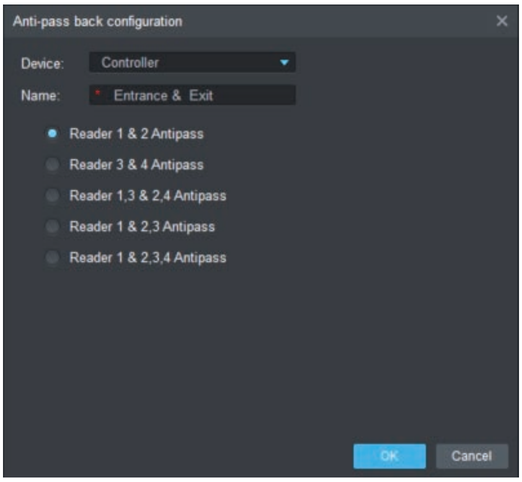
Click the **Add** button.



Select a controller from the dropdown list & enter a reference name.

Select the anti-passback configuration from the available options, click **OK** to save and apply the setting.

Reader 1 & 2 Antipass	Reader 1 enter, Reader 2 exit.
Reader 3 & 4 Antipass	Reader 3 enter, Reader 4 exit.
Reader 1,3 & 2,4 Antipass	Readers 1 & 3 enter, Readers 2 & 4 exit.
Reader 1,3 & 2,4 Antipass	Readers 1 & 3 enter, Readers 2 & 4 exit.
Reader 1 & 2,3 Antipass	Reader 1 enter, Readers 2 & 3 exit.
Reader 1 & 2,3,4 Antipass	Reader 1 enter, Readers 2, 3 & 4 exit.



Anti-pass back configuration ×

Device: Controller

Name: * Entrance & Exit

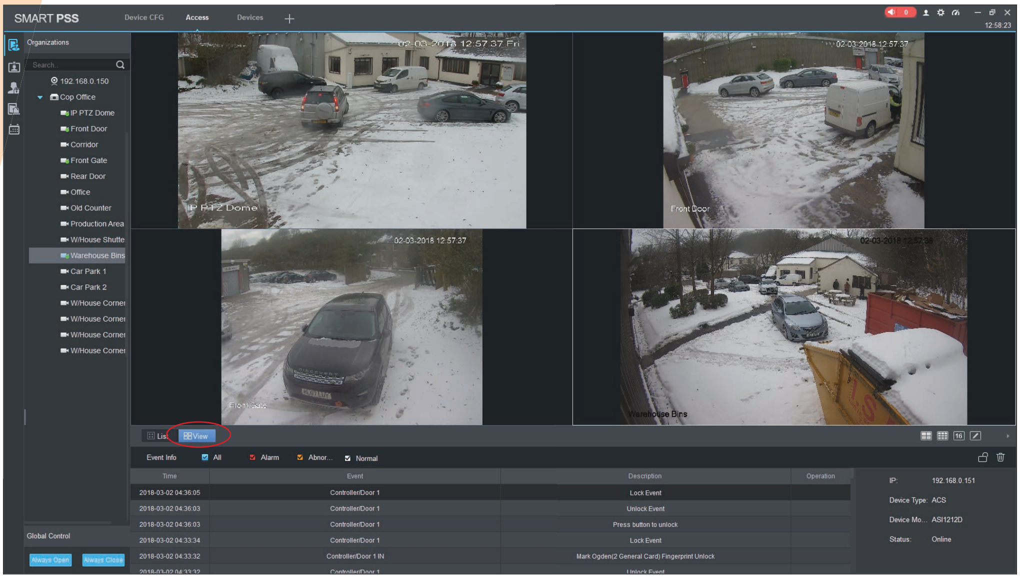
● Reader 1 & 2 Antipass
○ Reader 3 & 4 Antipass
○ Reader 1,3 & 2,4 Antipass
○ Reader 1 & 2,3 Antipass
○ Reader 1 & 2,3,4 Antipass

OK Cancel

INTEGRATION WITH CCTV

It is possible to integrate Dahua access control with Dahua CCTV products, enabling the ability to monitor both systems from a single platform.

Cameras can be monitored by selecting the **View** button from the access console page and selecting the cameras to view from the left window pane.



Time	Event	Description	Operation
2018-03-02 04:36:05	Controller/Door 1	Lock Event	
2018-03-02 04:36:03	Controller/Door 1	Unlock Event	
2018-03-02 04:36:03	Controller/Door 1	Press button to unlock	
2018-03-02 04:33:34	Controller/Door 1	Lock Event	
2018-03-02 04:33:32	Controller/Door 1 IN	Mark Ogden(2 General Card) Fingerprint Unlock	
2018-03-02 04:33:32	Controller/Door 1	Unlock Event	

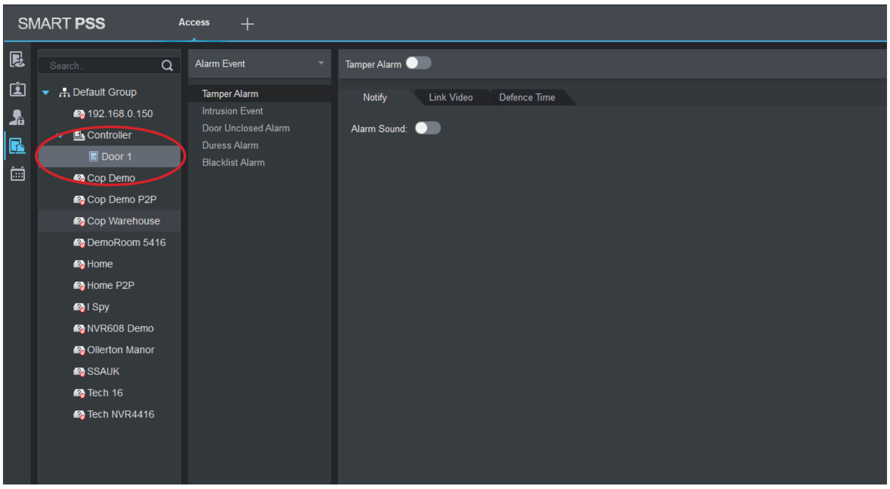
IP: 192.168.0.151
Device Type: ACS
Device Mo... ASI1212D
Status: Online

Push Events with Video

When incorporating Dahua access control and Dahua CCTV within SmartPSS, it is possible to configure access control events to push video alerts to the operator. This can be done by following the steps below.

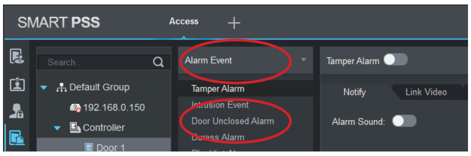
Select the event menu icon.

From the left window pane, select the controller and door that will push events.



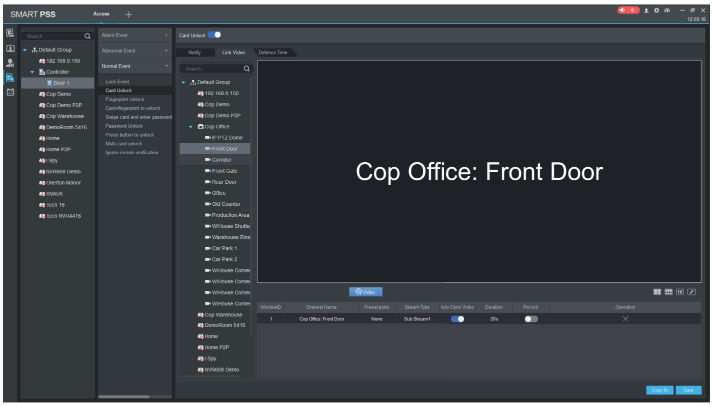
From the middle window pane select the event group such as Alarm Event, Normal Event or Abnormal Event. In the list that appears select the event type such as Unlock event, Intrusion event etc.

After selecting the event type, select the enable option at the top of the window and from the notify tab select whether SmartPSS should play a sound or not when the event occurs.



Alarm Sound: ○

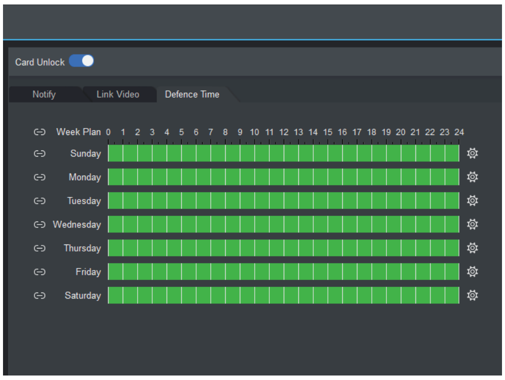
Select the link video tab and then choose which cameras should be pushed when the event occurs by double clicking on the cameras within the right window pane.



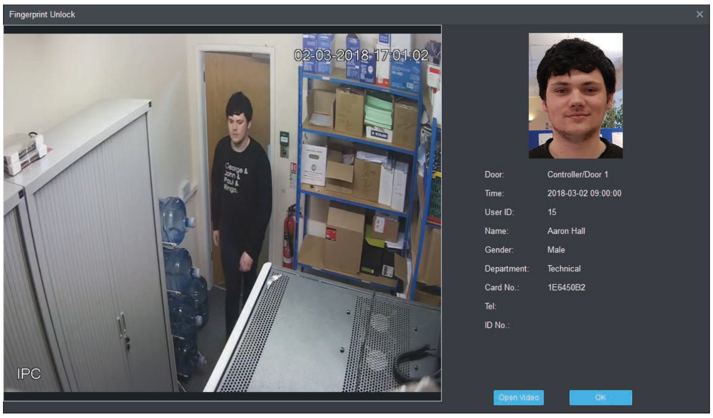
Card Unlock ●

WindowID	Channel Name	Preset point	Stream Type	Auto Open Video	Duration	Record	Operation
1	Cop Office: Front Door	None	Sub Stream1	●	20s	○	×

Select the defence time tab to set specific days and times that the push event should run. Once all settings have been configured click the **Save** button.



When the event occurs a pop up will appear when the event takes place displaying the user information.



Door: Controller/Door 1
Time: 2018-03-02 09:00:00
User ID: 15
Name: Aaron Hall
Gender: Male
Department: Technical
Card No.: 1E6450B2
Tel:
ID No.:

COP UK, Delph New Road, Dobcross, OL3 5BG England