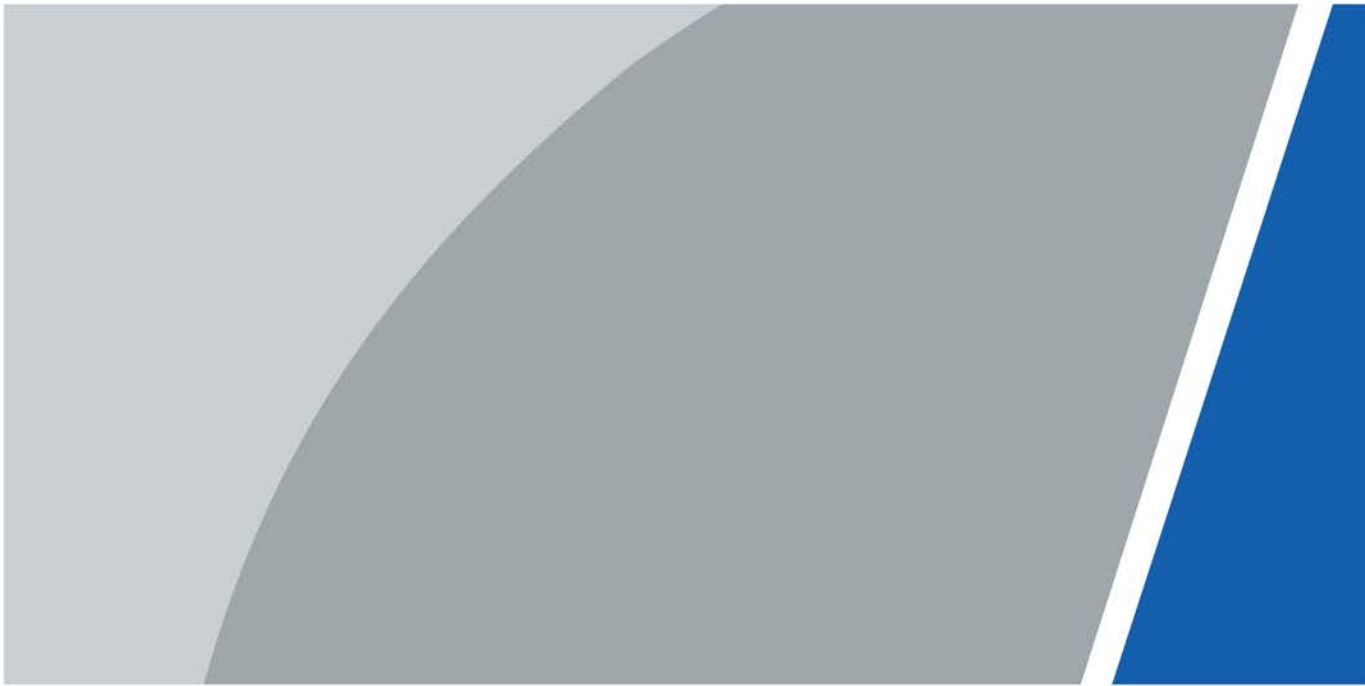# Access Standalone

User's Manual

V1.0.1

Foreword

General

This manual introduces the functions and operations of the Access Standalone. Read carefully before using the device, and keep the manual safe for future reference.

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
V1.0.1	Updated the configurations on the platform.	November 2022
V1.0.0	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 Standalone, hazard prevention, and prevention of property damage. Read carefully before using the Access Standalone, and comply with the guidelines when using it.

Transportation Requirement

⚠️

Transport, use and store the Access Standalone under allowed humidity and temperature conditions.

Storage Requirement

⚠️

Store the Access Standalone under allowed humidity and temperature conditions.

Installation Requirements

⚠️ WARNING

- Do not connect the power adapter to the Access Standalone 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 Controller.
- Do not connect the Access Standalone to two or more kinds of power supplies, to avoid damage to the Access Standalone.
- 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 Standalone in a place exposed to sunlight or near heat sources.
- Keep the Access Standalone away from dampness, dust, and soot.
- Install the Access Standalone on a stable surface to prevent it from falling.
- Install the Access Standalone 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 Standalone label.
- The Access Standalone is a class I electrical appliance. Make sure that the power supply of the Access Standalone is connected to a power socket with protective earthing.

Operation Requirements

⚠️

- Check whether the power supply is correct before use.

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

Table of Contents

1 Product Overview

Waterproof standalone Access Standalone 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.
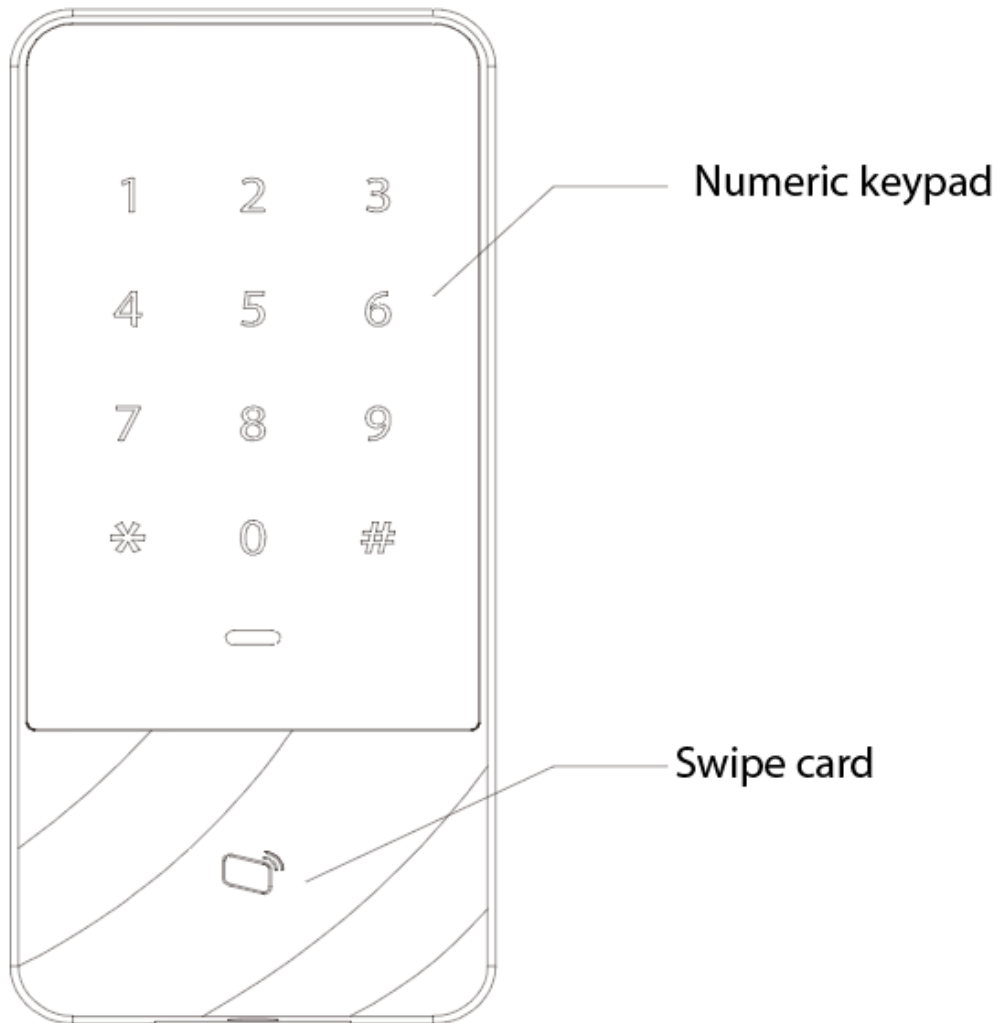
1.1 Dimensions

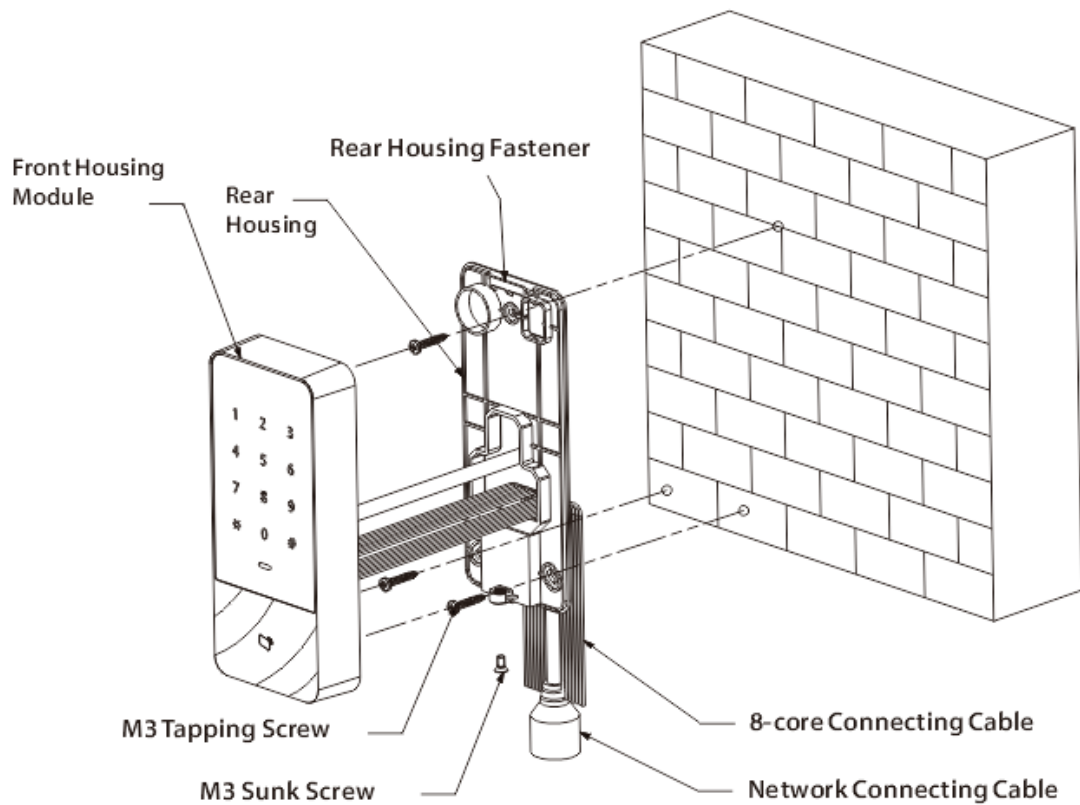Figure 1-1 Dimensions (mm [inch])
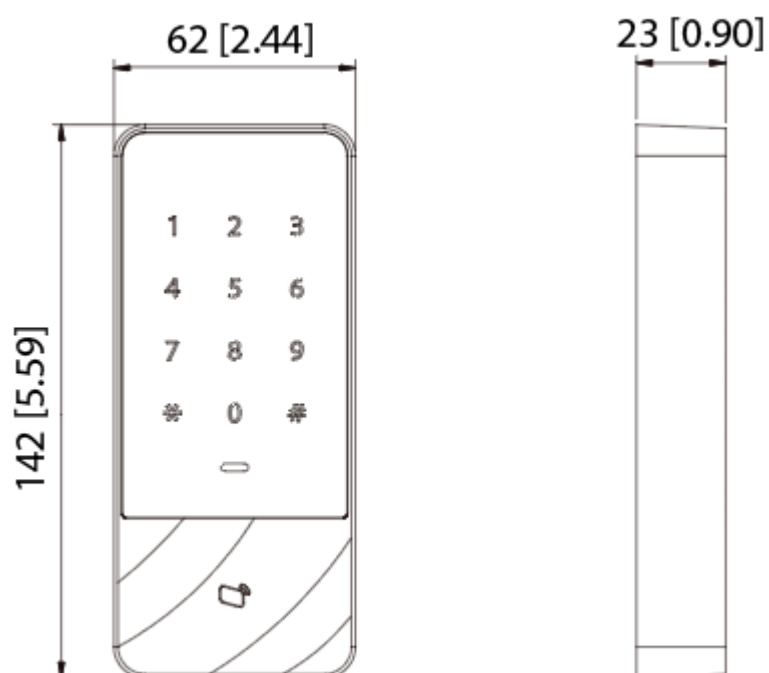
1.2 Structure

Figure 1-2 Structure

Numeric keypad

Swipe card

2 Installation

Background Information

Figure 2-1 Installation

Procedure

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 device and the wall.

Figure 2-2 Apply silicone

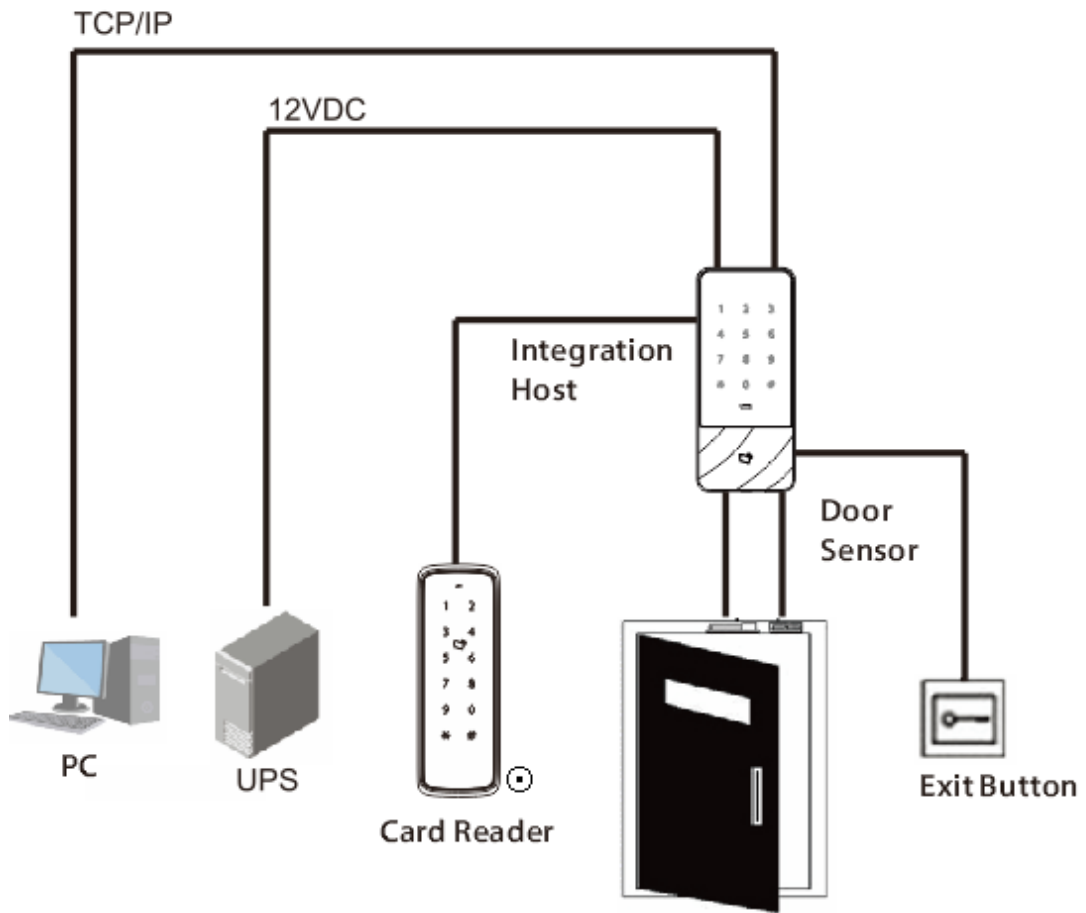Apply silicone sealant to gaps between the device and the wall.
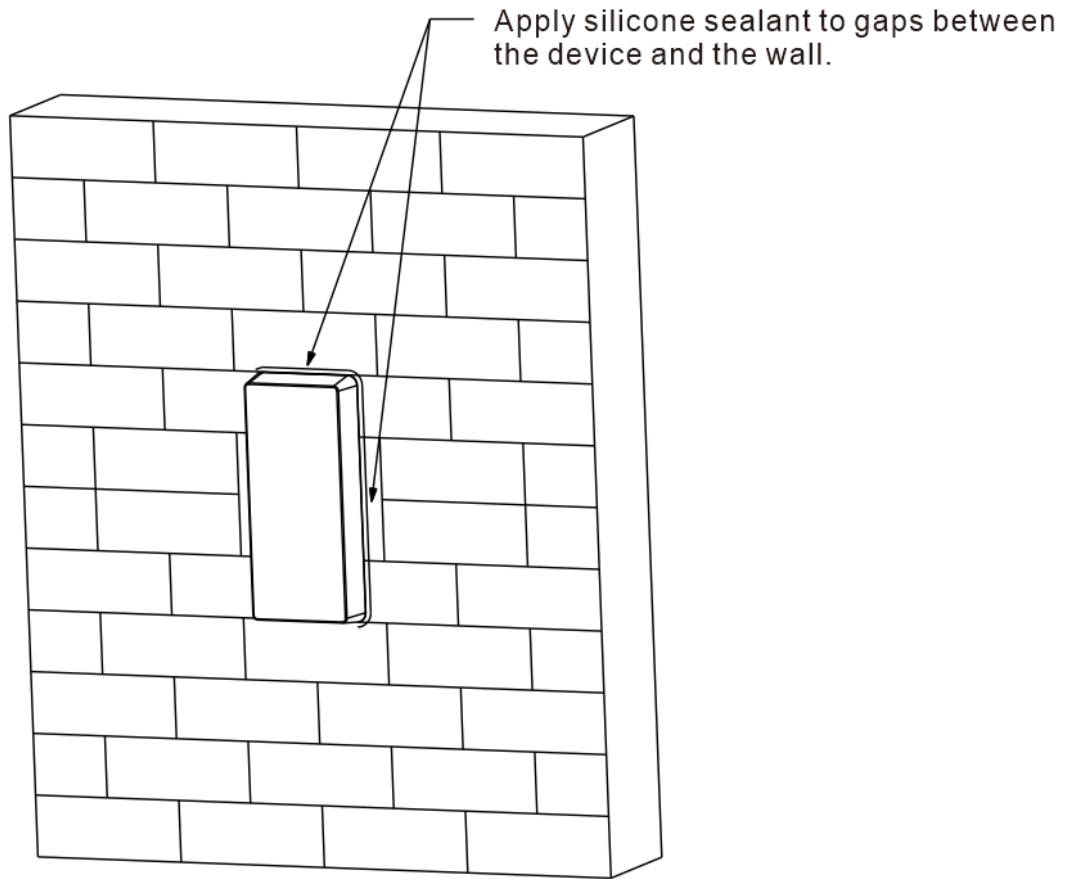
3 Network Diagram

The network diagram of a basic access control system is shown below.
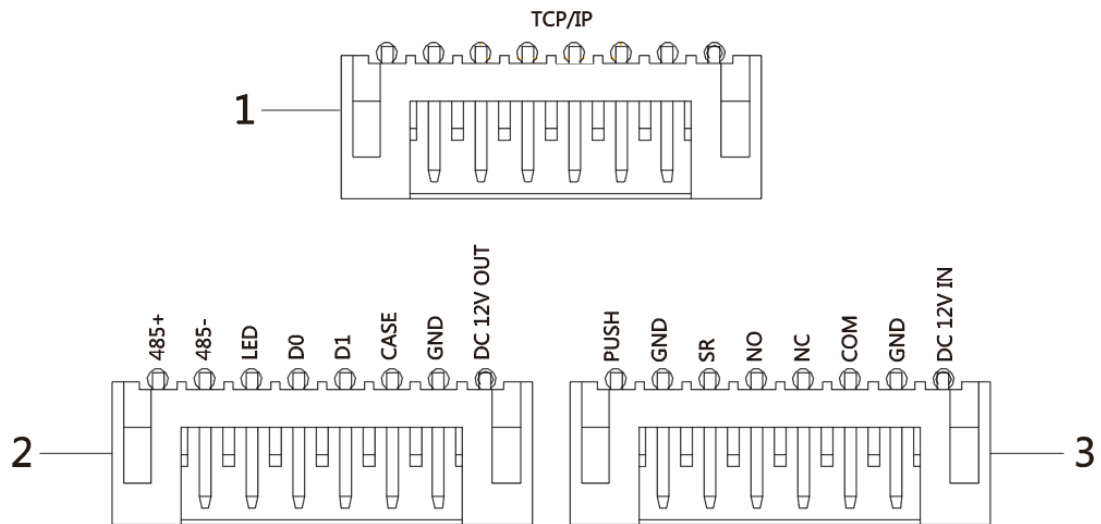
Figure 3-1 Network diagram

4 Wiring

Figure 4-1 Wiring

Table 4-1 Wiring description

No.	Port	Description
1	RJ45	TCP/IP (network port).
2	485+	Connects RS-485 card reader.
	485-	
	LED	Connects the LED wire of the card reader to transmit indicator signals.
	D0	Connects the Wiegand card reader.
	D1	
	CASE	Connects the anti-tampering signals of the card reader.
	GND	Connects grounding wire.
	12 VDC OUT	12 VDC power supply of reader.
3	PUSH	Connects the door exit button.
	GND	Connects grounding wire, which is shared by the door detector and the door exit button.
	SR	Connects the door detector.
	NO	Connects the NO port of door lock.
	NC	Connects the NC port of door lock.
	COM	Connects the COM port of door lock.
	GND	Connects the grounding wire.
	12 VDC IN	12 VDC power input.

5 Local Configuration

5.1 Main Menu

Procedure

Step 1   Touch the screen to wake up the Access Standalone, and tap **#**.

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

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

Step 3   After entering the main menu, you can tap 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 blue, 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, tap ***** to go to the previous page.
- On the main menu, tap *****to exit the main menu.

5.2 Changing Admin Password

Change the admin password regularly to improve account security.

Procedure

Step 1   Enter the main menu.

Step 2   tap **0** and **#**.

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

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

📖

- 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.

Procedure

Step 1   Enter the main menu.

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

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

📖

If the user ID exists already, it cannot be added.

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

📖

If you do not want to add card, tap **#** to skip this step.

3) Add password: Enter a password and tap **#**.

📖

- If you do not want to set password, tap **#** to skip this step.
- Set the password if you did not add the card number. If password is not set, the user cannot be added.

Step 3   Repeat Step2 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 3 times, which means user adding failure.

📖

After adding users, the system stays at **Add User** screen. Tap ***** to return to the main menu.

5.4 Deleting Users

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

Procedure

Step 1   Enter the main menu.

Step 2   tap **2** and **#**.

- Swipe the card directly and tap **#** to delete the user.
- Enter the user ID and tap **#** to delete the user.
- Enter 0000 and tap **#** 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. tap ***** 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.

Procedure

Step 1　Enter the main menu.

Step 2　tap **3** and **#**.

Step 3　Select unlocking mode.

Table 5-2 Select the unlocking mode

Unlocking Mode	Unlock Method
Card (by default): Tap **0** and **#**.	Swipe the card on the card reader to unlock the door.
Card + password: Tap **1** and **#**.	Swipe the card, enter the password, and then tap **#** to unlock the door.
User ID + password: Tap **2** and **#**.	Enter the user ID and tap **#**, and then enter the password and tap **#** to unlock the door.

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

Procedure

Step 1　Enter the main menu.

Step 2　tap **4** and **#**.

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

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

5.7 Configuring Working Modes

The Access Standalone has 2 working modes. It can function as an access controller or card reader.

Procedure

Step 1   Enter the main menu.

Step 2   tap **5** and **#**.

Step 3   Select the working mode.

- Access controller: Controls access after people verify their identities.

  Tap **0** and **#**.

- Reader: Only reads card.

  Tap **1** and **#**.

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

5.8 Configuring Door Detector

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

Procedure

Step 1   Enter the main menu.

Step 2   tap **6** and **#**.

Step 3   Select whether door sensor is enabled.

- Disable (default): tap **0** and **#**.

- Enable: tap **1** and **#**.

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

5.9 Restoring to Factory Defaults

Procedure

Step 1   Enter the main menu.

Step 2   tap **9** and **#**.

Step 3   Enter **000**, and then tap **#**.

After configurations, the Access Standalone will restart automatically.

⚠

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

6 Smart PSS Lite Configuration

This section introduces how to manage and configure the Access Standalone through Smart PSS Lite. You can also configure time attendance rules on the platform, such as shifts, modes, schedules and more. For details, see the user's manual of Smart PSS Lite.

6.1 Installing and Logging In

Install and log in to Smart PSS Lite. For details, see the user manual of Smart PSS Lite.

Procedure

Step 1   Get the software package of the Smart PSS Lite from the technical support, and then install and run the software according to instructions.

Step 2   Initialize Smart PSS Lite when you log in for the first time, including setting password and security questions.

Set the password is for the first-time use, and then set security questions to reset your password when you forgot it.

Step 3   Enter your username and password to log in to Smart PSS Lite.

6.2 Adding Devices

You need to add the Access Standalone to Smart PSS Lite. You can add them in batches or individually.

6.2.1 Adding Individually

You can add Access Standalone individually by entering their IP addresses or domain names.

Procedure

Step 1   Log in to Smart PSS Lite.

Step 2   Click **Device Manager** and click **Add**.

Step 3   Enter the device information.

Figure 6-1 Device information

Table 6-1 Device parameters Description

Parameter	Description
Device Name	Enter a name of the Access Standalone. We recommend you name it after its installation area.
Method to add	Select **IP** to add the Access Standalone by entering its IP Address.
IP	Enter IP address of the Access Standalone.
Port	The port number is 37777 by default.
User Name/Password	Enter the username and password of the Access Terminal.

Step 4   Click **Add**.

The added Access Standalone displays on the **Devices** page. You can click **Add and Continue** to add more Access Standalones.

6.2.2 Adding in Batches

We recommend you use the auto-search function when you add want to Access Standalones in batches. Make sure the Access Standalones you add must be on the same network segment.

Procedure

Step 1   Log in to Smart PSS Lite.

Step 2   Click **Device Manager** and search for devices.

●   Click **Auto Search**, to search for devices on the same LAN.

●   Enter the network segment range, and then click **Search**.

Figure 6-2 Auto search
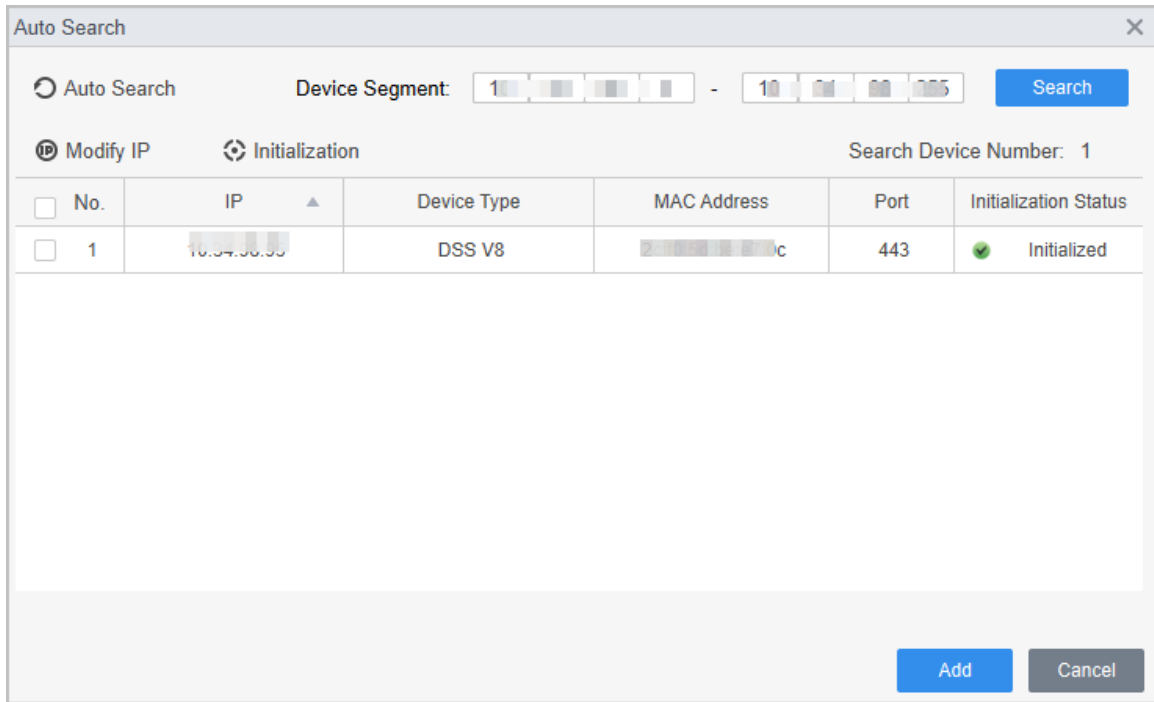
A device list will be displayed.

📖

Select a device, and then click **Modify IP** to modify its IP address.

Step 3   Select the Access Standalone that you want to add to Smart PSS Lite, and then click **Add**.

Step 4   Enter the username and the password of the Access Standalone.

You can view the added Access Standalone on the **Devices** page.

📖

The Access Standalone automatically logs in to Smart PSS Lite after being added. **Online** is displayed after successful login.

6.3 User Management

Add users, assign cards to them, and configure their access permissions.

6.3.1 Configuring Card Type

Set the card type before you assign cards to users. For example, if the assigned card is an ID card, set card type to ID card.

Procedure

Step 1   Log in to Smart PSS Lite.

Step 2   Click **Access Solution** > **Personnel Manager** > **User**.

Step 3   On the **Card Issuing Type** and then select a card type.

📖

Make sure that the card type is same to the actually assigned card; otherwise, the card number cannot be read.

Step 4 Click **OK**.

6.3.2 Adding Users

6.3.2.1 Adding Individually

You can add users individually.

Procedure

Step 1 Log in to Smart PSS Lite.

Step 2 Click **Access Solution** > **Personnel Manger** > **User** > **Add**.

Step 3 Click **Basic Info** tab, and enter the basic information of the user, and then import the face image.

Figure 6-3 Add basic information

Step 4 Click the **Certification** tab to add certification information of the user.

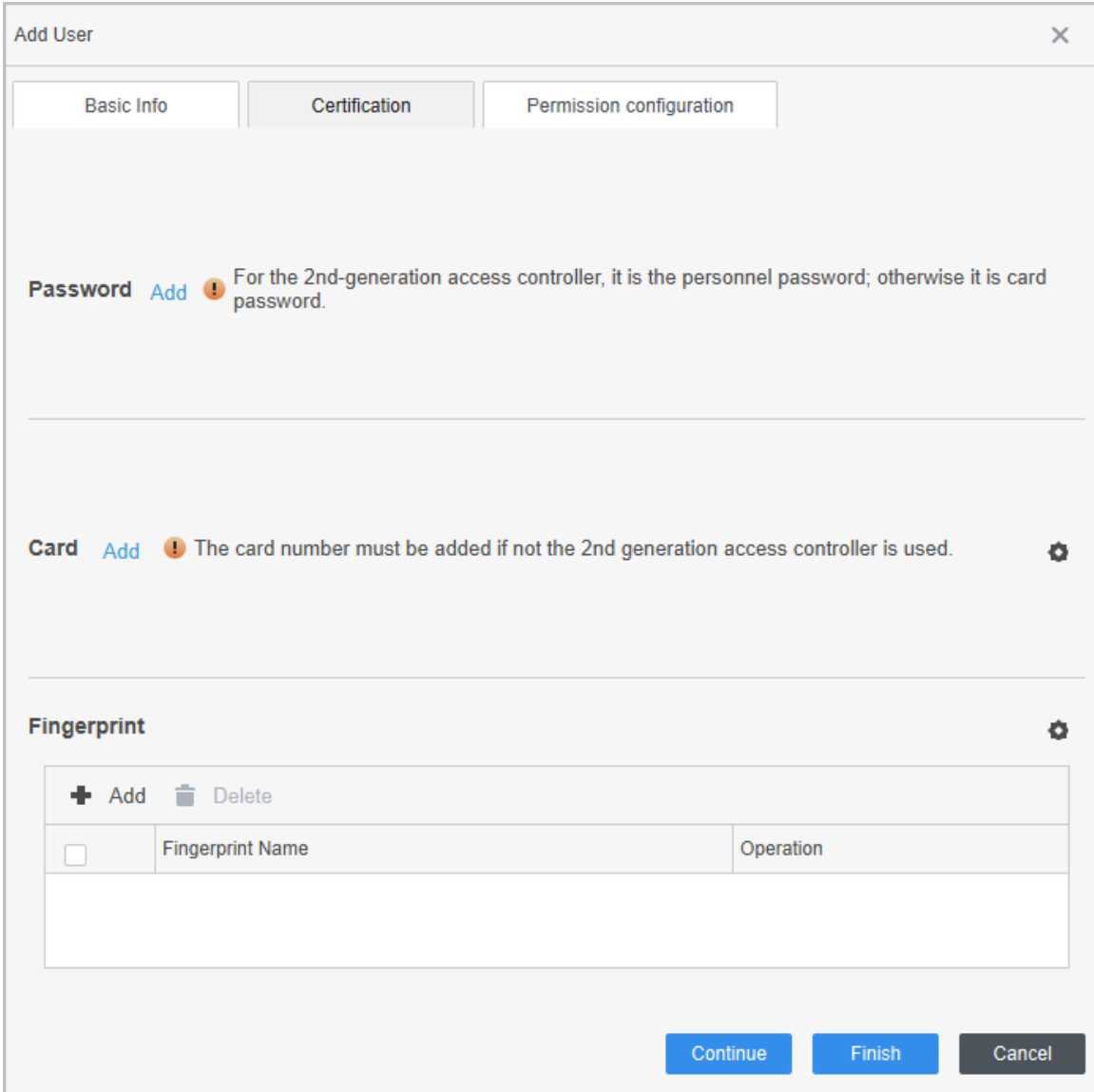- Configure password: The password must consist of 6–8 digits.

- Configure card: The card number can be read automatically or entered manually. To read the card number automatically, select a card reader, and then place the card on the card reader.
  1. On the **Card** area, click ⚙ and select **Card issuer**, and then click **OK**.
  2. Click **Add**, swipe a card on the card reader. The card number is displayed.
  3. Click **OK**.After adding a card, you can set the card to main card or duress card, or replace the card with a new one, or delete the card.
- Configure fingerprint.
  1. On the **Fingerprint** area, click ⚙ and select **Fingerprint Scanner**, and then click **OK**.
  2. Click **Add Fingerprint**, press your finger on the scanner three times in a row.

Figure 6-4 Add password, card, and fingerprint

Step 5   Configure permissions for the user. For details, see "6.3.3 Assigning Access Permission".

Step 6   Click **Finish**.

6.3.2.2 Adding in Batches

You can add users in batches.

Procedure

Step 1   Log in to Smart PSS Lite.

Step 2   Click **Personnel Manger** > **User** > **Batch Add**.

Step 3   Select **Card issuer** from the **Device** list, and then configure the parameters.

Figure 6-5 Add users in batches

Table 6-2 Add users in batches parameters

Parameter	Description
Start No.	The user ID starts with the number you defined.
Quantity	The number of users you want to add.
Department	Select the department that the user belongs to.
Effective Time/Expired Time	The users can unlock the door within the defined period.

Step 4   Click **Issue**.

The card number will be read automatically.

Step 5   Click **OK**.

Step 6   On the **User** page, click ✎ to complete user information.

6.3.3 Assigning Access Permission

Create a permission group that is a collection of door access permissions, and then associate users with the group so that users can unlock corresponding doors.

Procedure

Step 1   Log in to the Smart PSS Lite.

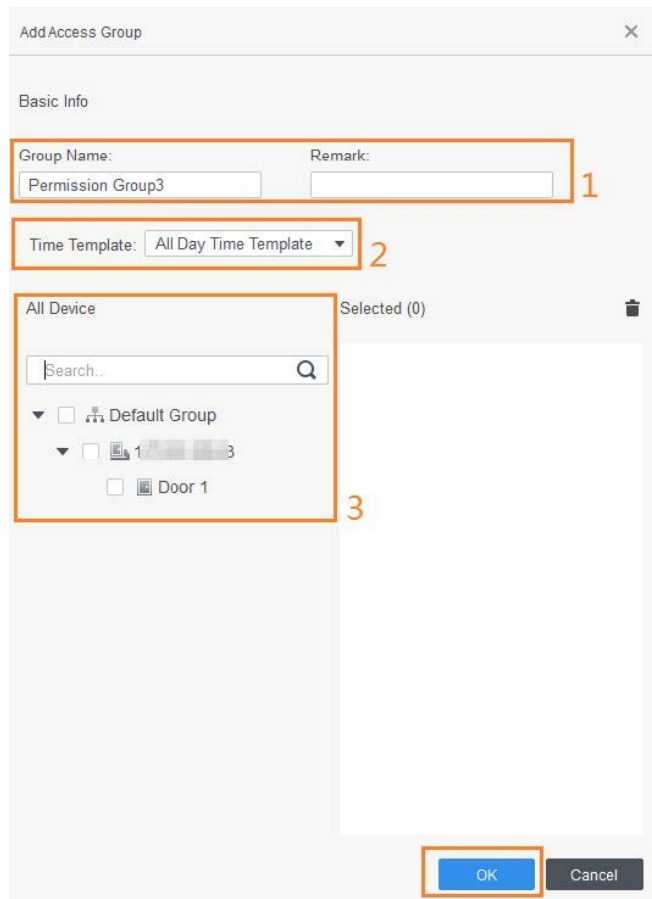Step 2   Click **Access Solution** > **Personnel Manger** > **Permission configuration**.

Step 3   Click + .

Step 4   Enter the group name, remarks (optional), and select a time template.

Step 5   Select the access control device.

Step 6   Click **OK**.
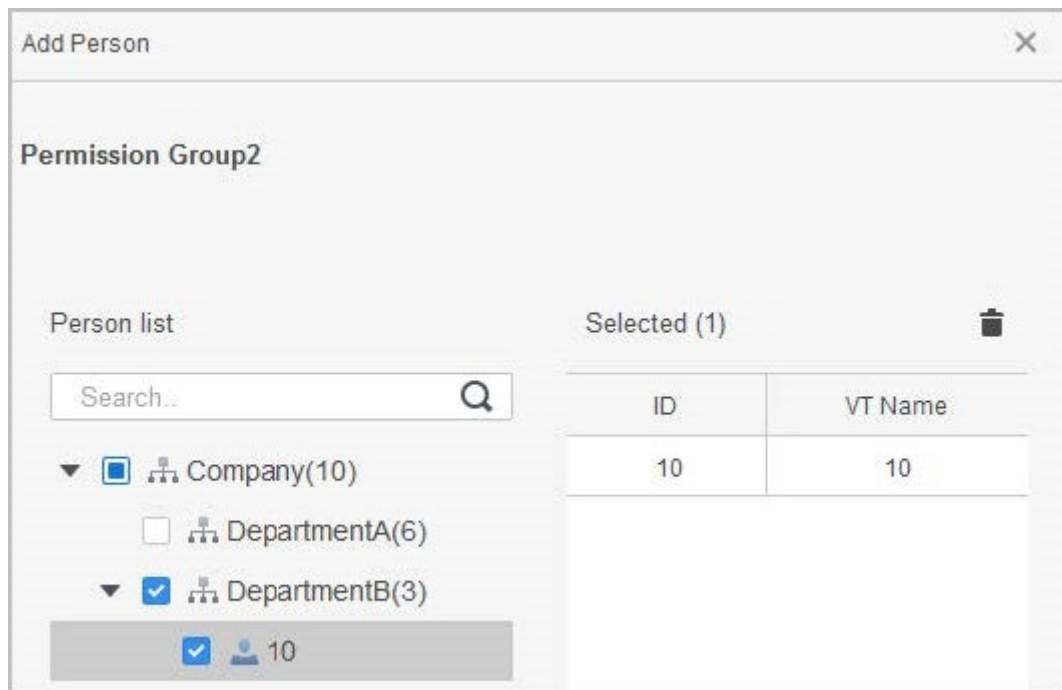
Figure 6-6 Create a permission group

Step 7   Click ![icon] of the permission group you added.

Step 8   Select users to associate them with the permission group.

Figure 6-7 Add users to a permission group

Step 9   Click **OK**.

Users in the permission group can unlock the door after valid identity verification.

6.4 Access Management

6.4.1 Remotely Opening and Closing Door

You can remotely monitor and control door through Smart PSS Lite. For example, you can remotely open or close the door.
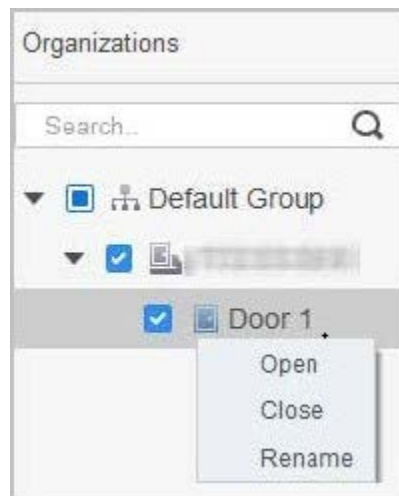
Procedure

Step 1   Click **Access Solution** > **Access Manager** on the Home page.

Step 2   Remotely control the door.

- Select the door, right click and select **Open** or **Close**.

Figure 6-8 Open door

- Click **[]** or **■** to open or close the door.

Related Operations

- Event filtering: Select the event type in the **Event Info**, and the event list displays the selected event type, such as alarm events and abnormal events.
- Event refresh locking: Click 🔓 to lock the event list, and then event list will stop refreshing. Click 🔒 to unlock.
- Event deleting: Click 🗑 to clear all events in the event list.

6.4.2 Setting Always Open and Always Close

After setting always open or always close, the door remains open or closed all the time.

Procedure

Step 1   Click **Access Solution** > **Access Manager** on the Home page.

Step 2   Click **Always Open** or **Always Close** to open or close the door.

Figure 6-9 Always open or close

The door will remain open or closed all the time. You can click **Normal** to restore the access control to normal status, and then the door will be open or closed based on the configured verification methods.

6.4.3 Monitoring Door Status

Procedure

Step 1   Click **Access Solution** > **Access Manager** on the Home page.

Step 2   Select the Access Standalone in the device tree, and right click the Access Terminal and then select **Start Real-time Event Monitoring**.

Real-time access control events will display in the event list.

$\square$

Click **Stop Monitor**, real-time access control events will not display.

Figure 6-10 Monitor door status
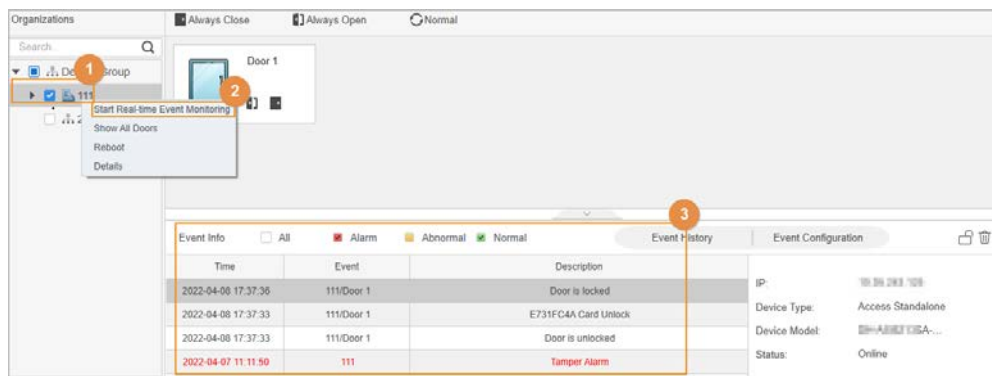
Related Operations

- Show All Door: Displays all doors controlled by the Access Standalone.
- Reboot: Restart the Access Standalone.
- Details: View the device details, such as IP address, model, and status.

6.4.4 Viewing Access Control Details

View the IP address, model, status, serial number, firmware version and other information of the

Access Standalones.

Procedure

<u>Step 1</u>   Click **Access Manager** on the home page. (You can also click **Access Guide** > 🖹).

<u>Step 2</u>   Click the Access Standalone that you want to view in the left organization tree, right-click
the device, and then click **Details** to view the detailed information of the device.

Figure 6-11 View details

6.4.5 Rebooting Access Standalone

Support remotely rebooting Access Standalones through the platform.
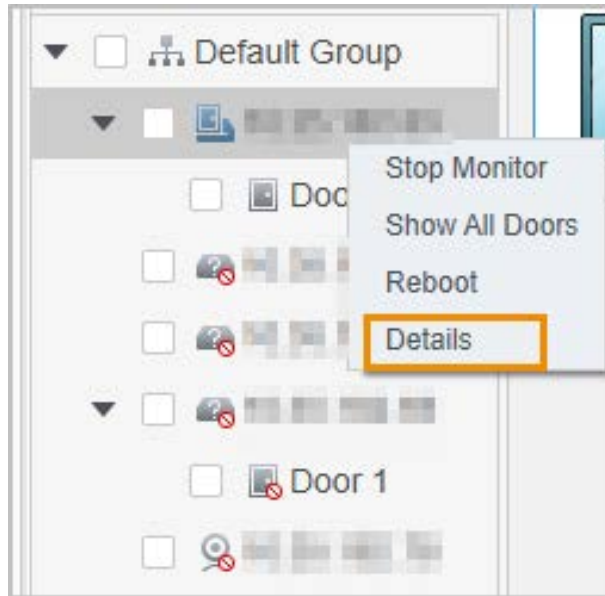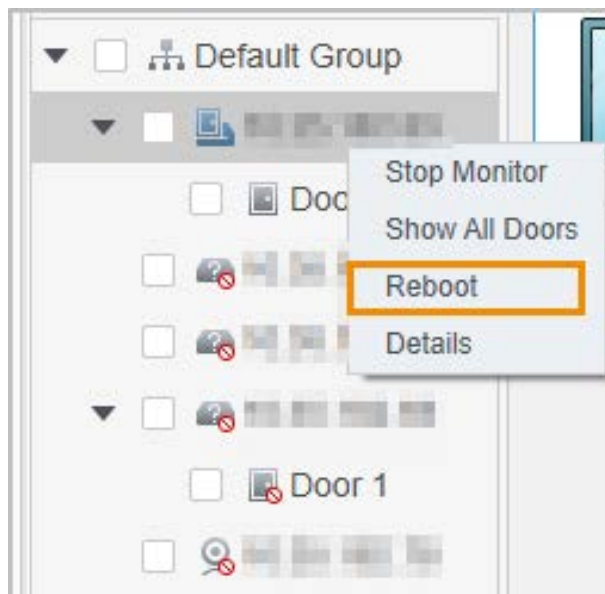
Procedure

<u>Step 1</u>   Click **Access Manager** on the home page. (You can also click **Access Guide** > 🖹).

<u>Step 2</u>   Click the Access Standalone that you want to reboot in the left organization tree, right-click
the device, and then click **Reboot** to reboot the device.

Figure 6-12 Reboot device

Appendix 1 Cybersecurity Recommendations

Mandatory actions to be taken for basic device 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 device (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 device 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 device network security:

1. **Physical Protection**

    We suggest that you perform physical protection to device, especially storage devices. For example, place the device 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 device (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 device, 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 device 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 device, 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 device 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.