



Access Control

FAQ Manual



Foreword

General

This manual provides solutions and instructions for common device faults, parameter settings, and typical ways the device is misused.

The instructions in this manual need to be analyzed according to the actual situation, and are not the only solution. If you have any questions, contact the technical support.

Safety Instructions

The following signal words might appear in the manual.

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

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	January 2025

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, audio, fingerprints, and license plate number. You need to be in compliance with your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures which include but are not limited: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.

- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.
- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Table of Contents

Foreword.....	I
1 Access Controller Problems.....	1
1.1 The default IP, port, account and password of the first generation access controller (ASI1XXX).....	1
1.2 The changed IP of the access controller is forgotten.....	1
1.3 Modifying the device IP.....	2
1.4 Restoring the access controller to the factory settings.....	2
1.5 Updating the access controller.....	3
1.6 Wiring of the access controller with the magnetic locks.....	3
1.7 Wiring of the access controller with the card reader.....	4
1.8 Wiring between the door station, access controller, and the lock.....	5
1.9 Connecting the door sensor feedback to the access controller.....	5
1.10 Wiring of the access controller for fire linkage.....	6
1.11 Card Reader determines the card type.....	7
1.12 Configuring duress card, password and fingerprint.....	7
1.13 The duress card of the access controller cannot open the door.....	8
1.14 The card cannot open the door after permissions are sent.....	8
1.15 The suffix -D and -S of the access controller name.....	9
1.16 Using the access control devices for attendance.....	9
1.17 Main board of the access controller (model C) keeps beeping.....	9
1.18 The access controller goes online and offline irregularly.....	10
1.19 Achieving multi-door interlock of the access controller	10
1.20 Person permissions of the access controller lost.....	11
1.21 Wiring of the access controller with the electric lock.....	11
1.22 Swiping the card once and the event is reported twice on the platform.....	11
1.23 Using the user ID to unlock, and the access controller (with the second generation protocol) prompts correct ID and wrong password.....	12
1.24 The default IP, port, account and password of the access controller (with the second generation protocol).....	12
1.25 Time synchronization fails on the access controller.....	12
1.26 Getting the card reader version.....	12
1.27 Fingerprint is available on one card reader after the access controller is connected to 4 card readers.....	13
1.28 When the platform sends the person information, the auto registered access controller goes offline.....	13
2 Access Standalone Problems.....	14
2.1 Using ASI1212A as the card reader.....	14
2.2 Using ASI1201A as the card reader to connect to the access controller.....	14
2.3 Access standalone fails to update.....	14

2.4	Updating ASI1212D through USB.....	14
2.5	Using A300 series as the card reader to connect to access controller.....	15
2.6	After the unlock mode is configured as password, password in ASI1212D cannot open the door.....	15
2.7	ASI1201E fails to send the card information through the platform.....	15
3	Face Recognition Access Controller Problems.....	16
3.1	ASI4214F and ASI6214F cannot send the face information.....	16
3.2	Images cannot be sent on the face recognition access controller.....	16
3.3	No face recognition function.....	17
3.4	Faces cannot be recognized to open the door.....	17
3.5	When used with the access controller, card verification cannot open the door.....	17
3.6	Device is too sensitive and starts recognizing faces from a long distance.....	18
3.7	Adjusting severe backlighting.....	18
3.8	Outdoor devices have fog inside the screen.....	19
3.9	There is no reaction after the USB is inserted.....	19
3.10	The password is forgotten.....	19
3.11	CGI command.....	19
3.12	Recognition screen has vertical stripes flickering issue.....	20
3.13	There is no output after the Wiegand is connected.....	20
3.14	The device fails to transfer the recognition records to IVSS after recognition.....	20
4	Other Devices Problems.....	21
4.1	Connecting the exit button to the access controller.....	21
4.2	Connecting the electronic sliding door to the access controller.....	21
4.3	Fingerprint card reader reports the unlock record under the sunshine.....	21
4.4	Attendance standalone is used with the platform or the software.....	21
4.5	The swing directions of the swing barrier (2 directions access) are the same when swiping the card in 2 sides.....	21
4.6	The added person cannot be found when sending the door group permissions in SmartPSS Lite.....	22
4.7	The consumption machine goes offline after it is added to the platform.....	22
4.8	There is no reaction and reported events after swiping the card on the card reader.....	22
4.9	The door cannot open after adding magnetic disk to the normal wired electric bolt lock.....	22
4.10	The lock strip detachment of the magnetic lock	22
4.11	The supported card type of the card reader.....	22
4.12	The IC card encryption rule and the NFC copied function.....	23
4.13	The valid card cannot open the door.....	23
4.14	The communication of the access control system is abnormal.....	23
4.15	The card reader cannot read the card.....	23
4.16	After the magnetic lock is suctioned, it vibrates and is not firm.....	24
4.17	Cards cannot be added to the DSS platform through ASM100-D.....	24
4.18	Fingerprints cannot be added to the DSS platform through ASM202.....	24

4.19 The suction plate is placed on the lock and the indicator turns red.....	24
4.20 Insufficient Magnetic Locking Force.....	25
4.21 The sub device goes offline on the integrated controller.....	25

1 Access Controller Problems

1.1 The default IP, port, account and password of the first generation access controller (ASI1XXX)

The default information of the first generation access controller (ASI1XXX) are as followings.

- The factory default IP: 192.168.0.2
- Port: 37777
- Account: admin
- Password: 123456

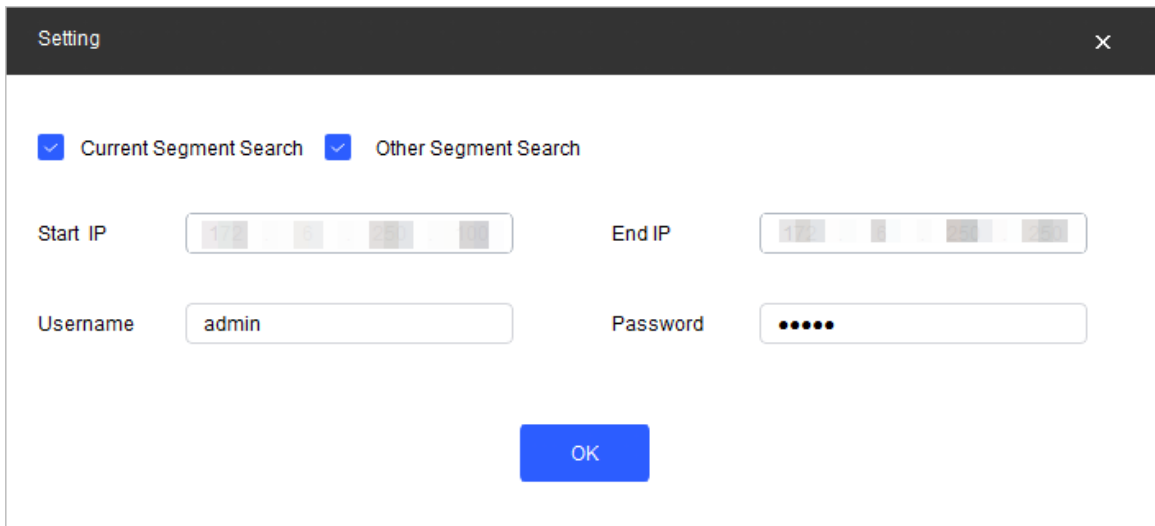
1.2 The changed IP of the access controller is forgotten

You can get the ConfigTool through <https://support.dahuasecurity.com/en/toolsDownloadDetails?IsDpValue=Q93jdSLr94chjRuQ1y%2FcQQ%3D%3D>.

- Use the access configuration tool ConfigTool to automatically search for the IP. Please contact technical support personnel to get the tool.

Open ConfigTool, click **Search Setting**, configure the IP segment, and then click **OK**. You can find the device through the device type, model, MAC address and more information.

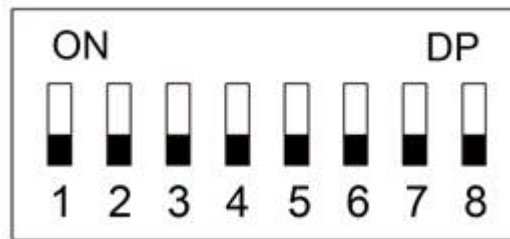
Figure 1-1 Auto search



- Restore the device to factory default settings and change the IP.

Restore the device to factory default settings by the DIP switch, and then configure the device IP.

Figure 1-2 DIP switch



: The switch is on, which represents 1.
 : The switch is off, which represents 0.

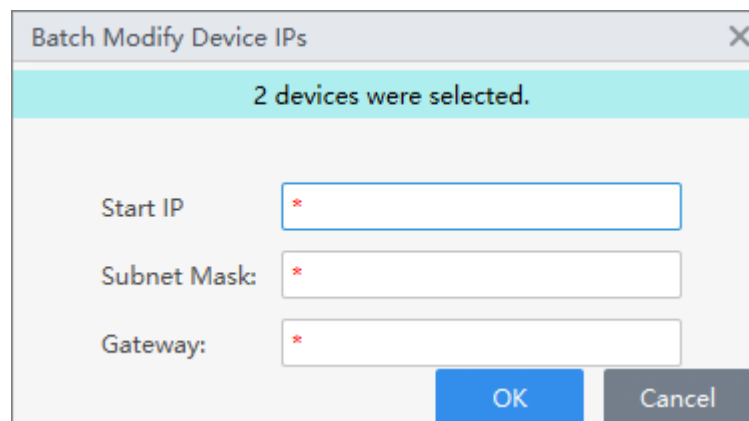
- ◇ If 1, 3, 5 and 7 are 1, and others are 0, the device is restored to factory settings after it restarts.
- ◇ If 2, 4, 6 and 8 are 1, and others are 0, the device is restored to factory settings after it restarts, but the user information will be kept.

1.3 Modifying the device IP

Procedure

- Step 1** Log in to SmartPSS Lite.
- Step 2** On the home page, click **Devices**.
- Step 3** Click **Auto Search**
- Step 4** Set the range of network segment, and then click **Search**.
- Step 5** Select devices, and then click **Change IP**.
- Step 6** Change the IP, subnet mask and gateway of the devices.

Figure 1-3 Change IP in batches



- Step 7** Click **OK**.

1.4 Restoring the access controller to the factory settings

- Single door access controller: Turn on switch 1 and 3. Power off and restart the device. Turn the switches off after you hear a beep sound.
- Double or four doors access controller: Turn on switch 1, 3, 5 and 7. Power off and restart the device. Turn the switches off after you hear a beep sound.

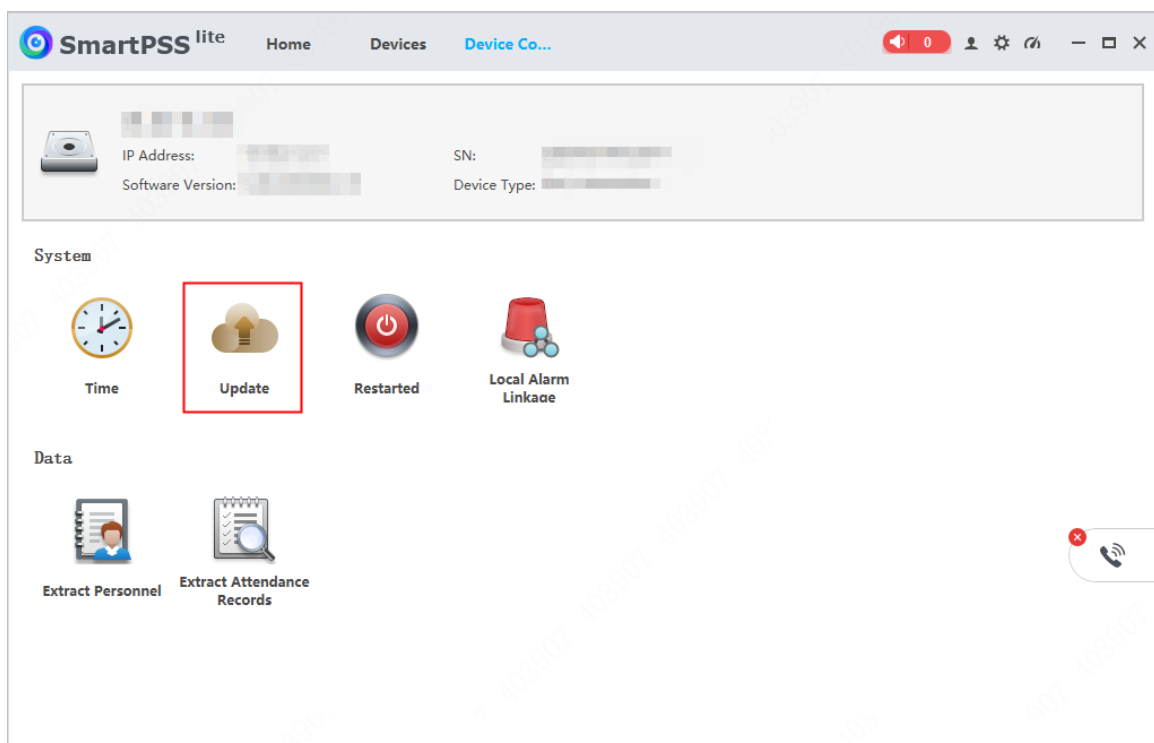
1.5 Updating the access controller

After obtaining the correct update file, update through SmartPSS Lite.

Procedure

- Step 1** Log in to SmartPSS Lite.
- Step 2** Select **Device Management**, and then add the device.
- Add the device by searching.
 1. On the **Device Management** page, click **Auto Search**.
 2. Configure the device IP segment, and click **Search**.
 3. Select the device that you want to add, and then click **Add**.
 - Add the device manually.
 1. On the **Device Management** page, click **Add**.
 2. Enter the device information, and click **Add**.
- Step 3** Click  next to the device.
- Step 4** Click **Update**.
- Step 5** Select the update file, and then click **Update**.

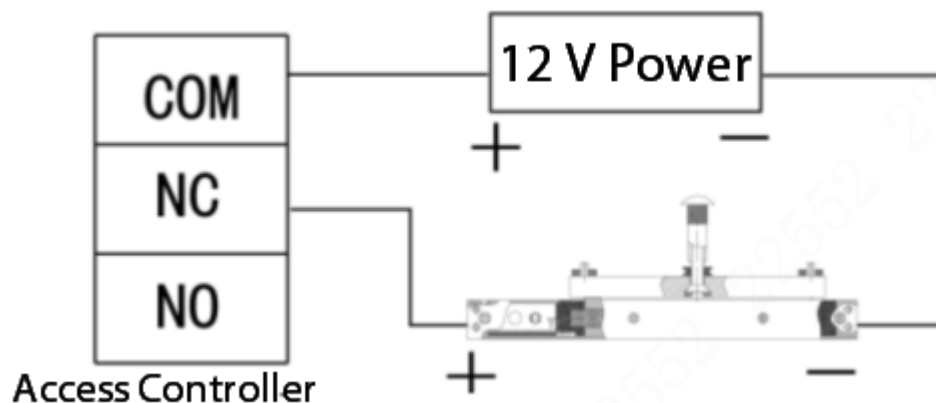
Figure 1-4 Update



1.6 Wiring of the access controller with the magnetic locks

Connect the positive side of the external power to the COM port of the access controller. Connect the NC port of the access controller to the positive side of the magnetic lock, and connect the negative side of the magnetic lock to the negative side of the 12 V power supply.

Figure 1-5 Wiring diagram



1.7 Wiring of the access controller with the card reader

One access controller can only be connected to one type of card reader. You can select RS-485 or Wiegand.

- Only connect to RS-485 cable: Red (12 V), black (GND), yellow (485-), purple (485+)
- Only connect to Wiegand cable: Red (12 V), black (GND), green (D0), white (D1).

Table 1-1 Wiring description

Cable Color	Port	Description
Red	12 V power	Card reader power
Black	GND	
Blue	CASE	Wiegand card reader
White	D1	
Green	D0	
Brown	LED	
Yellow	RS485-	RS-485 card reader
Purple	RS485+	



- The wiring standard of the network cable port is: White & orange (485+), orange (485-), white & green (LED), blue (D0), white & blue (D1), green (CASE), white & brown (GND), and brown (12 V +).
- We recommend that you use CAT5E or higher network cables for the wiring between card reader to the access controller. Use 4-core pure copper cables (RVV4 × 1.0) for the wiring between the access controller to the lock. The card reader with the distance over 100 meters needs independent power.

1.8 Wiring between the door station, access controller, and the lock

The door station and the access controller can be connected to the lock. If you successfully verify the identifications on the door station or the access controller, the lock opens. This section introduces one of the wiring methods.

Connect the positive side of the external power to the COM port of the access controller. Connect the NC port of the access controller to the COM port of the unit door station (VTO), connect the NC port of the unit door station to the positive side of the lock, and connect the negative side of the lock to the negative side of the external 12 V power.

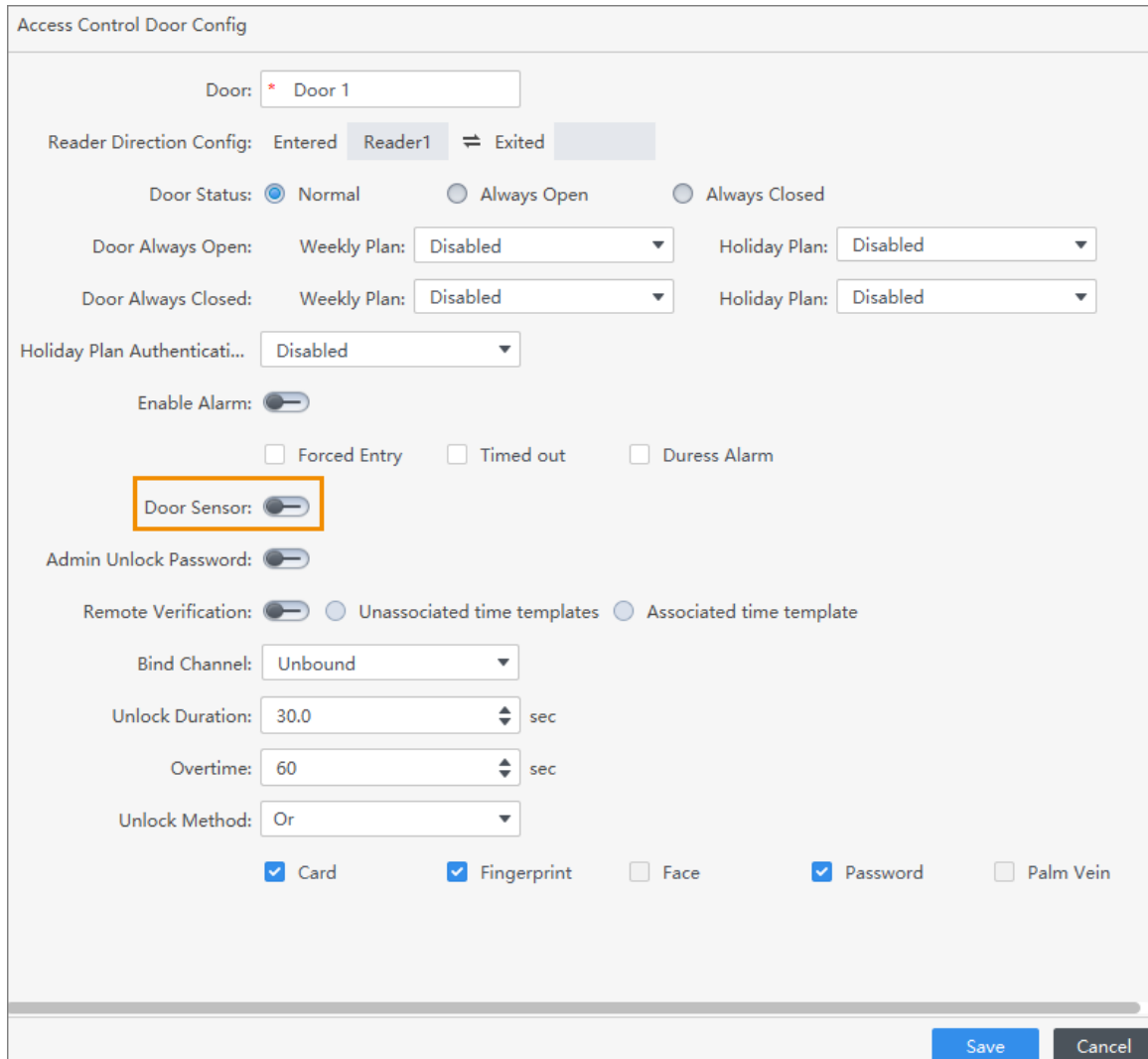
1.9 Connecting the door sensor feedback to the access controller

Connect the SR and GND port of the access controller, and make sure that the door detector function is enabled.

Procedure

- Step 1 Log in to SmartPSS Lite.
- Step 2 Select **Access Control Config > Door Parameters**.
- Step 3 Select a door and then enable **Door Sensor**.

Figure 1-6 Basic parameters

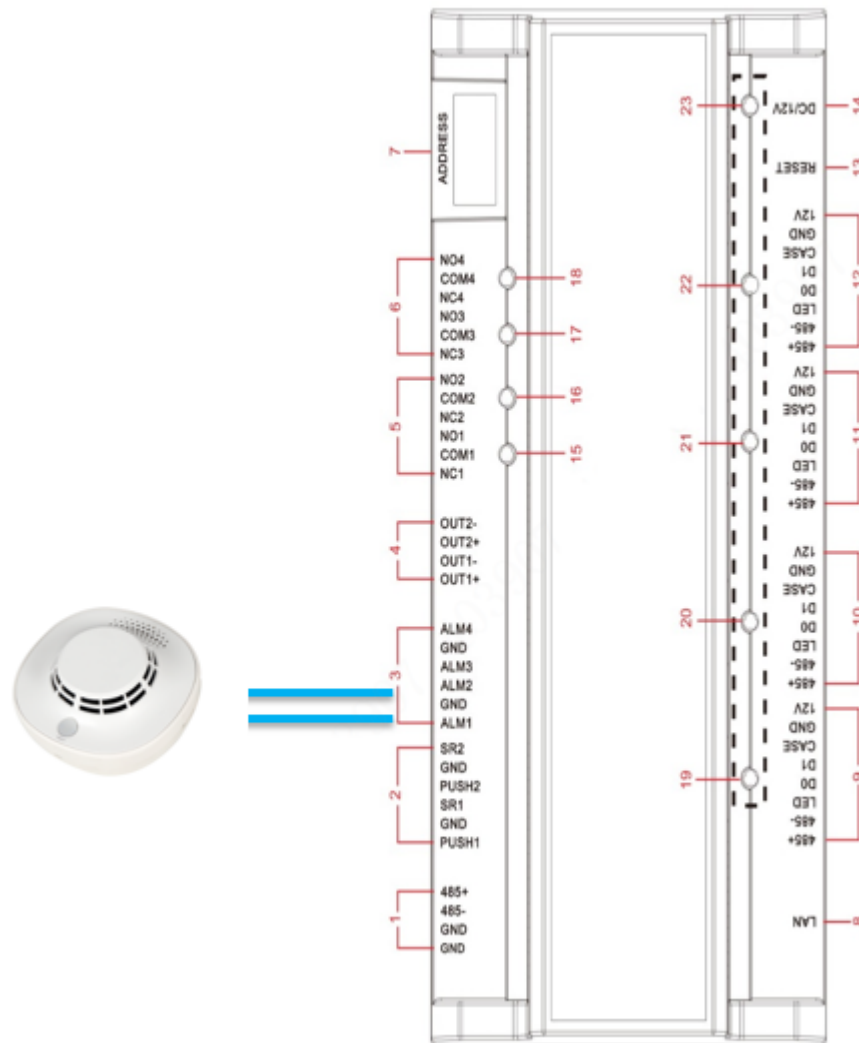


Step 4 Click **Save**.

1.10 Wiring of the access controller for fire linkage

Connect the alarm1 and GND ports of the access controller. When there is a signal input, all doors remain normally open.

Figure 1-7 Wiring diagram



1.11 Card Reader determines the card type

Refer to the model of the card readers to determine the card type. IC card is used by default. -D means ID card is supported, and -C means ID card is supported.

For example, if the model is ASR1100A. ASR1100A means IC card is supported. ASR1100A-D means ID card is supported.

1.12 Configuring duress card, password and fingerprint

When you add people in the software, set the card type as duress card. The corresponding fingerprint will be the duress fingerprint. Duress password is not supported by the baseline program.

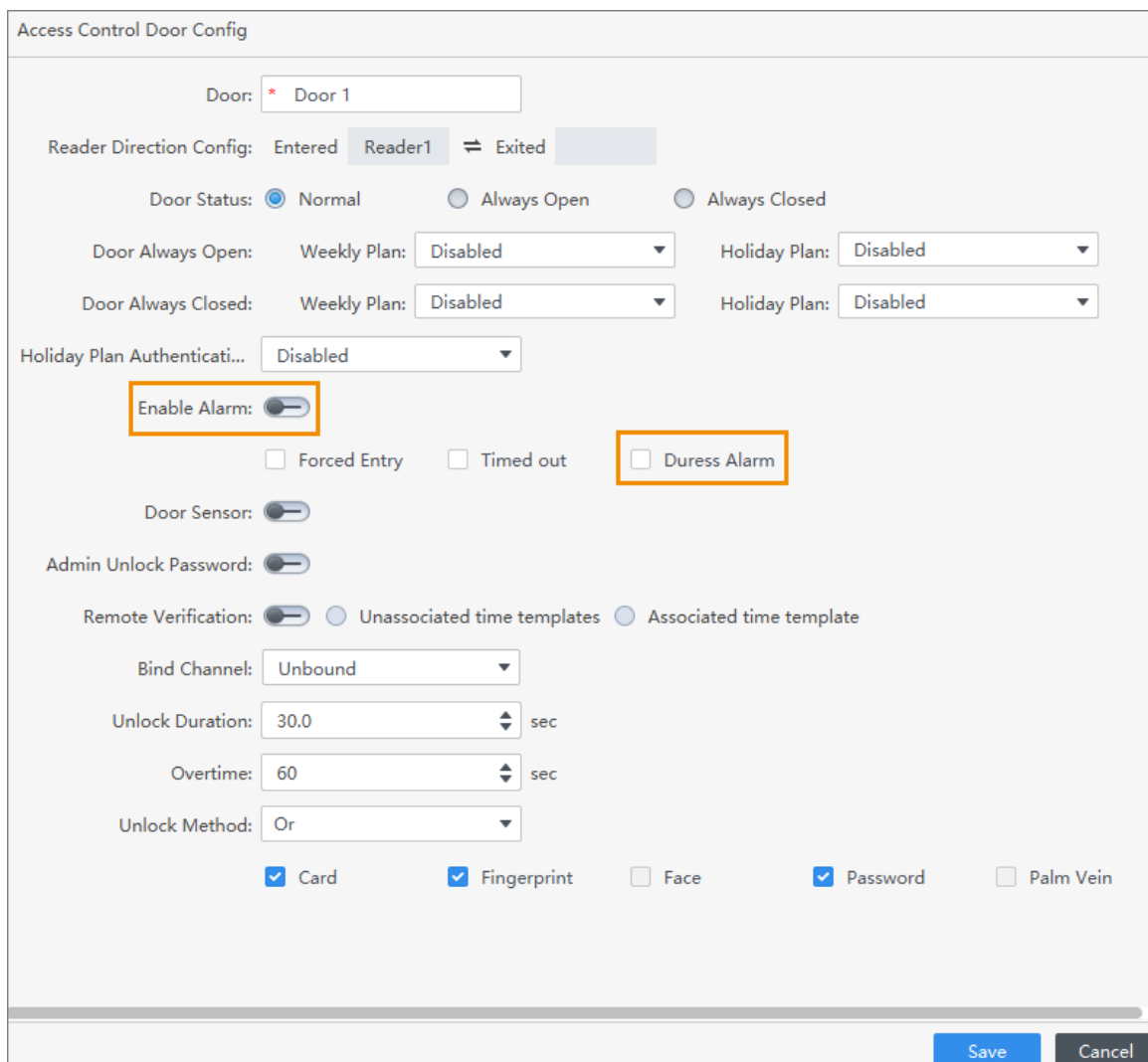
1.13 The duress card of the access controller cannot open the door

Set the card type as the duress card, and turn on alarms in door parameters configurations to unlock the door using the duress card and report the alarm information.

Procedure

- Step 1** Log in to SmartPSS Lite.
- Step 2** Select **Access Control Config > Door Parameters**.
- Step 3** Select a door, turn on **Enable Alarm**, and then select **Duress Alarm**.

Figure 1-8 Basic parameters



- Step 4** Click **Save**.

1.14 The card cannot open the door after permissions are sent

Procedure

- Step 1** Log in to SmartPSS Lite.

Step 2 Click **Access Control Monitoring** on the home page.

Step 3 View door status on **Event Info** list to troubleshoot.

- If there are no events, it means card reader wiring has problems. Connect the cables again or change the device.
- If there is event saying that the door is normally open, it means lock wiring has problems. Connect the cables again or change the device.
- If other events are reported, such as wrong card validity period or wrong open mode, troubleshoot according the description.

Figure 1-9 Event information

List

View

Event Info

All

Alarm

Abnormal

Normal

Event History

Event Config

Time	Device Name	Event Description
2024-09-03 19:14:40	1 Door 1	Reader Tamper Alarm
2024-09-03 19:14:07	10 Door 2	82 The card is not authorized or was reported lost.
2024-09-03 19:13:43	10 Door 2	111(1 Normal User) Not within Valid Period

IP:

1012

Device Type:

Access Controller

Model:

A-B

State:

Online

1.15 The suffix -D and -S of the access controller name

The suffix -D of the access controller name means the door can be opened in 2 directions.

The suffix -S of the access controller name means the door can be opened in the single direction.

1.16 Using the access control devices for attendance

Log in to SmartPSS Lite, select **Attendance Management**, and then configure the attendance points, person shifts, periods and more information. For details, see the corresponding user's manual.



- Up to 10 attendance points are supported.
- The attendance system uses the first and the last verification records of each day as the attendance records.

1.17 Main board of the access controller (model C) keeps beeping

Procedure

Step 1 Remove the red, black and yellow cables from 5 power supply cables, and retain the red and black cables.

Step 2 Check if the problem is solved.

If there is still the problem, contact the technical support personnel.

1.18 The access controller goes online and offline irregularly

Problem

After the access controller is added to the platform, it is sometimes online and sometimes offline.

Possible Causes

- There is an IP conflict.
- The switch is abnormal.
- The platform is abnormal.

Solutions

1. Modify the IP address of the device.

Modify the IP address of the device on DSS or through other methods.

2. Check if other devices in the same network segment are offline when the access controller is offline.

If other devices are offline, the switch is abnormal. Check the power supply, network and other problems. Otherwise, perform the following steps.

3. Add devices through SmartPSS Lite.

Log in to SmartPSS Lite, and then select **Device Management** to add devices.

- Add the device by searching.
 - a. On the **Device Management** page, click **Auto Search**.
 - b. Configure the device IP segment, and click **Search**.
 - c. Select the device that you want to add, and then click **Add**.
- Add the device manually.
 - a. On the **Device Management** page, click **Add**.
 - b. Enter the device information, and click **Add**.

4. Check if the problem is solved.

If the problem is solved, the platform is abnormal. Troubleshoot the platform problems. If there is still the problem, contact the technical support personnel.

1.19 Achieving multi-door interlock of the access controller

Procedure

- Step 1 Make sure that the door sensor feedback signal cable is connected to the SR and GND port of the access controller.
- Step 2 Enable **Door Sensor** in SmartPSS Lite.
- Step 3 Configure the interlock function between doors in SmartPSS Lite.

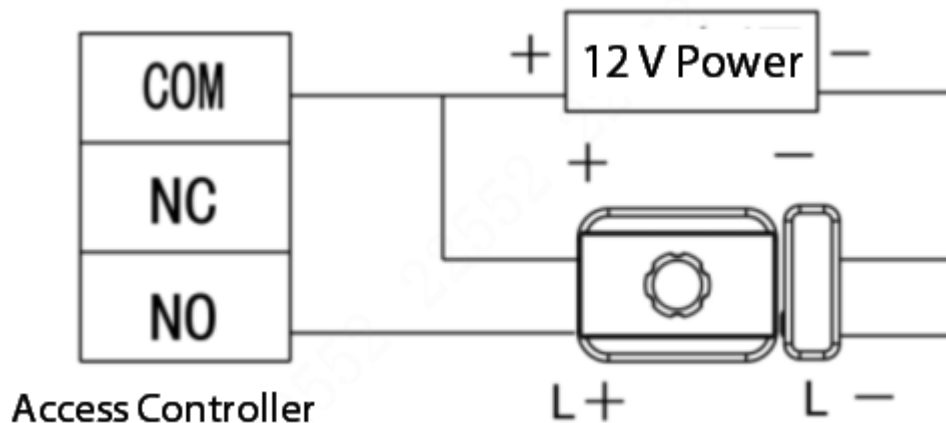
1.20 Person permissions of the access controller lost

Check whether the device program version is the latest. If not, update it to the latest baseline program first. On the SmartPSS Lite console, right-click the access controller and select **Extract Card Information** to check whether the person has the permission on the access controller.

1.21 Wiring of the access controller with the electric lock

Connect the positive side of the external power to the positive side of the electric lock. Connect the positive side of the external power to the COM port of the access controller. Connect the NO port of the access controller to the L+ port of the electric lock, and connect the L- of the electric lock to the negative side of the power.

Figure 1-10 Wiring diagram



1.22 Swiping the card once and the event is reported twice on the platform

Problem

The event is reported twice on the platform when the card is swiped just once on the access controller.

Possible Causes

The connection between the card reader and the access controller is abnormal. The RS-485 and Wiegand cables are connected at the same time, and the person information is reported twice when the card is swiped for verification.

Solutions

Remove RS-485 or Wiegand cable.

1.23 Using the user ID to unlock, and the access controller (with the second generation protocol) prompts correct ID and wrong password

Problem

When person ID is used to unlock the door on the access controller (with the second generation protocol), enter ID and # without the password, and the device prompts that the ID is correct, but the password is wrong.

Possible Causes

The cable connection between the card reader and the access controller (with the second generation protocol) is incorrect. RS-485 and Wiegand cables are connected at the same time, resulting in ID and # being sent twice, so that an error is reported.

Solutions

Remove RS-485 or Wiegand cable.

1.24 The default IP, port, account and password of the access controller (with the second generation protocol)

The default information of the access controller (with the second generation protocol) are as followings.

- The factory default IP: 192.168.1.108
- Port: 37777
- Account: admin
- Password: admin123

1.25 Time synchronization fails on the access controller

You need to update the access controller to the latest version if there is no custom function.

1.26 Getting the card reader version

Connect the card reader to the access controller to view the card reader version.

1.27 Fingerprint is available on one card reader after the access controller is connected to 4 card readers

Problem

When the access controller (with the first generation protocol) is connected to 4 external card readers (ASI1212D), after the person permissions are sent, people can swipe the card to open the door, but the fingerprint is only available on the card reader 1.

Solutions

Update the access controller (with the first generation protocol) to the latest baseline version if the ASI1212D version is 210802.

1.28 When the platform sends the person information, the auto registered access controller goes offline

Problem

If the access controller (with the second generation protocol) is automatically registered to the third-party platform, the device always goes offline when the platform is sending person information to the device.

Solutions

During the sending process, the platform needs to receive the response from the device first, and then send again.

2 Access Standalone Problems

2.1 Using ASI1212A as the card reader

You can use ASI1212A as the card reader. Use 485 protocol, connect the card reader port, and configure the working mode of the device as card reader mode.



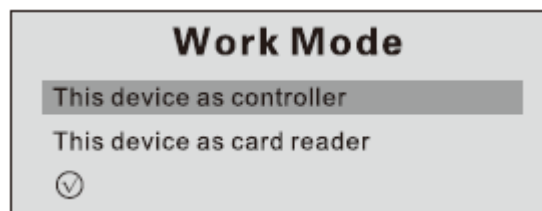
We recommend that the ASI1212A is powered separately.

Procedure

- Step 1** Use 485 protocol, connect the access standalone to the card reader port of the access controller.
- Step 2** Configure the working mode of the access standalone as card reader mode.
1. Log in to the home screen.
 2. Press $\uparrow$ or $\downarrow$ to select **System Settings**, and then press $\checkmark$.
 3. Press $\uparrow$ or $\downarrow$ to select **Mode Settings**, and then press $\checkmark$.
 4. Select **Work Mode** and then press $\checkmark$.
 5. Press $\uparrow$ or $\downarrow$ to select the work mode, and then press $\checkmark$.

After the selection is successful,  will be displayed next to the work mode.

Figure 2-1 Work mode



2.2 Using ASI1201A as the card reader to connect to the access controller

Currently, ASI1201A cannot be used as the card reader to connect to the access controller.

2.3 Access standalone fails to update

Contact the technical personnel to get the correct update program, and then update again.

2.4 Updating ASI1212D through USB

Procedure

- Step 1** Rename the update file as **AutoUpDate.bin**, save it in USB root directory, and then insert USB into the device.

Step 2 On the main menu, select **Settings** , and then tap **OK**.

Step 3 Select **USB Upgrade** , and then tap **OK**.

Step 4 Press **↑** or **↓** to select **Yes**, and then tap **OK**.

The system starts to update, and it will restart automatically when updating is complete.

2.5 Using A300 series as the card reader to connect to access controller

Procedure

Step 1 Use the Wiegand protocol, and then connect the access control devices to the access controller.



Access control devices must be grounded together with the access controller.

Step 2 Convert the decimal person ID in the access control device to hexadecimal (8 or 16) format, add it as the card number in the access controller, and then assign access permissions.

2.6 After the unlock mode is configured as password, password in ASI1212D cannot open the door

You can only use the public password to open the door. If you want to enter the individual password, you need to use the card together. The unlock mode is card and password.

2.7 ASI1201E fails to send the card information through the platform

When adding person on the platform for the access standalone of this model, the user ID length cannot exceed 8, and the first character cannot be 0.

3 Face Recognition Access Controller Problems

3.1 ASI4214F and ASI6214F cannot send the face information

The devices (ASI4214F and ASI6214F) are IR device, and cannot send the face information directly through face images.

Procedure

- Step 1 Register faces on the device.
- Step 2 Use SmartPSS Lite to extract the features on one device, and then send the information to the other device.
- Step 3 Use the USB to export the data from one device, and then import the data to the other device.

3.2 Images cannot be sent on the face recognition access controller

Procedure

- Step 1 Check the information. Make sure that you select the correct model when adding the device to the platform.
- Step 2 Select the image in the jpg format.



Some images may have a .jpg suffix, but they are not actually in JPG format. Use the software to save them as JPGs. Directly changing the suffix won't work. The image must be less than 100 kB and should clearly show the face, occupying less than 2/3 of the frame.

Figure 3-1 Head position



Figure 3-2 Face distance



3.3 No face recognition function

When the face recognition access controller does not have the face recognition function, perform the following steps.

Procedure

- Step 1 Restore to the factory settings on the webpage of the device, power off, and then restart the device.
- Step 2 Print logs to check whether the face algorithm has expired. If it is expired, contact the technical support to apply for the license.

3.4 Faces cannot be recognized to open the door

Procedure

- Step 1 Check whether the face image has been sent to the device.
- Step 2 Check whether the unlock method includes unlock by face. Check the face recognition period settings and whether the time is within the configured valid period for face recognition.
- Step 3 Check whether the face image is blurry and whether it is not similar to the actual face.
- Step 4 Change the recognition threshold to 85 on the device webpage.
- Step 5 Check the information reported to the platform.
- Step 6 Use the multimeter to detect whether the device normally outputs switch quantity signals.
- Step 7 Print device logs for analysis, and provide the face image and video stream during the recognition.

3.5 When used with the access controller, card verification cannot open the door

Procedure

- Step 1 Go to the management background of the device.

- Step 2 Select **Communication Settings** > **Serial Port Settings** > **Serial Port Output**, change the serial port input to serial port output.
- Step 3 Grant person permissions to the face recognition access controller and the access controller.

3.6 Device is too sensitive and starts recognizing faces from a long distance

On the face detection page of the device webpage, adjust the pupillary distance and draw the target detection area.

3.7 Adjusting severe backlighting

Log in to the webpage of the device and adjust the parameters.



The original 7-inch and 10-inch face recognition access controller do not have the second IR channel. Just configure the parameters for the first channel.

Outdoor Scenes with Sunlight

- Face parameters: Enable face exposure and set the face exposure interval detection as 10 seconds.
- Video configurations.
- First channel (color): Set the image WDR level to 50.
- Second channel (IR): Set the image WDR level to 50, and set exposure compensation to 50.

Semi-indoor Scenes with Strong Backlight

- Face detection: Enable face exposure and leave the other settings as default.
- Video configurations.
 - ◇ First channel (color): Set the image WDR level to 50, and set exposure compensation to 70–80.
 - ◇ Second channel (IR): Enable backlight compensation, and set exposure compensation to 65–75.

Indoor Scenes

- Face parameters: Use the default settings.
- Video configurations.
 - ◇ First channel (color): Use the default settings.
 - ◇ Second channel (IR): Set the image WDR level to 50, and set exposure compensation to 50.

3.8 Outdoor devices have fog inside the screen

This phenomenon is caused by a large temperature difference. After the device has been powered on and running for a while, it will automatically defog. Subsequent devices have improved and optimized this issue.

3.9 There is no reaction after the USB is inserted

Check the USB. We recommend using a USB drive formatted as FAT32.

3.10 The password is forgotten



The password refers to webpage login password or the password that is used to add the device to the platform.

- Go to the background of the device, restore the device to default settings, and then configure the password again.
 - ◇ For example, if you forget the password of ASI1212D, enter the admin password (88888888 by default) to go to the device background, restore the device to default settings, and then configure the password again.
 - ◇ If you forget the password of the 7-inch or 10-inch face recognition access controller, enter the admin password, swipe the card or use the face of the administrator to go to the device background, restore the device to default settings, and then configure the password again.
- Use the tool to restore the device to default settings, and then configure the password again.
- Reset the password through the provided e-mail address.

For example, if you forget the password of the 7-inch or 10-inch face recognition access controller, enter the IP address in the browser, go to the login page, scan the QR code, and then reset the password through the provided e-mail address.

- Contact the technical support personnel to solve the problem.

3.11 CGI command

You can enter the CGI command in the browser to directly modify the parameters of the device. The computer and the device must be on the same network.



The device IP should be the IP address of the actual device. The last value should be the value to be modified or searched. Enter the command, press the Enter key, and there is the pop-up window. You need to enter the user name and password of the device.

- Function: Enable SSH for access control devices (true is on, and false is off).

CGI command: `http://device IP/cgi-bin/configManager.cgi?action=setConfig&SSHD.Enable=true`

- Function: Modify screen off time.

CGI command: `http://device IP/cgi-bin/configManager.cgi?action=setConfig&GUISet[0].LCDCloseTime=30`

- Function: Search for information such as card numbers of one user.

CGI command: `https://device IP/cgi-bin/recordFinder.cgi?action=find&name=AccessControlCard&condition.UserID=User ID`

- Function: Search whether a user has face image registered.

CGI command: `http://device IP/cgi-bin/recordFinder.cgi?action=find&name=FaceEigenValue&condition.StrFilePath=/mnt/appdata/FaceImage/user ID.jpg`

3.12 Recognition screen has vertical stripes flickering issue

Problem

On the recognition screen of the face recognition access controller, there are vertical stripes flickering.

Possible Causes

The poor quality of the extension cable increases the impedance, resulting in insufficient voltage reaching the device, which leads to malfunctions.

Solutions

If the power need to be modified on the site, the voltage at the end should be measured to ensure it is 12 V.

3.13 There is no output after the Wiegand is connected

Problem

There is no output after the Wiegand is connected

Possible Causes

The GND is not connected.

Solutions

Connect 4 cables for the Wiegand: D0, D1, LED and CASE.

3.14 The device fails to transfer the recognition records to IVSS after recognition

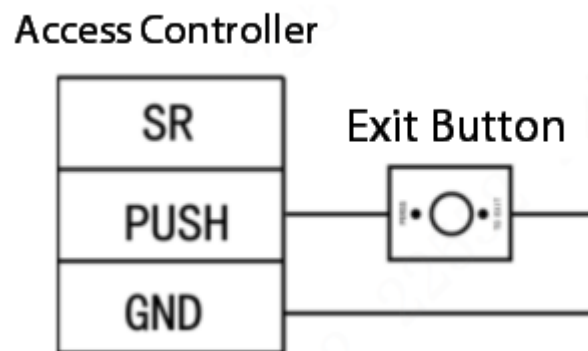
The baseline device supports reporting to the platform after the device comparison is completed, specifically reporting the access control event. However, what is needed on-site is for the device to report to the platform as soon as it captures a face, which requires reporting the face detection event. This needs to be supported through customization.

4 Other Devices Problems

4.1 Connecting the exit button to the access controller

Connect PUSH and GND ports of the access controller.

Figure 4-1 Wiring diagram



4.2 Connecting the electronic sliding door to the access controller

The electric sliding door uses 220 VDC power supply. Connect the positive and negative lines of the unlock signal of the electric sliding door in series to the COM port and NO port of the access controller.

4.3 Fingerprint card reader reports the unlock record under the sunshine

The recognition performance of the optical fingerprint module is affected in strong sunlight. Adjust the installation environment or contact technical support.

4.4 Attendance standalone is used with the platform or the software

The attendance standalone can be used with the platform or the software.

4.5 The swing directions of the swing barrier (2 directions access) are the same when swiping the card in 2 sides

The cable connection of the access control card reader is incorrect.

To follow the right hand swiping principle, 2 card readers should be connected to the card reader 1 and the card reader 3.

4.6 The added person cannot be found when sending the door group permissions in SmartPSS Lite

The permission is bound to the card number. You need to fill in the card number before sending the permissions.

4.7 The consumption machine goes offline after it is added to the platform

You can only set the subnet mask as 255.255.255.0. Other subnet masks are not supported. Otherwise, the device will go offline and lost the packages.

4.8 There is no reaction and reported events after swiping the card on the card reader

Procedure

- Step 1 Reconnect the card reader by referring to the corresponding installation guide.
 - Step 2 Use the voltmeter to detect the voltage at both ends of the card reader. Make sure that the voltage at both ends is above 10 V.
 - Step 3 Check if the problem is solved.
- If there is still the problem, contact the technical support personnel.

4.9 The door cannot open after adding magnetic disk to the normal wired electric bolt lock

The wiring for the ASF809 differs from that of the regular electric lock. It requires the door opening signal to be connected in series with the 12V power supply and the COM and NO ports of the access controller. Therefore, the ASF809 locks when powered on and unlocks when powered off.

4.10 The lock strip detachment of the magnetic lock

- Decrease the closing speed of the door closer to slow down the contact of the door and lock. If the door and lock collide for a long time, the lock screws will be loosened.
- Move the mounting position of the lock strip backward.
 1. Fix the suction plate, and close the door.
 2. Determine the installation position of the lock body and the lock plate, and then mark the position.
 3. Move the lock strip backward to avoid collision between the lock plate and lock body.

4.11 The supported card type of the card reader

You can know the supported card type from the model name. -D means ID cards are supported. -C means CPU cards are supported. If no suffix exists, it means IC cards are supported.

- Supports ID cards (with -D): ASR1102A-D, ASR2102A-D.

- Supports IC cards (without suffix): ASR1102A, ASR2102A.

4.12 The IC card encryption rule and the NFC copied function

Currently, the IC cards are not encrypted for factory status and can be copied using the NFC feature on the phone. If security is a concern, the program can be customized to upgrade both the card issuer and reader.

Once encrypted, the contents of the card sectors cannot be copied. The card sectors must match the reader sectors for access, effectively preventing duplication.

4.13 The valid card cannot open the door

- Check whether the administrator has set the normally closed mode or if it is in the normally closed period.
- Check whether the electric lock is normal, and check the power supply or replace the electric lock.
- Check whether the deadbolt and lock catch are mechanically stuck. Fix the mechanical failure or replace the parts.
- Check whether the communication between the access controller and the module is normal by viewing the indicator light on the control board.
- Check whether the power supply of the card reader is normal. Replace the power supply cord or supply the power separately.
- Check whether the card reader is normal. If the card reader is abnormal, replace it.
- Check whether the communication between the card reader and the access controller is normal. If it is abnormal, replace the communication cable.
- Check whether the access control configuration is set and advanced time template configuration such as first-card unlock, multi-user combination unlock, anti-passback and multi-door interlock is enabled.
- Check whether the operator has initialized the access control system or canceled the access card permission through other commands.

4.14 The communication of the access control system is abnormal

- Check whether the serial port is incorrectly configured. Confirm the used serial port.
- Check whether there is short circuit or open circuit in the access control communication cable.
- Check whether the RS-485 communication port is damaged.
- Check whether the network cable and Ethernet crystal head are intact, whether the network communication is blocked, and whether the network has delay, jitter, or packet loss.

4.15 The card reader cannot read the card

- Check whether the access control settings of the access controller take effect.
- Check whether the validity period of the card reader was configured when the IC card was being granted the permission. You can restore the validity period of the IC card permission to the default full day.

- Check whether the power supply of the card reader is normal and whether the line has a breakpoint.
- Check whether the card reader is normal. If the card reader is abnormal, replace it.
- Check whether the access controller works properly. If the access controller is abnormal, replace it.

4.16 After the magnetic lock is suctioned, it vibrates and is not firm

- Check whether the magnetic lock is firmly installed and whether the locking screws are loose.
- Check whether the suction surface of the magnetic lock and the lock plate have been completely sucked and there are no foreign objects.
- Check whether the voltage and current of the power adapter meet requirements.

4.17 Cards cannot be added to the DSS platform through ASM100-D

Currently, DSS baseline version does not support ID cards.

If the DSS platform supports ID cards, when adding people, select the card type, and then add the cards.

4.18 Fingerprints cannot be added to the DSS platform through ASM202

Problem

When ASM202 is connected to the PC installed with DSS, the system prompts that the driver is abnormal and that the registration failed when the fingerprint is added on the fingerprint adding page.

Solutions

Install the BRMICRO tool on the PC, and open the fingerprint scanner on the tool page. The device can be used normally.

To obtain the tool, please contact the technical support.

4.19 The suction plate is placed on the lock and the indicator turns red

Procedure

Step 1 Check whether the lock plate is placed on the black part of the lock body.

Figure 4-2 Lock



- Step 2** Use the multimeter to measure whether the voltage on both the V+ and V- sides is equal to or greater than 10 VDC.
- Step 3** Check if the jumper cap is properly inserted.
- Step 4** If the above items are normal, change the circuit board, and then test again.

For the dual-door magnetic lock, first turn off the power after it shows a green light when engaged. Then test the other side to see if it turns green. If it does, this indicates insufficient voltage. If it remains red, it means there is a problem with the circuit board, and the circuit board needs to be replaced.

4.20 Insufficient Magnetic Locking Force

Procedure

- Step 1** Check if the lock plate is positioned correctly.
- Step 2** Use the multimeter to measure whether the power supply voltage of the electric lock is equal to or greater than 9 VDC.
- Step 3** Check if the jumper cap is properly inserted or if it is loose.
- Step 4** Adjust the anti-detection so that it doesn't protrude too much; The lock plate should not be fixed too tightly and should use pin holes.

Figure 4-3 Lock plate



4.21 The sub device goes offline on the integrated controller

- Check if the sub-controller is connected in the cascade way. If it's not, change it to the cascade way.
- The baud rates of the main controller and sub-controller need to be set to be consistent.
- The ID of each sub-controller cannot conflict. Use the DIP switch to distinguish the ID.

- Perform time synchronization for the sub-controller on the webpage of the main controller.

ENABLING A SMARTER SOCIETY AND BETTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

Address: No. 1399, Binxing Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053

Email: dhoverseas@dhvisiontech.com | Tel: +86-571-87688888 28933188