Waterproof Standalone Access Terminal

Quick Start Guide

V.1.0.0

Foreword

General

This manual introduces the functions and operations of the Waterproof Standalone Access Terminal (hereinafter referred to as " Access Terminal").

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.
ESD	Electrostatic Sensitive Devices. Indicates a device that is sensitive to electrostatic discharge.
⚠ ELECTRIC SHOCK	Indicates dangerous high voltage. Take care to avoid coming into contact with electricity.
⚠ LASER RADIATION	Indicates a laser radiation hazard. Take care to avoid exposure to a laser beam.
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
V.1.0.0	First Release.	January 2022

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, 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.

Important Safeguards and Warnings

This section introduces content covering the proper handling of the Access Terminal, hazard prevention, and prevention of property damage. Read carefully before using the Access Terminal, comply with the guidelines when using it, and keep the manual safe for future reference.

Operation Requirements

⚠

- Check whether the power supply is correct before use.
- Do not unplug the power cord on the side of the Access Terminal while the adapter is powered on.
- Operate the Access Terminal within the rated range of power input and output.
- Transport, use and store the Access Terminal under allowed humidity and temperature conditions.
- Do not drop or splash liquid onto the Access Terminal, and make sure that there is no object filled with liquid on the Access Terminal to prevent liquid from flowing into it.
- Do not disassemble the Access Terminal without professional instruction.

Installation Requirements

⚠ WARNING

- Do not connect the power adapter to the Access Terminal while the adapter is powered on.
- Strictly comply with the local electric safety code and standards. Make sure the ambient voltage is stable and meets the power supply requirements of the Access Terminal.
- Do not connect the Access Terminal to two or more kinds of power supplies, to avoid damage to the Access Terminal.
- Improper use of the battery might result in a fire or explosion.

⚠

- Personnel working at heights must take all necessary measures to ensure personal safety including wearing a helmet and safety belts.
- Do not place the Access Terminal in a place exposed to sunlight or near heat sources.
- Keep the Access Terminal away from dampness, dust, and soot.
- Install the Access Terminal on a stable surface to prevent it from falling.
- Install the Access Terminal in a well-ventilated place, and do not block its ventilation.
- Use an adapter or cabinet power supply provided by the manufacturer.
- Use the power cords that are recommended for the region and conform to the rated power specifications.
- The power supply must conform to the requirements of ES1 in IEC 62368-1 standard and be no higher than PS2. Please note that the power supply requirements are subject to the Access Terminal label.
- The Access Terminal is a class I electrical appliance. Make sure that the power supply of the Access Terminal is connected to a power socket with protective earthing.

Table of Contents

Foreword I

Important Safeguards and Warnings III

1 Product Overview 1

1.1 Dimensions 2

1.2 Structure 2

2 Installation 3

3 Network Diagram 4

4 Wiring 5

5 Local Configuration 6

5.1 Main Menu 6

5.2 Changing Admin Password 6

5.3 Adding Users 7

5.4 Deleting Users 7

5.5 Configuring Unlock Modes 8

5.6 Configuring Door Open Duration 8

5.7 Configuring Working Modes 8

5.8 Configuring Door Sensor 9

5.9 Restoring to Factory Defaults 9

6 Smart PSS Configuration 10

6.1 Logging In 10

6.2 Adding Devices 10

6.2.1 Adding Individually 10

6.2.2 Adding in Batches 12

Appendix 1 Cybersecurity Recommendations 14

1 Product Overview

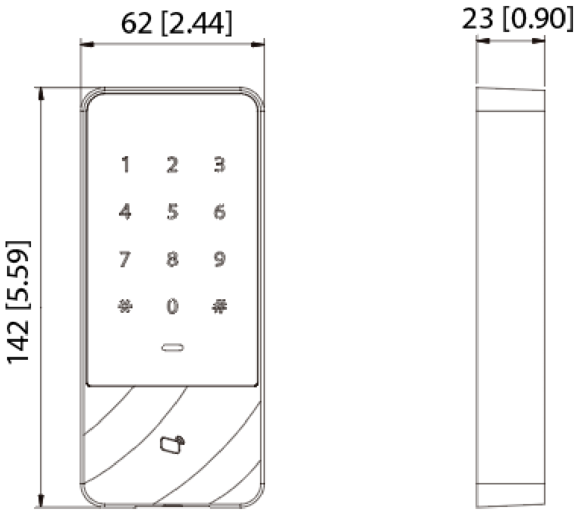
Waterproof standalone access terminal is intended for access management in a controlled area. With a neat appearance and IPX6 waterproof grade, it can be used outdoors.

It has the following main features:

- Supports touch keyboard and TCP/IP protocol.
- Support 30,000 valid cards and can store up to 60,000 records.
- Supports unlocking the door through card, card + password, and user ID + password.
- Supports overtime alarm, intrusion alarm, duress alarm, and tamper alarm.
- Supports guest card, duress card, blocklist/allowlist card, and patrol card.
- Support 128 groups of time schedules, 128 groups of period, and 128 groups of holiday period.

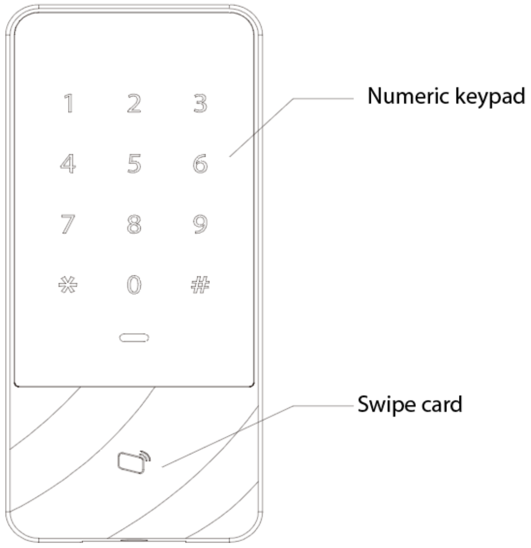
1.1 Dimensions

Figure 1-1 Dimensions (mm [inch])



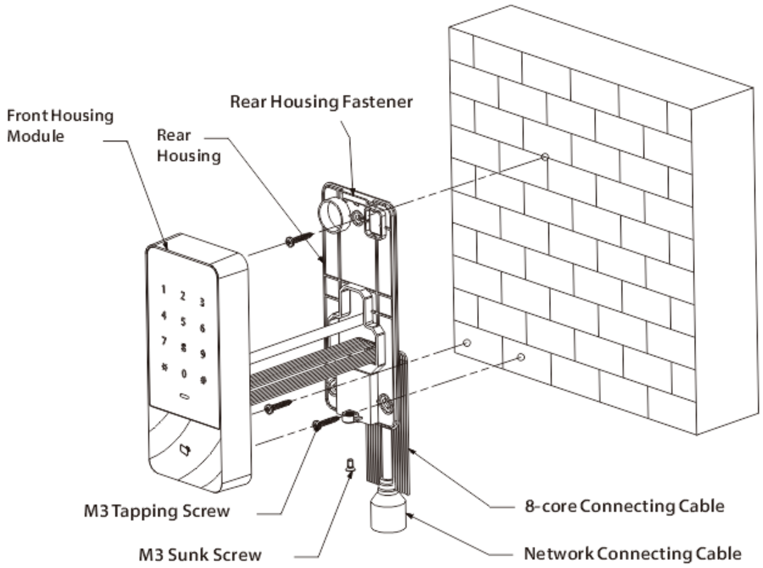
1.2 Structure

Figure 1-2 Structure



2 Installation

Figure 2-1 Installation



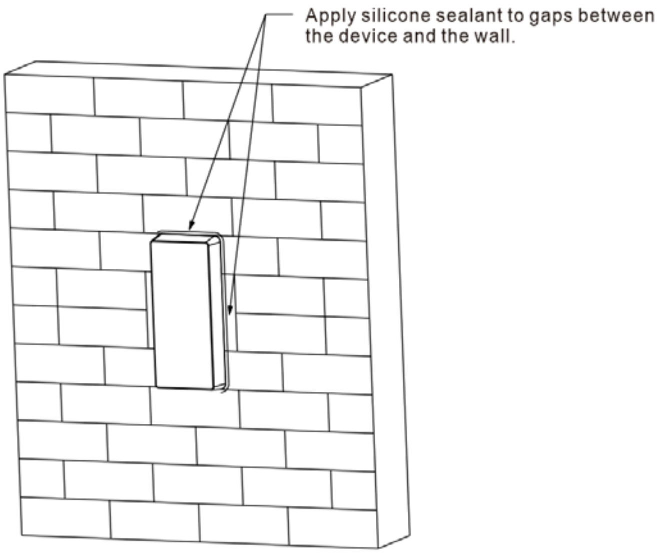
Step 1 Fix the rear housing onto the wall with M3 tapping screws; leave a wiring space for networking connecting cable between the rear housing and wall.

Step 2 Pass the network connecting cable and two 8-core connecting cable through the slot of the rear housing and wall, and then tighten M3 tapping screws.

Step 3 Attach the top of front housing module to the rear housing fastener, and then tighten the M3 sunk screws at the bottom to fix them.

Step 4 Apply silicone sealant to gaps between the Access Terminal and the wall.

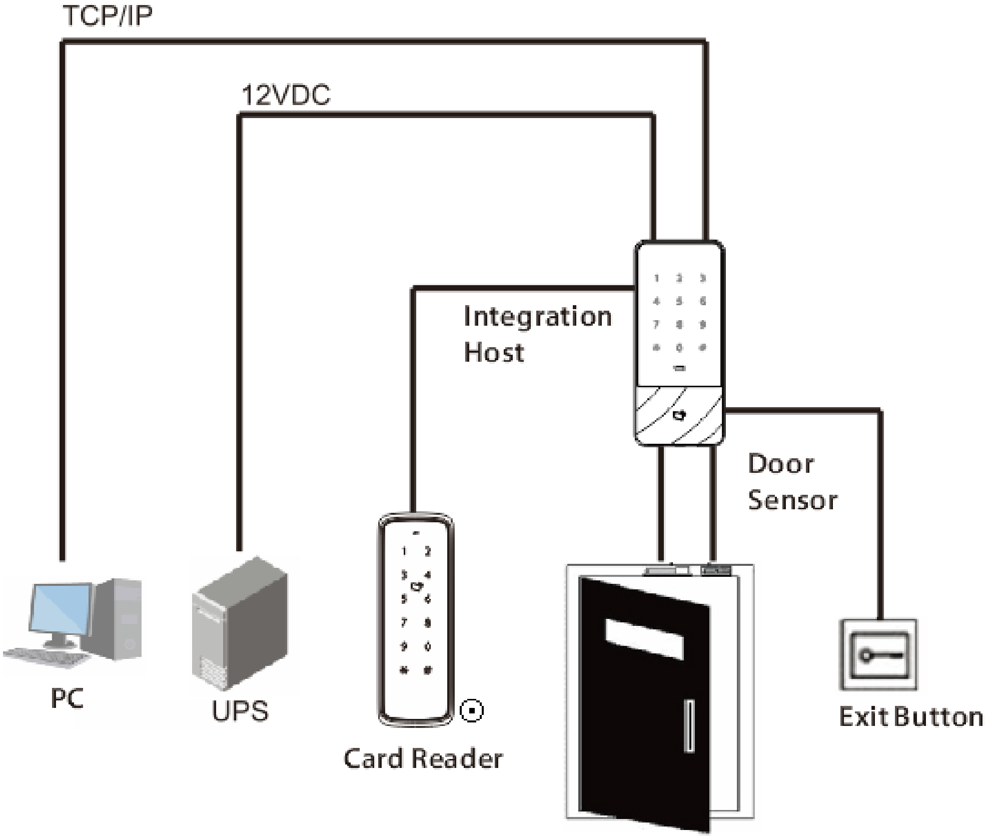
Figure 2-2 Apply silicone


Apply silicone sealant to gaps between the device and the wall.

3 Network Diagram

The network diagram of a basic access control system is shown below.

Figure 3-1 Network diagram



4 Wiring

Figure 4-1 Wiring

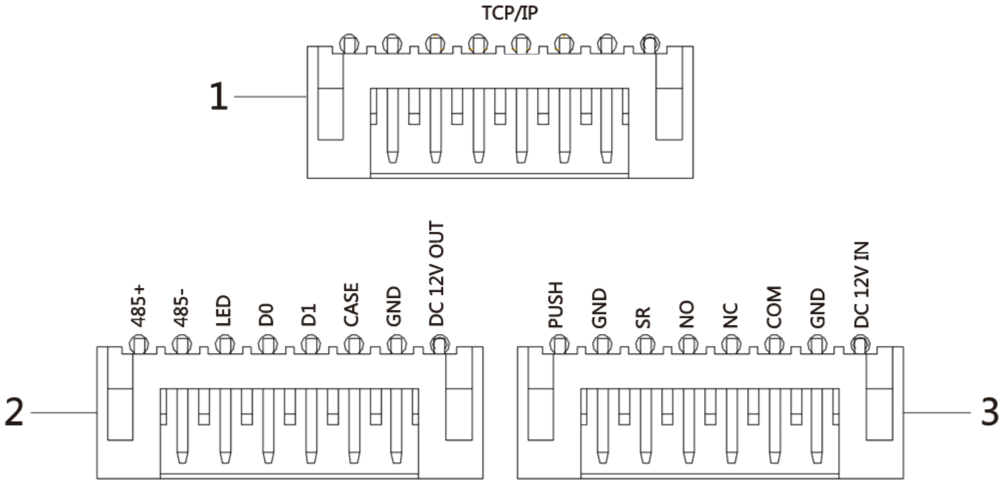


Table 4-1 Wiring description

No.	Port	Description
1	RJ45	TCP/IP (network port).
2	485+	Connects 485 reader.
	485-	
	LED	Connects the wiegand card swiping indicator signal line.
	D0	Connects the wiegand data transmission line.
	D1	
	CASE	Tamper input of reader.
	GND	Connects grounding wire.
	DC 12V OUT	12VDC power supply of reader.
3	PUSH	Connects the door exit button.
	GND	Connects grounding wire, which is shared by door detector and door exit button.
	SR	Connects door detector.
	NO	Connects the NO terminal of door lock.
	NC	Connects the NC terminal of door lock.
	COM	Lock relay.
	GND	Connects grounding wire.
	DC 12V IN	12VDC power input.

5 Local Configuration

5.1 Main Menu

Step 1 Touch the screen to wake up the Access Terminal, and press **#**.

Indicator light is solid blue and the numeric keyboard turns on, which means the Access Terminal is woken up.

Step 2 Enter the admin password, and then press **#**.

Step 3 After entering the main menu, you can press numeric keys to configure parameters.

Table 5-1 Main menu Description

Numeric key	Description
0	Modify the admin password.
1	Add users.
2	Delete users.
3	Set unlock modes.
4	Set the hold time of door lock relay.
5	Set the working mode.
6	Enable the door sensor.
9	Restore factory defaults.

- The default admin password is 88888888.
- Indicator light flashes bule, which means that you enter the main menu successfully.
- The indicator is solid red. After the buzzer sounds three times, the indicator light is solid blue, which means that wrong password is entered.
- After configurations, press * to go to the previous page.
- On the main menu, press *to exit the main menu.

5.2 Changing Admin Password

Change the admin password regularly to improve account security.

Step 1 Enter the main menu.

Step 2 Press **0** and **#**.

Step 3 Enter the new password and press **#**.

Step 4 Confirm the new password, and then press **#**.

- Indicator light is solid green and the buzzer sounds once, which means that the password is changed successfully.
- Indicator light is solid red and the buzzer sounds three times, which means the password is not changed.

5.3 Adding Users

Add a user and associate the user with card.

Step 1 Enter the main menu.

Step 2 Press **1** and **#** to add a user.

1) Add user ID: Enter the user ID and then click **#**.

   If the user ID exists already, it can not be added.

2) Add a card: Swipe a card and then press **#**.

   If card number is not needed, press**#** to skip this step.

3) Add password.

   - If it is necessary to set password, enter a password and press **#**. Otherwise, press **#** to skip this step.
   - Set the password if you do not swipe card to add card number. If password is not set, the user can not be added.

Step 3 Repeat step 2 to add more users.

Indicator light is solid green and the buzzer sounds once, which means that the user is added successfully. Indicator light is solid red and the buzzer sounds three times, which means user adding failure.

After adding users, the system stays at **Add User** menu. You can press ***** to return to the main menu.

5.4 Deleting Users

Delete users and their will not have permission to unlock the door.

Step 1 Enter the main menu.

Step 2 Press **2** and **#**.

- Swipe the card directly and press **#** to delete the user.
- Enter the user ID and press **#** to delete the user.
- Enter 0000 and press **#** to delete all users.

- Indicator light is solid green, and the buzzer sounds once, which means that the user is deleted successfully. Indicator light is solid red, and the buzzer sounds three times, which means the user is not successfully added. After deletion, the system stays at the **Delete User** screen. Press * to return to the main menu.

5.5 Configuring Unlock Modes

Configure door unlocking modes, such as unlocking through card, card + password, and user ID + password.

Step 1 Enter the main menu.

Step 2 Press **3** and **#**.

Step 3 Select unlocking mode.

- Card or user ID+ password (default): Press **0** and **#**.
- Card + password: Press and **#**.
- **1**
- User ID + password: Press **2** and **#**.

After configurations, the system returns to the main menu automatically. Press * to exit the main menu.

5.6 Configuring Door Open Duration

The door remains open for a defined duration for people to access before it automatically closes again.

Step 1 Enter the main menu.

Step 2 Press **4** and **#**.

Step 3 Enter the time (ranging from 1s to 600s) and press **#**.

After configuration, the system returns to the main menu automatically. Press * to exit the main menu.

5.7 Configuring Working Modes

The Access Terminal has two working modes. It can function as an access controller or card reader.

Step 1 Enter the main menu.

Step 2 Press **5** and **#**.

Step 3 Select the working mode.

- Access controller: Control access after people verify their identities. Press **0** and **#**.
- Reader: Reads access card. Press **1** and **#**.

After configurations, the system returns to the main menu automatically. Press * to exit main menu.

5.8 Configuring Door Sensor

Door detector can monitor door status and trigger an alarm when the door opens abnormally.

Step 1 Enter the main menu.

Step 2 Press **6** and **#**.

Step 3 Select whether door sensor is enabled.

- Disable (default): Press **0** and **#**.
- Enable: Press **1** and **#**.

After configurations, the system returns to the main menu automatically. Press ***** to exit the main menu.

5.9 Restoring to Factory Defaults

⚠

Restoring to factory defaults will cause data loss. Please be advised.

Step 1 Enter the main menu.

Step 2 Press **9** and **#**.

Step 3 Enter 000 and press **#**.

After configurations, the Access Terminal will restart automatically.

6 Smart PSS Configuration

This section introduces how to manage and configure the Access Terminal through SmartPSS. For details, see the user's manual of SmartPSS.

📖

The pictures in the user manual are only for reference, and might differ from the actual product.

6.1 Logging In

Install the Smart PSS client, and double click the icon to run it. Follow the on-screen instructions to log in.

6.2 Adding Devices

You need to add the access terminal to SmartPSS. You can add in batches or individually.

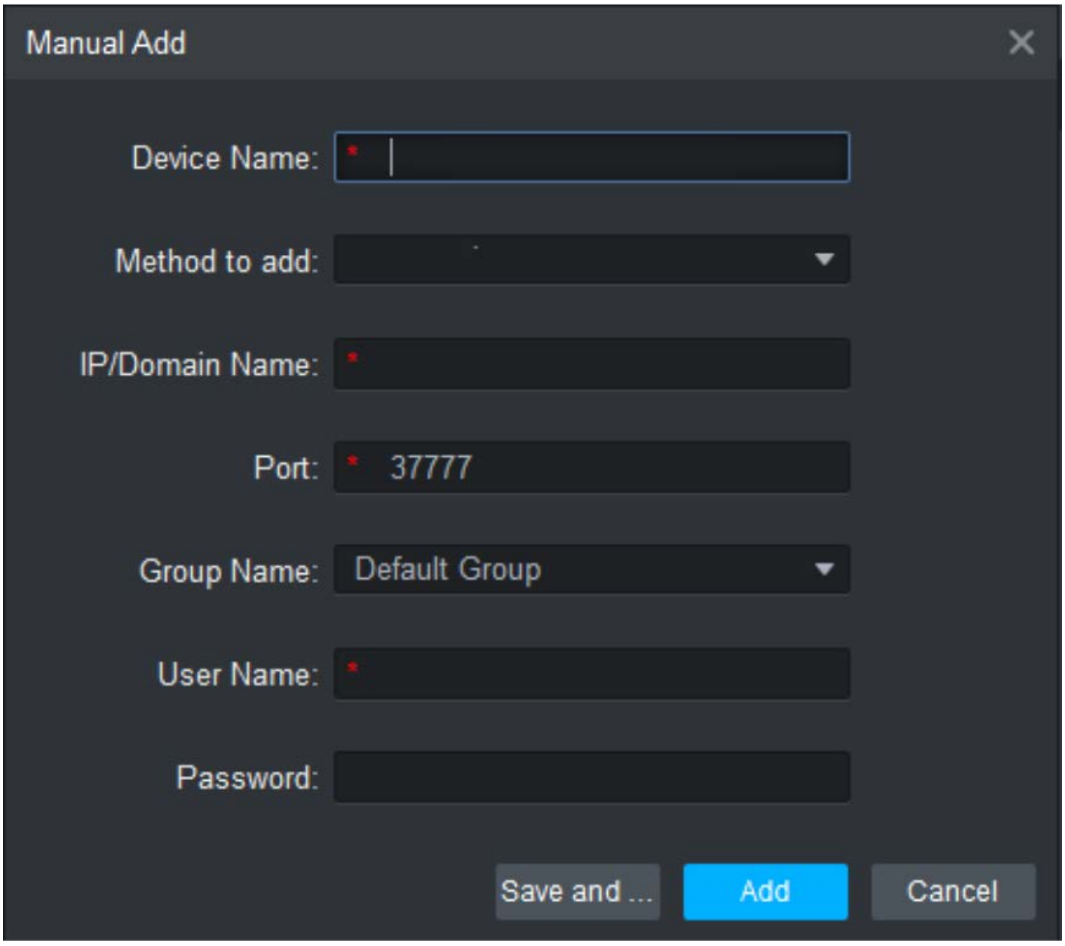
6.2.1 Adding Individually

You can add devices individually by entering the exact IP address and domain name.

Step 1 On the **Devices** page, click **Add**.

Step 2 Enter the device information.

Figure 6-1 Add manually



Device Name: *

Method to add:

IP/Domain Name: *

Port: * 37777

Group Name: Default Group

User Name: *

Password:

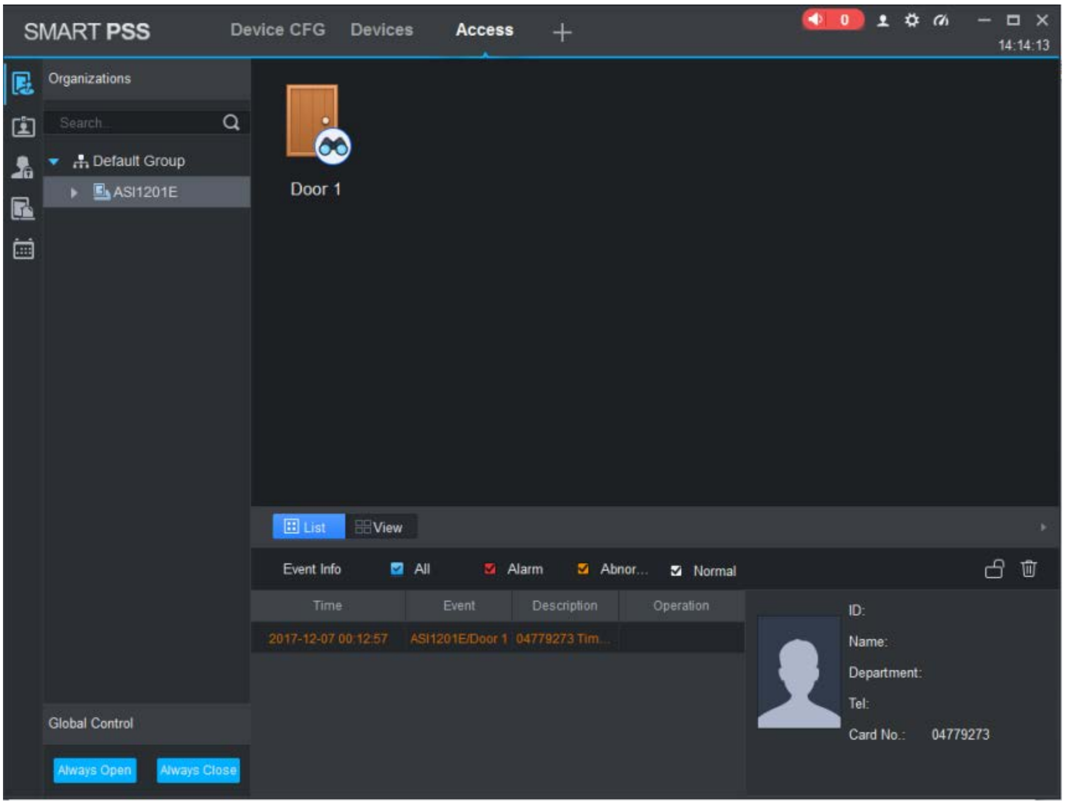
Table 6-1 Device information description

Parameter	Description
Device Name	The name of the device. We recommend you name the device after its installation area.
Method to add	Add devices according to the IP address or domain name.
IP/Domain Name	IP address or domain name of the device.
Port	Port number of the device. The default port number is 37777.
Group Name	The group of the device.
User Name and password	User name and password of the device.

Step 3 Click **Add** to add a device.

The system displays the added device list.

Figure 6-2 Added devices



Time	Event	Description	Operation
2017-12-07 00:12:57	ASI1201E/Door 1	04779273 Tim...	

ID:

Name:

Department:

Tel:

Card No.: 04779273

- To add more devices, click **Save and Continue**.
- **Online** is displayed after successful login.

6.2.2 Adding in Batches

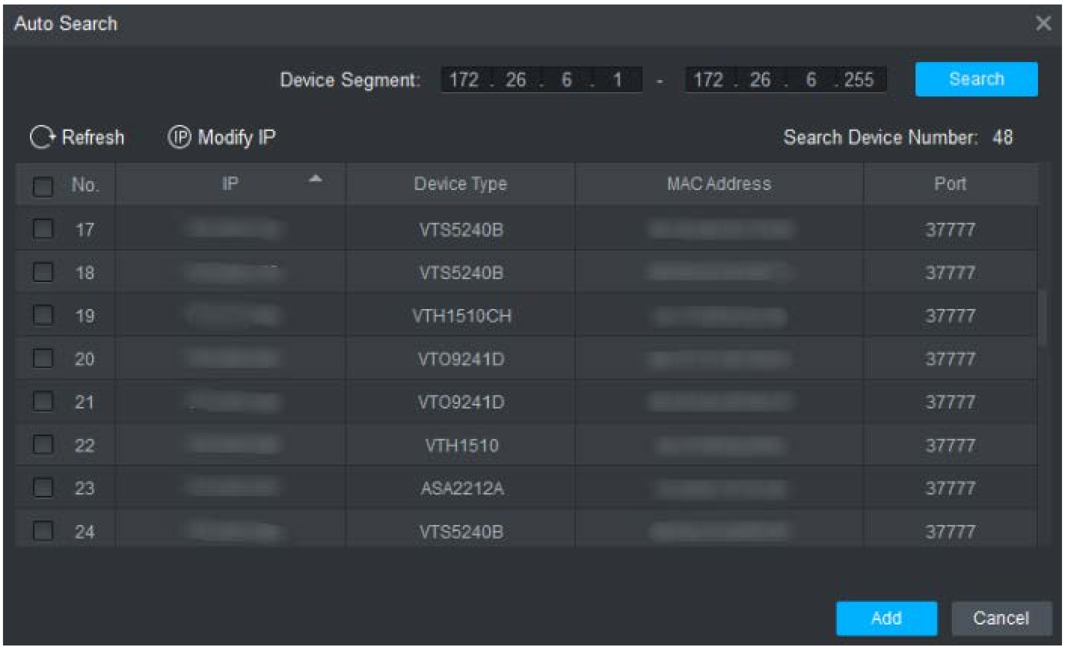
We recommend the auto-search function when you want to add devices in batches. The devices must be on the same network segment.

Step 1 On the **Devices** page, click **Auto Search**.

Step 2 Enter the network segment, and then click **Search**.

A device list is displayed.

Figure 6-3 Auto search



Device Segment: 172 . 26 . 6 . 1 - 172 . 26 . 6 . 255

Search Device Number: 48

□ No.	IP	Device Type	MAC Address	Port
□ 17	[redacted]	VTS5240B	[redacted]	37777
□ 18	[redacted]	VTS5240B	[redacted]	37777
□ 19	[redacted]	VTH1510CH	[redacted]	37777
□ 20	[redacted]	VTO9241D	[redacted]	37777
□ 21	[redacted]	VTO9241D	[redacted]	37777
□ 22	[redacted]	VTH1510	[redacted]	37777
□ 23	[redacted]	ASA2212A	[redacted]	37777
□ 24	[redacted]	VTS5240B	[redacted]	37777

- Click **Search** to refresh the device list.
- Select a device, and then click **Modify IP** to modify its IP address. For details, see the user's manual of SmartPSS.

Step 3 Select devices that you want to add to the SmartPSS, and then click **Add**.

Step 4 Enter the username and the password of the device.

You can view the added devices on the **Devices** page.

Online is displayed after successful login.

Appendix 1 Cybersecurity Recommendations

Mandatory actions to be taken for basic equipment network security:

1. **Use Strong Passwords**

   Please refer to the following suggestions to set passwords:

   - The length should not be less than 8 characters.
   - Include at least two types of characters; character types include upper and lower case letters, numbers and symbols.
   - Do not contain the account name or the account name in reverse order.
   - Do not use continuous characters, such as 123, abc, etc.
   - Do not use overlapped characters, such as 111, aaa, etc.

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

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

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

1. **Physical Protection**

   We suggest that you perform physical protection to equipment, especially storage devices. For example, place the equipment in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable equipment (such as USB flash disk, serial port), etc.

2. **Change Passwords Regularly**

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

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

   The device supports password reset function. Please set up related information for password reset in time, including the end user’s mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

4. **Enable Account Lock**

   The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

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

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

6. **Enable HTTPS**

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

7. **MAC Address Binding**

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

8. **Assign Accounts and Privileges Reasonably**

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

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

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

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

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

10. **Audio and Video Encrypted Transmission**

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

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

11. **Secure Auditing**

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

12. **Network Log**

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

13. **Construct a Safe Network Environment**

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

    - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
    - The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
    - Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
    - Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.