# Access Standalone

## User's Manual

V1.0.4

# Foreword

## General

This manual introduces the installation and detailed operations of the Access Standalone (hereinafter referred to as "the Standalone").

## 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, lower performance, or unpredictable result. |
| 🔑 **TIPS** | Provides methods to help you solve a problem or save you time. |
| 📖 **NOTE** | Provides additional information as the emphasis and supplement to the text. |

## Revision History

| Version | Revision Content | Release Date |
|---|---|---|
| V1.0.4 | Updated the manual. | October 2022 |
| V1.0.3 | Updated screens and DSS configurations. | September 2021 |
| V1.0.2 | Corrected certain numbers and functions. | June 2021 |
| V1.0.1 | Added recommended installation height. | June 2020 |
| V1.0.0 | First release. | March 2020 |

## Privacy Protection Notice

As the Standalone 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 Standalone.
- 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 Standalone, hazard prevention, and prevention of property damage. Read carefully before using the Standalone, comply with the guidelines when using it, and keep the manual safe for future reference.

## Transportation Requirements

⚠

Transport the Standalone under allowed humidity and temperature conditions.

## Storage Requirements

⚠

Store the Standalone under allowed humidity and temperature conditions.

## Installation Requirements

⚠ **WARNING**

- Connect the Standalone to the adapter before power on.
- Strictly abide by local electrical safety standards, and make sure that the voltage in the area is steady and conforms to the power requirements of the Standalone.
- Do not connect the Standalone to more than one power supply. Otherwise, the Standalone might become damaged.

⚠

- Observe all safety procedures and wear required protective equipment provided for your use while working at heights.
- Do not expose the Standalone to direct sunlight or heat sources.
- Do not install the Standalone in humid, dusty or smoky places.
- Install the Standalone in a well-ventilated place, and do not block the ventilator of the Standalone.
- Use the power adapter or case power supply provided by the Standalone manufacturer.
- The power supply must conform to the requirements of ES1 in IEC 62368-1 standard and be no higher than PS2. Note that the power supply requirements are subject to the Standalone label.
- Connect class I electrical appliances to a power socket with protective earthing.
- The appliance coupler is a disconnection device. When using the coupler, keep the angle for easy operation.

## Operation Requirements

⚠

- Make sure that the power supply of the Standalone works properly before use.

- Do not pull out the power cable of the Standalone while it is powered on.
- Only use the Standalone within the rated power range.
- Use the Standalone under allowed humidity and temperature conditions.
- Prevent liquids from splashing or dripping on the Standalone. Make sure that there are no objects filled with liquid on top of the Standalone to avoid liquids flowing into it.
- Do not disassemble the Standalone.
- Please use battery properly to avoid fire, explosion and other dangers.
- Please replace used battery with battery of the same type.
- If you use power plug or appliance coupler as disconnecting device, please maintain the disconnecting device available to be operated all the time.

# Table of Contents

**Foreword** ........ **I**

**Important Safeguards and Warnings** ........ **III**

**1 Overview** ........ **1**

1.1 Introduction ........ 1

1.2 Features ........ 1

1.3 Dimensions and Components ........ 1

**2 Installation** ........ **3**

2.1 Cable Connection ........ 3

2.2 Installation ........ 3

**3 Local Configuration** ........ **6**

3.1 Button Description ........ 6

3.2 Initialization ........ 6

3.3 Standby Screen ........ 7

3.4 Unlocking Method ........ 8

3.4.1 User Password ........ 8

3.4.2 Administrator Password ........ 9

3.5 Logging in to the Main Menu ........ 9

3.6 User Management ........ 10

3.6.1 Adding New User ........ 10

3.6.2 Viewing User Information ........ 12

3.7 Access Management ........ 12

3.7.1 Setting Unlock Mode ........ 12

3.7.2 Setting Door Status ........ 13

3.7.3 Setting Lock Holding Time ........ 13

3.7.4 Setting Door Sensor Type ........ 13

3.7.5 Setting Remote Verification ........ 13

3.8 Network Communication ........ 14

3.8.1 Configuring IP ........ 14

3.8.2 Configuring Wiegand ........ 15

3.8.3 Configuring TCP Port ........ 16

3.8.4 Configuring Serial Port ........ 16

3.9 System Configuration ........ 17

3.9.1 Setting Time ........ 17

3.9.2 Setting Volume ........ 17

3.9.3 Setting ScreenSaver ........ 17

3.9.4 Setting Privacy ........ 17

3.9.5 Setting Card No. Reverse ........ 18

3.9.6 Setting Auto Test ........ 18

3.9.7 Restoring to Default Settings ........ 18

3.9.8 Restarting the Standalone ........ 19

3.10 USB Management ........ 19

3.10.1 Exporting to USB ........ 19

3.10.2 Importing from USB ........ 20

3.10.3 Updating System ........ 21

3.10.4 Importing Pictures ....21
3.10.5 Exporting Records ....21
3.11 System Information ....21
**4 Web Configurations .... 22**
4.1 Initialization ....22
4.2 Logging In ....24
4.3 Resetting the Password ....24
4.4 Configuring Door Parameter ....26
4.5 Alarm Linkage Configuration ....27
4.5.1 Setting Alarm Linkage ....27
4.5.2 Viewing Alarm Log ....28
4.6 Time Section Configuration ....29
4.6.1 Setting Time Section ....29
4.6.2 Setting Holiday Group ....30
4.6.3 Setting Holiday Plan ....32
4.7 Data Capacity ....33
4.8 Setting Volume ....33
4.9 Network Configuration ....33
4.9.1 Setting TCP/IP ....33
4.9.2 Setting Port ....34
4.9.3 Setting P2P ....35
4.10 Setting Data ....36
4.11 Safety Management ....37
4.11.1 Configuring IP Authority ....37
4.11.2 Configuring System Service ....38
4.11.3 User Management ....39
4.11.4 Maintenance ....39
4.11.5 Configuration Management ....40
4.11.6 Updating System ....40
4.11.7 Version Information ....41
4.11.8 Viewing Online Users ....41
4.11.9 Viewing System Log ....42
4.12 Logging Out ....43
**5 Phone Configuration .... 44**
**6 DSS Configuration .... 45**
6.1 Adding Device ....45
6.2 Access Control Management ....46
6.2.1 Configuring Door ....46
6.2.2 Creating Door Group ....48
6.2.3 Configuring Access Permission Group ....48
6.2.4 Configuring Advanced Function ....50
6.2.5 First Card Unlock ....50
6.2.6 Viewing Access Control Record ....56
**Appendix 1 Cybersecurity Recommendations .... 58**

# 1 Overview

## 1.1 Introduction

The Access Standalone is an access control terminal that supports unlock through fingerprint, passwords, and card, and supports their combinations.

## 1.2 Features

- Unlock by card, fingerprint, password or their combinations, unlock button and remote control.
- Supports 30,000 users, 30,000 cards, and 5,000 fingerprints.
- Stores 100,000 access records and 1,000 alarm records.
- Supports duress alarm and tamper alarm with one alarm input and one alarm output.
- Support general users, restricted users, guest users, patrol users, VIP users, and other users.
- Supports voice prompts.
- The timer can work properly for one year after power off.
- Supports NTP for time synchronization.

## 1.3 Dimensions and Components

Figure 1-1 Front view (mm [inch])

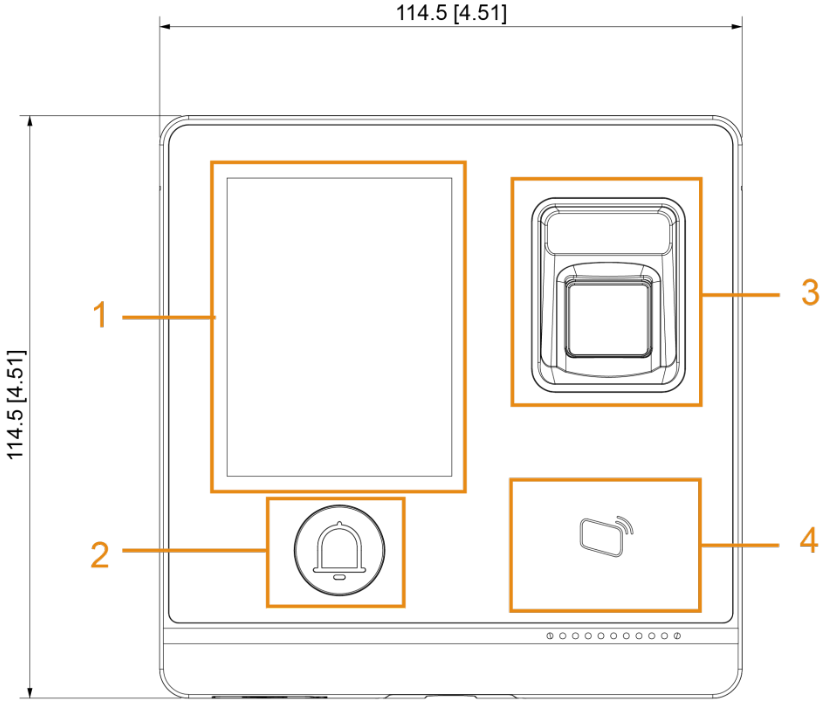


Figure 1-2 Back view (mm [inch])

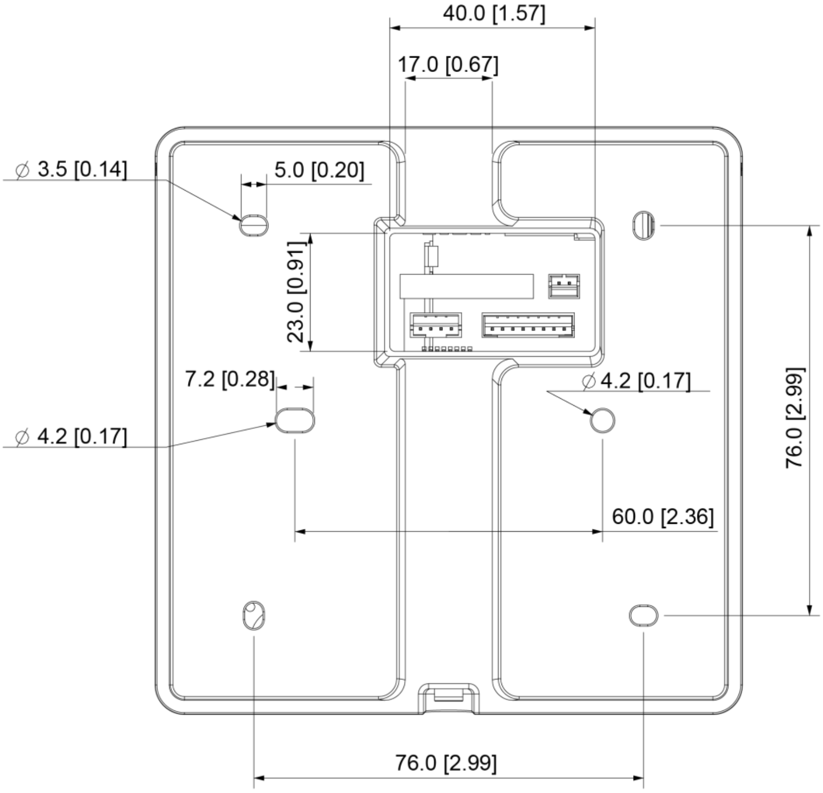


Figure 1-3 Side and bottom view (mm [inch])

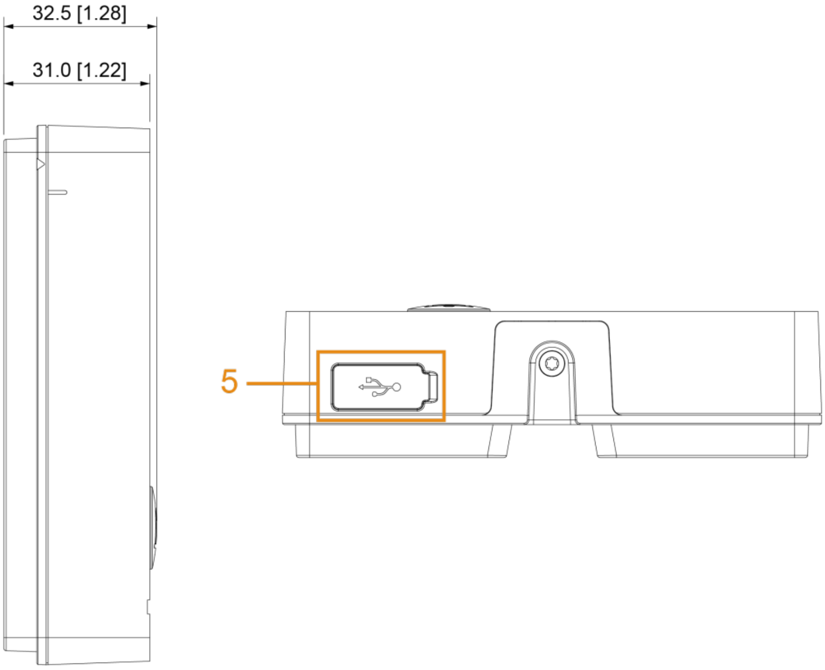


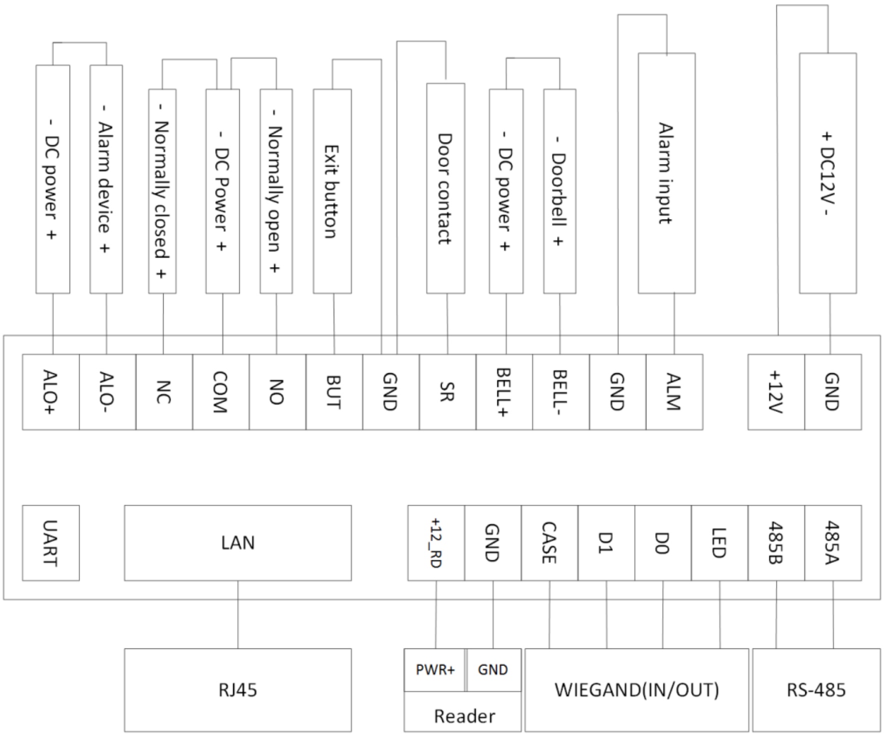
Table 1-1 Component description

| No. | Name |
|---|---|
| 1 | VA area |
| 2 | Doorbell button |
| 3 | Fingerprint sensor |
| 4 | Card swiping area |
| 5 | USB Port |

# 2 Installation

## 2.1 Cable Connection

Figure 2-1 Cable connection



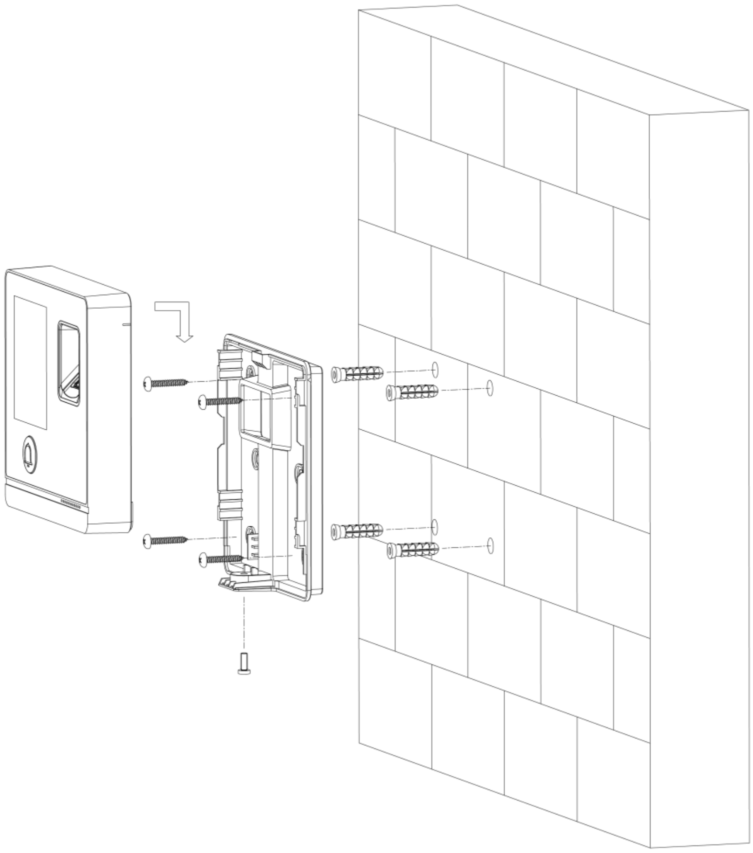
## 2.2 Installation

The recommended installation height is 1.4 m –1.6 m.

The Standalone supports surface installation and concealed installation.

## Surface installation

Figure 2-2 Surface installation



## Installation Procedure

Step 1 Stick installation map on the wall, and then drill holes according to hole positions on the map.

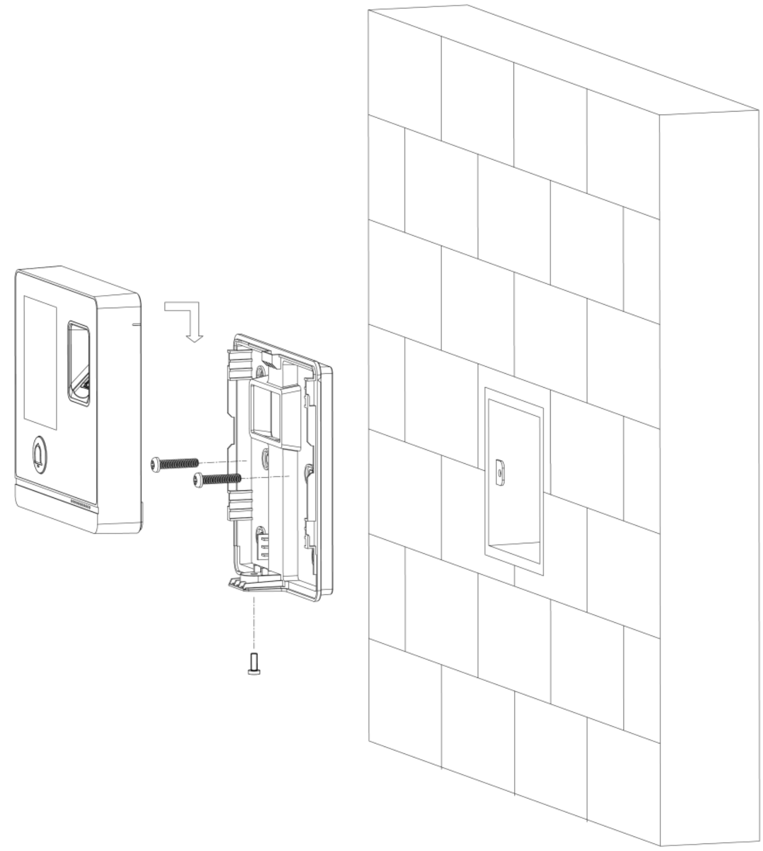
Step 2 Insert expansion bolt into installation holes.

Step 3 Fix the rear cover onto the wall with self-tapping screws.

Step 4 Put machine screws through the bottom hole; lock the front cover on to the rear cover.

## Concealed installation

Figure 2-3 Concealed installation



## Installation Procedure

Step 1 Draw the cables through the outlet.

Step 2 Fix the back cover on the mounted box with screws.

Step 3 Neaten the cables and buckle the front cover onto the back cover.

# 3 Local Configuration

## 3.1 Button Description

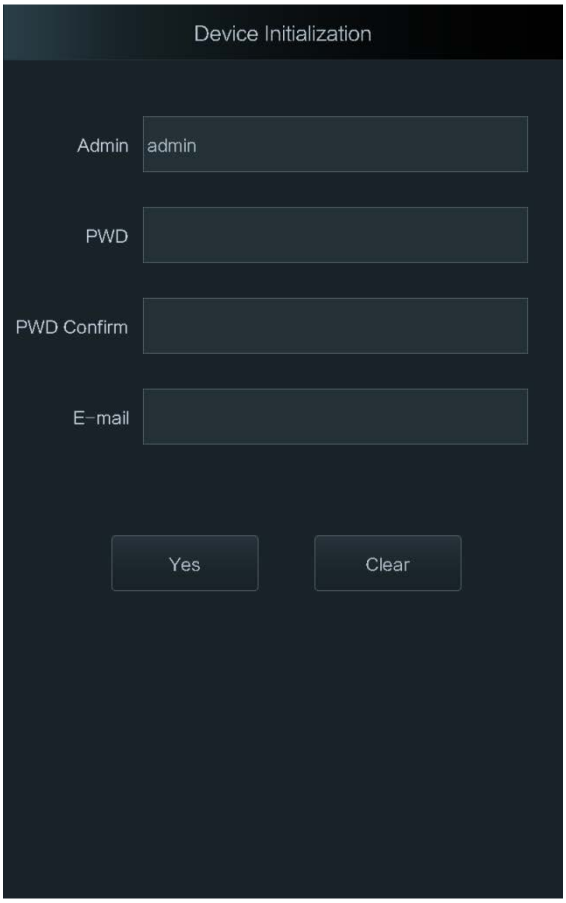
Table 3-1 Button description

| Button | Description |
|---|---|
| \|< | Go to the first page. |
| >\| | Go to the last page. |
| < | Go to the previous page. |
| > | Go to the next page. |
| ← | Go to the previous menu. |
| → | Go to the next menu. |

## 3.2 Initialization

Set the administrator password and link an email address.

Figure 3-1 Initialization



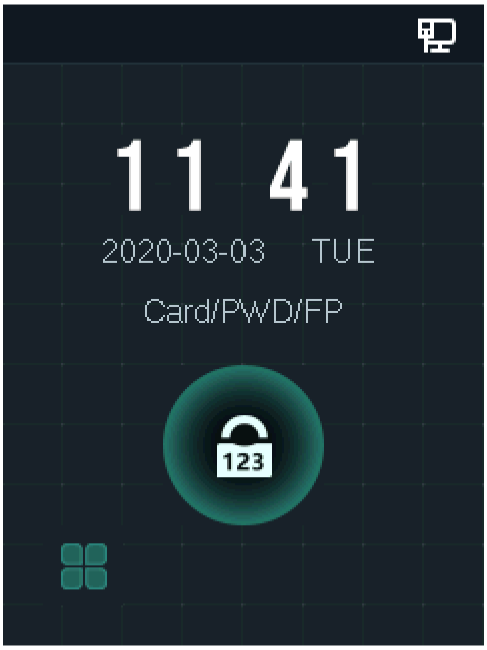
Admin admin

- Administrator and password set on this screen are used to log in to the web management platform.

- The administrator password can be reset through the linked email address if you forget the administrator password.
- The password should consist of 8 to 32 non-blank characters and contain at least two types of characters among upper case, lower case, number, and special character (excluding ' " ; : &).

After the initialization is completed, the standby screen is displayed.

Figure 3-2 Standby screen



## 3.3 Standby Screen

You can unlock the door through fingerprint, passwords, and card.

- After 30 seconds of inactivity, the Standalone goes to screensaver mode when the screensaver is enabled and pictures have been imported for screensaver play; After 30 seconds screensaver play, the Standalone goes to the standby mode.
- The screens in this manual are only for reference, and might differ from the actual product.

Figure 3-3 Standby screen

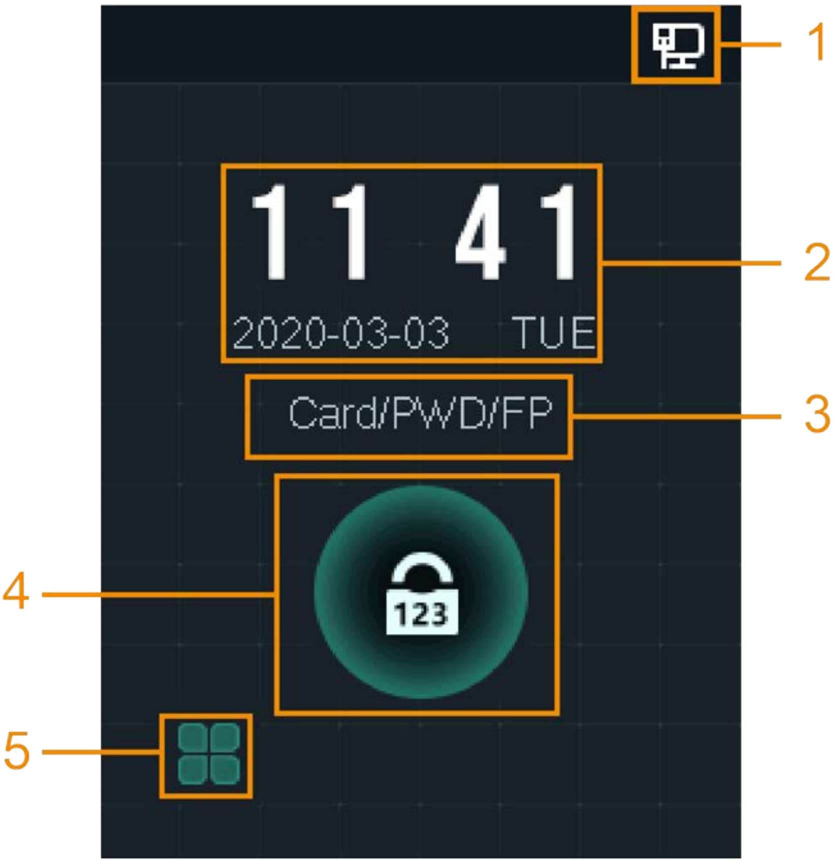


Table 3-2 Standby screen description

| No. | Description |
|---|---|
| 1 | Network status. |
| 2 | Date & Time: Current date and time. |
| 3 | Displays the configured unlock methods. |
| 4 | Password unlock icon. |
| 5 | Main menu icon.<br>📖<br>Only the administrator can enter the main menu. |

## 3.4 Unlocking Method

You can unlock the door through card, password, fingerprint, and the combination mode. For details, see "3.7.1 Setting Unlock Mode."

### 3.4.1 User Password

Enter the user passwords, and then you can unlock the door.

Step 1 Tap 🔒 on the standby screen.

Step 2 Tap PWD, and enter the user ID, and then tap **OK**.

Step 3 Enter the user password, and then tap **OK**.

Step 4 Tap □.

The door is unlocked.

### 3.4.2 Administrator Password

Enter the administrator password, and then you can unlock the door. The administrator password can unlock the door without being subject to user levels, unlock modes, periods, holiday plans, and anti-passback.

- You can only set one administrator password for a single Standalone.
- The DSS client can issue up to 100 passwords for a single Standalone.
- Administrator is not the password that was set during initialization.

Step 1 Tap 123 on the home screen.

Step 2 Tap Admin PWD.

Step 3 Enter the administrator password, and then tap **OK**.

The door is unlocked.

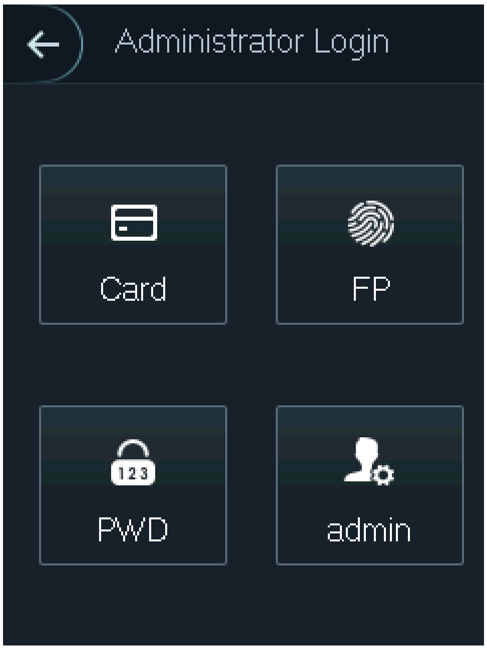
You can set and enable Administrator PWD on the **Administrator PWD** screen.

## 3.5 Logging in to the Main Menu

Administrators can add users of different levels, configure access control, network, and more.

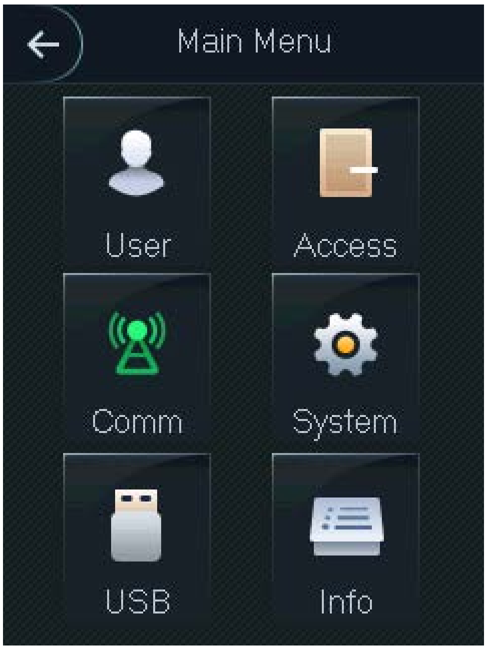
Step 1 Tap ⊞ on the standby screen.

Figure 3-4 Administrator login



Step 2 Select a login method to enter the main menu.

Figure 3-5 Main menu



## 3.6 User Management

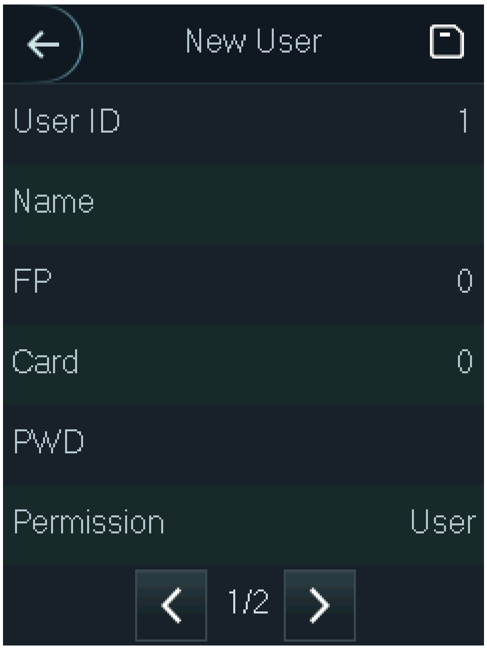
You can add new users, view user lists, admin lists, and change the administrator password on the **User** screen.

### 3.6.1 Adding New User

You can add new users by entering user IDs, names, importing fingerprints, cards, passwords, and more.

Step 1 Tap , and then tap .

Figure 3-6 New user



New User

User ID 1

Name

FP 0

Card 0

PWD

Permission User

Step 2 Configure parameters on the screen.

Table 3-3 New user parameter description

| Parameter | Description |
|---|---|
| User ID | You can enter user IDs. The ID consist of 18 characters (including numbers and letters, but not special characters), and each ID is unique. |
| Name | You can enter names with at most 32 characters (including numbers, symbols, and letters). |
| FP | Fingerprint registration. Enroll the user's fingerprints. |
| Card | Card registration. Record the card information. |
| PWD | The door unlocking password. The maximum length is 8. |
| Permission | Set the user's permission: **User** or **Admin**.<br>● User: **User** only has the permission to unlock the door.<br>● Admin: **Admin** has the permission to unlock the door and configure the Standalone. |
| Period | Set a period during which the user can unlock the door. |
| Holiday Plan | Set a holiday plan in which the user can unlock the door. |
| Valid Date | Set a date during which the door access of the user is valid. |
| User Type | ● **General**: General users can unlock the door normally.<br>● **Restricted**: When users in the blocklist unlock the door, the service personnel will receive notifications.<br>● **Guest**: Guests have very limited door access during specified periods. When they run out of access times, they cannot unlock the door.<br>● **Patrol**: Patrolling users can get their attendance tracked, but they have no unlock authority.<br>● **VIP**: When VIP users unlock the door, service personnel will receive notifications.<br>● **Other**: When special users (such as people with a physical disability and pregnant people) unlock the door, there will be a delay of 5 seconds before the door is closed. |

| Parameter | Description |
|---|---|
| Use Time | When the user level is **Guest**, you can set the maximum number of times that the guest can unlock the door. |

Step 3 Tap 🖫 to save changes.

### 3.6.2 Viewing User Information

You can search for users, view user list and admin list, enable administrator password, and delete user information through the **User** screen.

## 3.7 Access Management

Configure access control, including unlock modes, door status, lock holding time, door sensor type, and remote verification, and more.

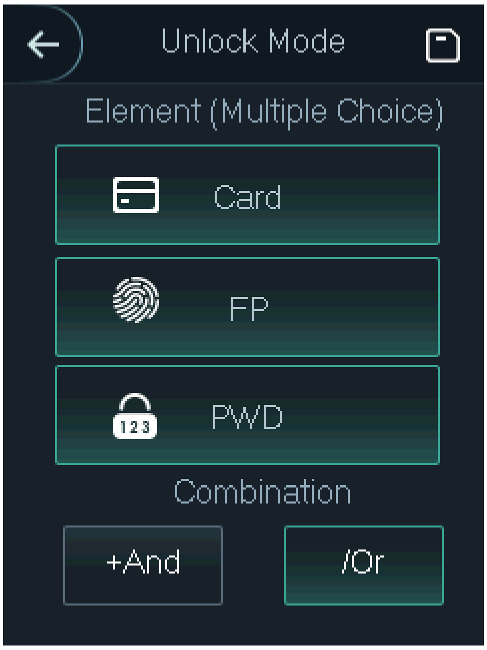
Tap Access to go to the access management screen.

### 3.7.1 Setting Unlock Mode

When the **Unlock Mode** is configured, users can unlock the door through card, password, fingerprint, and their combinations.

Step 1 Select **Access** > **Unlock Mode**.

Figure 3-7 Element (multiple choice)



Step 2 Select unlock mode(s).

To cancel selection, tap a selected unlock mode again.

Step 3 Select a combination mode.

- **+ And** means "and". For example, when you select **Card** and **FP**, you need to swipe your card first, and then get your fingerprint scanned to unlock the door.
- **/ Or** means "or". For example, when you select card/FP, you can either swipe your card or get your fingerprints scanned to unlock the door.

Step 4 Tap 💾 to save changes.

Step 5 Enable the **Unlock Mode**.

- means enabled.
- means not enabled.

## 3.7.2 Setting Door Status

There are three options: **NO**, **NC**, and **Normal**.

- NO (Normally open): The door remains open all the time.
- NC (Normally close): The door remains closed all the time.
- Normal: The door access is controlled according to your settings.

## 3.7.3 Setting Lock Holding Time

**Lock Holding Time** is the duration during which the door remains unlocked before it automatically locks again.

## 3.7.4 Setting Door Sensor Type

There are two door sensor types: **NO** and **NC**.

## 3.7.5 Setting Remote Verification

Tap **Remote Verification** to set time, and then tap to enable it. Remote verification is required when a person attempts to unlock the door.

- means enabled.
- means not enabled.

## 3.8 Network Communication

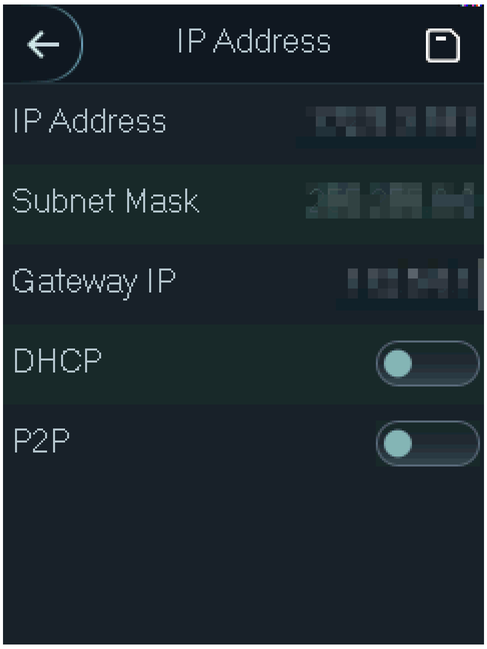
Configure network, serial ports and Wiegand ports to make sure the Standalone can work properly.

## 3.8.1 Configuring IP

### 3.8.1.1 Setting IP Address

Configure the IP address of the Standalone to connect it to the network.

Figure 3-8 IP address configuration



IP Address

IP Address [redacted]

Subnet Mask [redacted]

Gateway IP [redacted]

DHCP ○

P2P ○

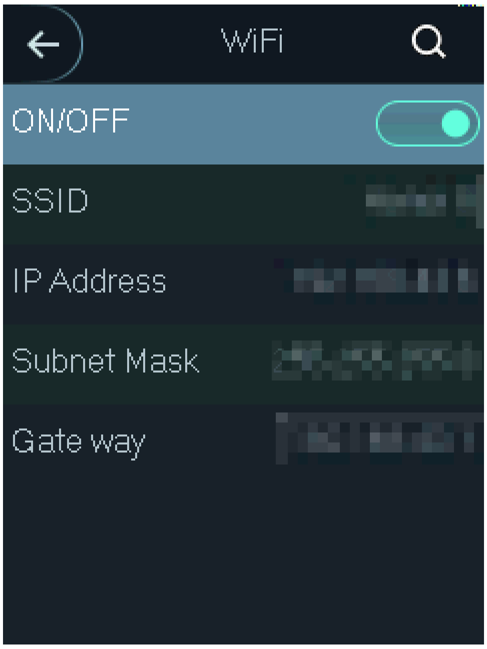
Table 3-4 IP configuration parameters

| Parameter | Description |
|---|---|
| IP Address/Subnet Mask/Gateway IP Address | The IP address, subnet mask, and gateway IP address must be on the same network segment. After configuration, tap 💾 to save changes. |
| DHCP | DHCP (Dynamic Host Configuration Protocol).<br>When the DHCP is enabled, the IP address is automatically obtained, and the IP address, subnet mask and gateway IP address cannot be manually configured. |
| P2P | P2P is a private network traversal technology which enables user to manage devices without DDNS, port mapping or transit server. |

### 3.8.1.2 Setting Wi-Fi

Connect the Standalone to the network through Wi-Fi when the Wi-Fi function is enabled.

Figure 3-9 Wi-Fi



WiFi

ON/OFF

SSID [redacted]

IP Address [redacted]

Subnet Mask [redacted]

Gate way [redacted]

## 3.8.2 Configuring Wiegand

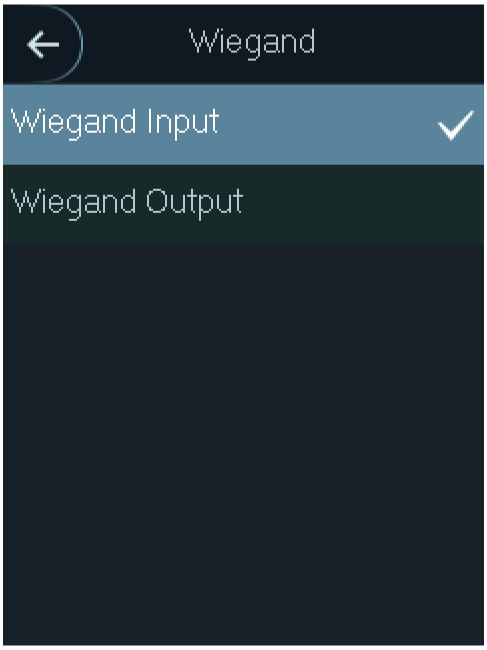
Configure Wiegand input or output to connect a card reader or access controller.

Step 1 Select **Comm** > **Wiegand**.

Step 2 Select Wiegand Input or Wiegand Output.

- Select **Wiegand Input** when an external card reader is connected to the Standalone.
- Select **Wiegand Output** when the Standalone functions as a card reader and you need to connect it to another access controller.

Figure 3-10 Wiegand



Wiegand

Wiegand Input ✓

Wiegand Output

Table 3-5 Wiegand output

| Parameter | Description |
|---|---|
| Wiegand output type | The Wiegand output type determines the card number or the digit of the number than can be read by the Standalone.<br>● Wiegand26, three bytes, six digits.<br>● Wiegand34, four bytes, eight digits.<br>● Wiegand66, eight bytes, sixteen digits. |
| Pulse Width | Set pulse width and pulse interval. |
| Pulse Interval | |
| Output Data Type | You can select the types of output data.<br>● **User ID**: Outputs the ID of the user who swipes a card.<br>● **Card No.**: Outputs the card number that is used. |

## 3.8.3 Configuring TCP Port

The range is 1025-65535, and it is 37777 by default. If you modify the port, the system will restart automatically.

## 3.8.4 Configuring Serial Port

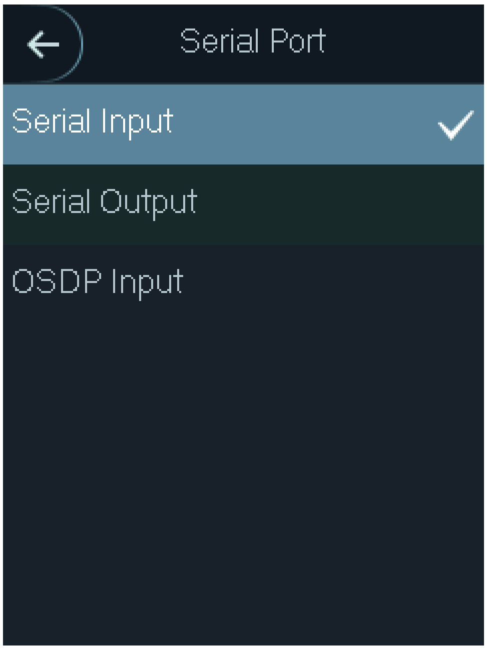
Select serial input or serial output according to connection directions.

Step 1 Select **Comm** > **Serial Port**.

Step 2 Configure serial port.

- Select **Serial Input** when an external card reader is connected to the Standalone. The card information will be sent to the Standalone and the management platform.
- Select **Serial Output** when the Standalone functions as a card reader, and the Standalone sends card number or user ID to a controller.
- Select **OSDP Input** when the Standalone connects a card reader through the OSDP protocol.

Figure 3-11 Serial port



## 3.9 System Configuration

### 3.9.1 Setting Time

Configure the time of the Standalone, such as date, time, and date format.

### 3.9.2 Setting Volume

Tap − or + to adjust the volume.

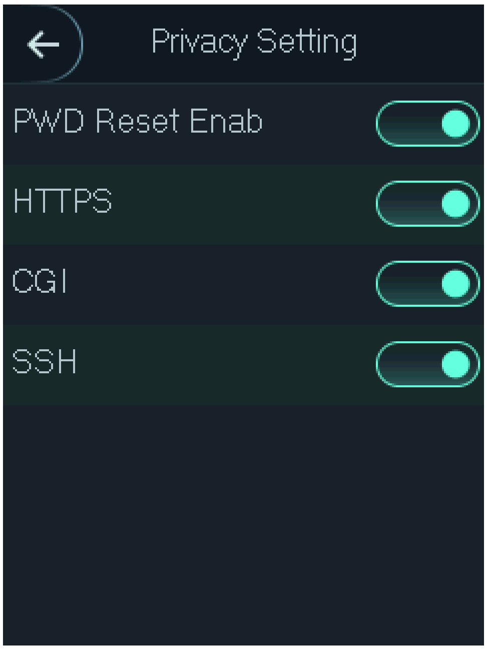
### 3.9.3 Setting ScreenSaver

Enable **ScreenSaver**, the screen saver is displayed after 30 seconds of inactivity.

- To display the screen saver, you need to import pictures first. For details, see "3.10.4 Screensaver."
- ○● means enabled.
- ●○ means not enabled.

### 3.9.4 Setting Privacy

Figure 3-12 Privacy setting



Privacy Setting

PWD Reset Enab ○●

HTTPS ○●

CGI ○●

SSH ○●

Table 3-6 Features

| Parameter | Description |
|---|---|
| PWD Reset Enable | If the **PWD Reset Enable** function is enabled, you can reset the password.<br>The PWD Reset function is enabled by default. |
| HTTPS | Hypertext Transfer Protocol Secure (HTTPS) is a protocol for secure communication over a computer network.<br>When HTTPS is enabled, HTTPS will be used to access CGI commands; otherwise HTTP will be used. |
| CGI | Common Gateway Interface (CGI) offers a standard protocol for web servers to execute programs that execute like console applications running on a server that generates web pages dynamically.<br>When CGI is enabled, CGI commands can be used. The CGI is enabled by default. |
| SSH | Secure Shell (SSH) is a cryptographic network protocol for operating network services securely over an unsecured network.<br>When SSH is enabled, SSH provides cryptographic service for the data transmission. |

When HTTPS is enabled, the Standalone will restart automatically.

## 3.9.5 Setting Card No. Reverse

When the third-party card reader is connected to the Standalone through the Wiegand output port, you need to enable the Card No. Reverse function; otherwise the communication between the Standalone and the third-party card reader might fail because of protocol discrepancy.

## 3.9.6 Setting Auto Test

When you use the Standalone for the first time or when the Standalone malfunctions, use auto test function to check whether the Standalone can work properly.

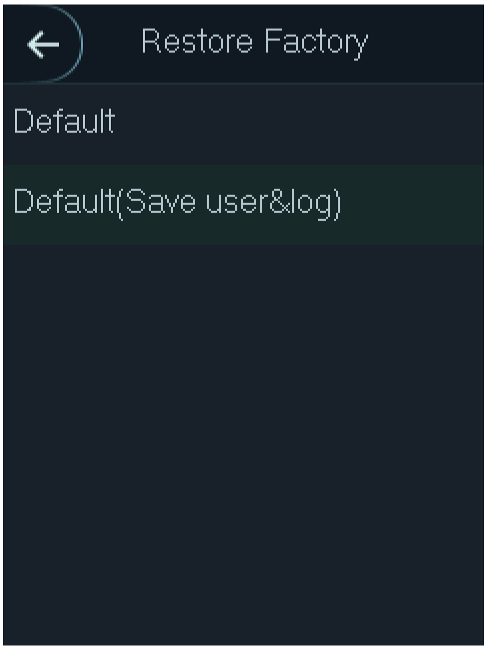
## 3.9.7 Restoring to Default Settings

Data will be lost if you restore the Standalone to factory defaults. Please be advised.

You can select whether to retain user information and logs.

- Tap **Default** to restore the Standalone to the factory defaults and deletes all data, including users, device information, and logs.
- Tap **Default (Save user&log)** to restores factory defaults and deletes all data except user information and logs.

Figure 3-13 Restore factory



### 3.9.8 Restarting the Standalone

Select **System > Reboot**, tap **Yes**, and the Standalone will restart.

## 3.10 USB Management

⚠

- USB can also be used to update the system.
- Make sure that a USB drive is inserted to the Standalone before exporting user information or upgrading system. To avoid failure, do not pull out the USB drive or perform any operation during the process.
- If you want to import data from one device to another, you must export the data to a USB drive first.

### 3.10.1 Exporting to USB

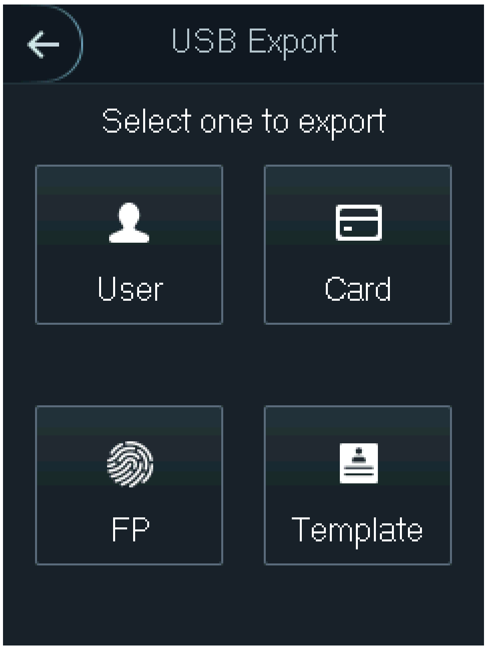
Export data from the Standalone to USB. The exported template is in .xml format, and you can edit user information and import it to the Standalone. The first three pieces of information are encrypted and cannot be edited.

Only the FAT32 file system is supported.

Step 1 Select **USB** > **USB Export**.

The **USB Export** screen is displayed.

Figure 3-14 Export to USB



Step 2 Select the data type that you want to export.

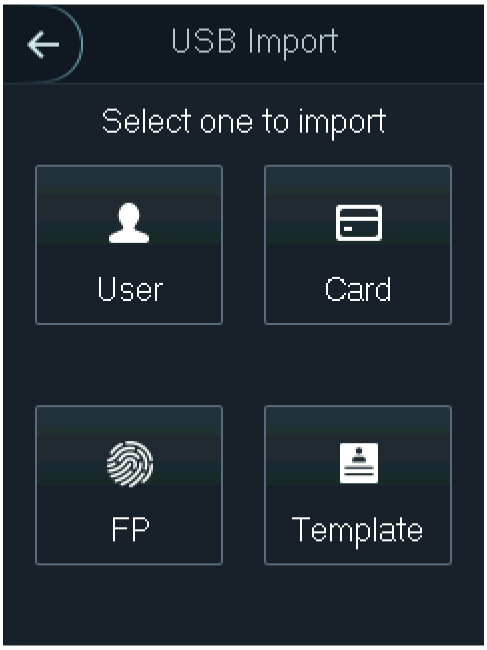
Step 3 Tap **OK**.

## 3.10.2 Importing from USB

You can import data from USB to the Standalone.

Step 1 Select **USB** > **USB Import**.

Figure 3-15 USB import



Step 2 Select the data type that you want to import.

Step 3 Tap **OK**.

### 3.10.3 Updating System

You can use a USB drive to update the system of the Standalone.

Step 1 Rename the updating file name to "update.bin", and save the "update.bin" file in the root directory of the USB.

Step 2 Select **USB** > **USB Update**.

The prompt **Confirm to Update** is displayed.

Step 3 Tap **OK**.

The Standalone restarts when update is complete.

### 3.10.4 Importing Pictures

Insert a USB, and tap **ScreenSaver** to import pictures to the Standalone from the USB.

- The picture format should be .png, and .jpg is not supported.
- The pictures must be in the same scale with 240 × 320.
- The picture name must be Screensaver1-5.

### 3.10.5 Exporting Records

You can search for and export all unlocking records.

## 3.11 System Information

You can search all unlocking records, and view data capacity and device version on the **System Info** screen.

# 4 Web Configuration

Open the web browser on your computer. Log in to the web portal to configure and update the Standalone.

## 4.1 Initialization

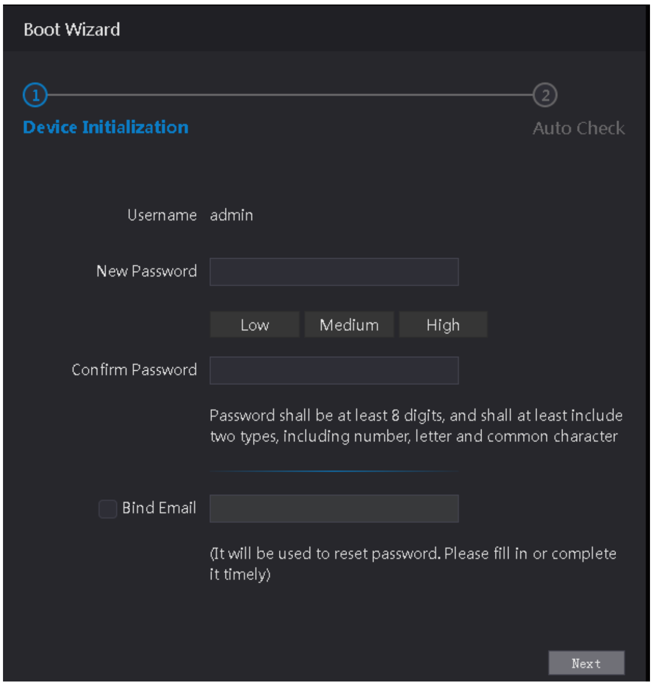
Set your password and link an email address before logging in to the web portal for the first time.

Step 1 Open IE web browser, go to the IP address (the default address is 192.168.1.108) of the Standalone.

The **Initialization** window is displayed.

- Use browsers newer than IE 8.
- Make sure the computer is on the same LAN as the Standalone.

Figure 4-1 Initialization



Boot Wizard

Username admin

New Password

Confirm Password

Password shall be at least 8 digits, and shall at least include two types, including number, letter and common character

□ Bind Email

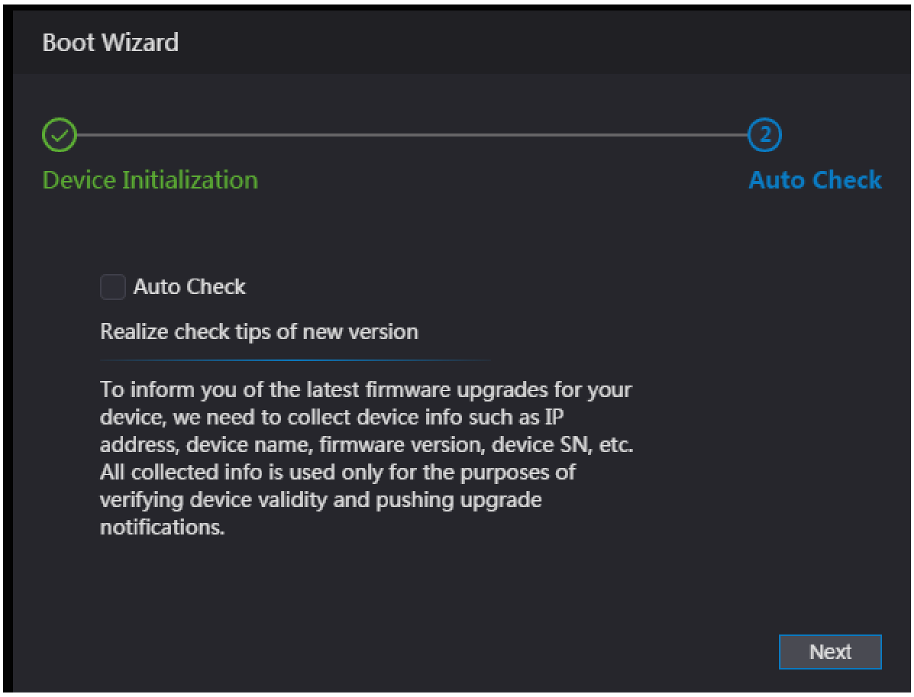
(It will be used to reset password. Please fill in or complete it timely)

Step 2 Enter the new password, confirm password, link an email address, and then tap **Next**.

- For security, keep the password properly after initialization and change the password regularly.
- The password must consist of 8 to 32 non-blank characters and contain at least two types of the following characters: upper case, lower case, numbers, and special characters (excluding ' " ; : &). Set a high-security password by following the password strength prompt.
- When you need to reset the administrator password by scanning the QR code, you need the linked email address to receive the security code.

Step 3 Click **Next**.

Figure 4-2 Auto check



□ Auto Check

Realize check tips of new version

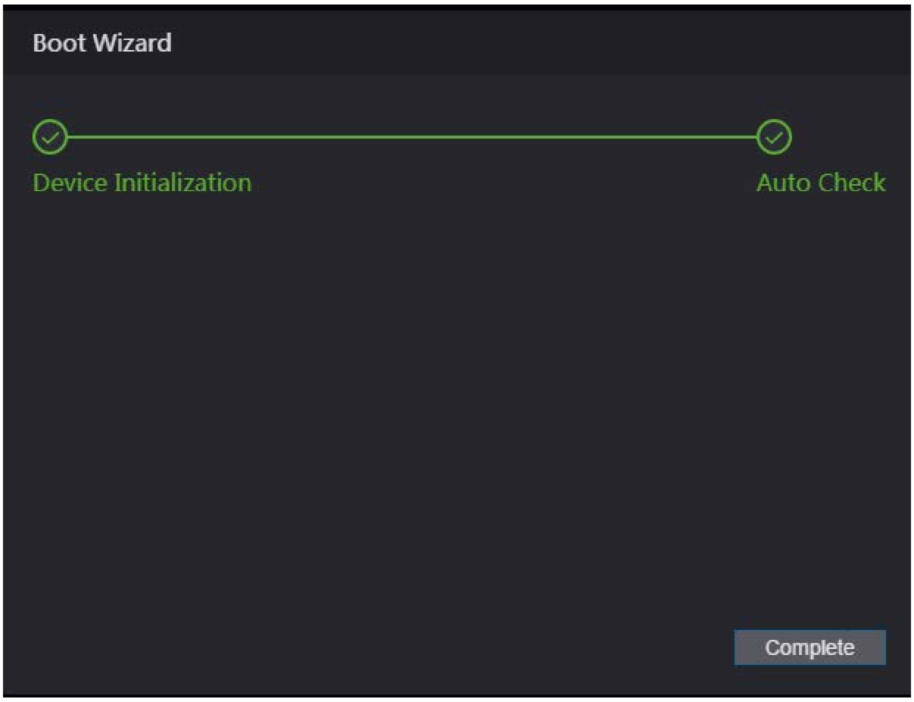
To inform you of the latest firmware upgrades for your device, we need to collect device info such as IP address, device name, firmware version, device SN, etc. All collected info is used only for the purposes of verifying device validity and pushing upgrade notifications.

Step 4 (Optional) Select **Auto Check**.

We recommend you to select **Auto Check** to get the latest version in time.

Step 5 Click **Next**.

Figure 4-3 Finished configuration



Step 6 Click **Complete**.

## 4.2 Logging In

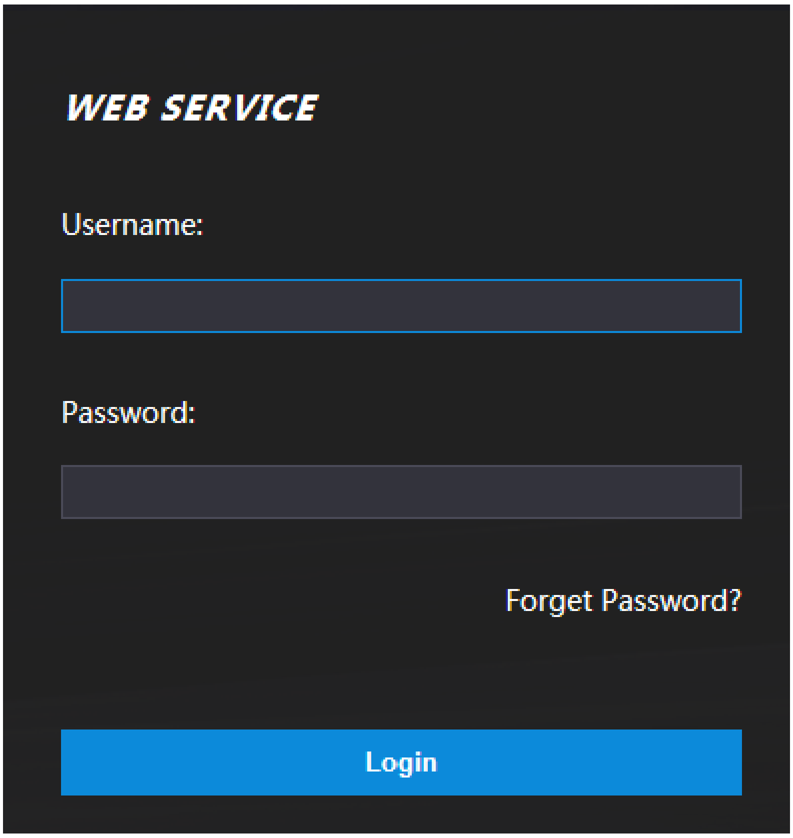
Step 1 Open IE web browser, go to the IP address of the Standalone.

Make sure the computer is on the same LAN as the Standalone.

Step 2 Enter the username and password.

- The default administrator name is admin, and the password is the login password after initializing the Standalone. Change the password regularly and keep it properly to improve security.
- When you forget the administrator login password, click **Forget password?** to reset it. For details, see "4.3 Resetting the Password."

Figure 4-4 Login



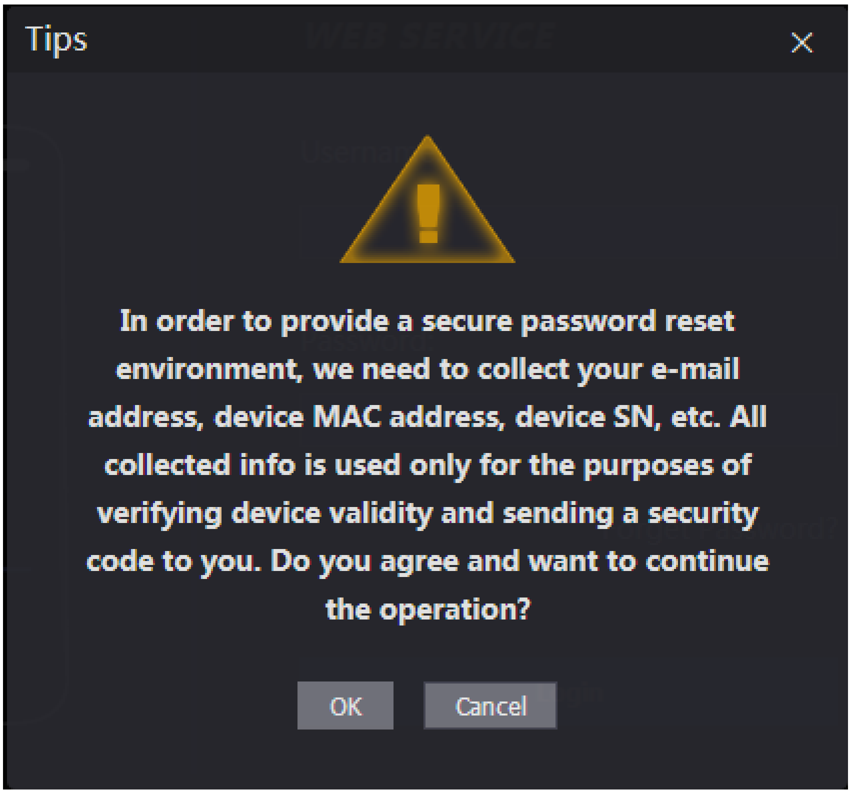
Step 3 Click **Login**.

## 4.3 Resetting the Password

When resetting the password of the admin account, your email address is required.

Step 1 Click **Forget password?** on the login window.

Figure 4-5 Tips

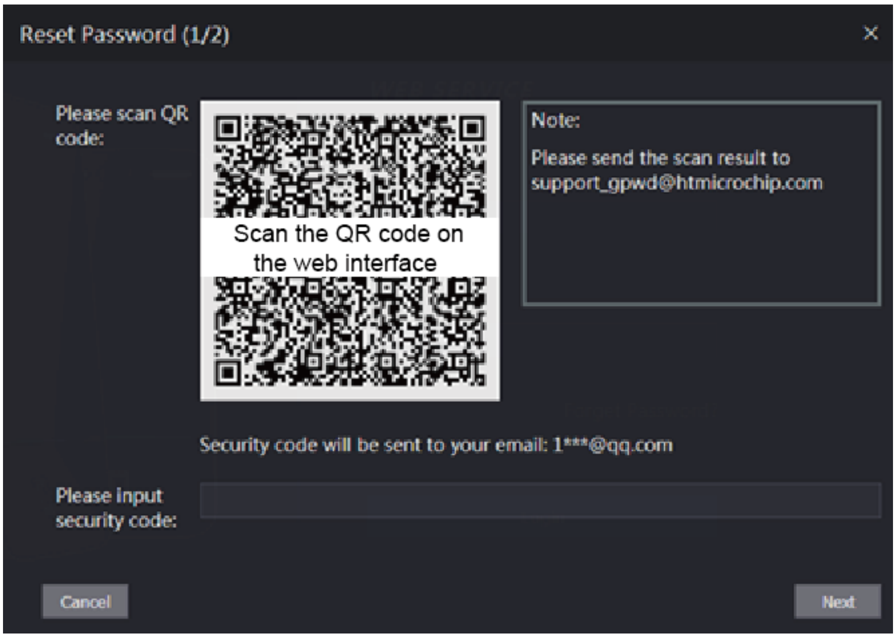


Tips

In order to provide a secure password reset environment, we need to collect your e-mail address, device MAC address, device SN, etc. All collected info is used only for the purposes of verifying device validity and sending a security code to you. Do you agree and want to continue the operation?

Step 2 Read the prompt message, and click **OK**.

Figure 4-6 Reset password



Reset Password (1/2)

Please scan QR code:

Note:

Please send the scan result to support_gpwd@htmicrochip.com

Security code will be sent to your email: 1***@qq.com

Please input security code:

Step 3 Scan the QR code on the window, and you will receive the security code.

- A maximum of two security codes will be generated by scanning the same QR code. If security codes become invalid, refresh the QR code and scan again.
- After you scanned the QR code, send the content that you received to the designated email address, and then you will receive a security code.
- Use the security code within 24 hours after you receive it. Otherwise, it will become invalid. If wrong security codes are entered for consecutive five times, the administrator will be frozen for five minutes.

Step 4 Enter the security code you have received.

Step 5 Click **Next**.

The **Reset Password** window is displayed.

Step 6 Reset and confirm the new password.

The password must consist of 8 to 32 non-blank characters and contain at least two types of the following characters: upper case, lower case, numbers, and special characters (excluding ' " ; : &). Set a high-security password by following the password strength prompt.

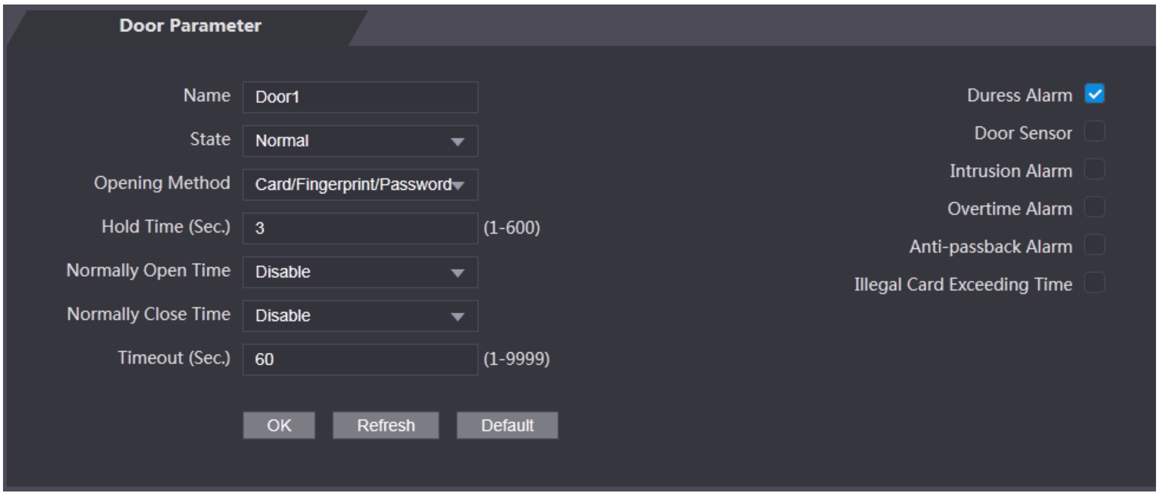
Step 7 Click **OK**.

## 4.4 Configuring Door Parameter

Set the door parameters such as door status, unlock methods and alarms.

Step 1 Click **Door Parameter**.

Figure 4-7 Door parameter



Door Parameter

Name: Door1

State: Normal

Opening Method: Card/Fingerprint/Password

Hold Time (Sec.): 3 (1-600)

Normally Open Time: Disable

Normally Close Time: Disable

Timeout (Sec.): 60 (1-9999)

Duress Alarm ☑

Door Sensor □

Intrusion Alarm □

Overtime Alarm □

Anti-passback Alarm □

Illegal Card Exceeding Time □

Step 2 Set the door parameters.

Table 4-1 Door parameter description

| Parameter | Description |
|---|---|
| Name | Enter a door name. |
| State | There are three options: **Normal**, **NC**, and **NO**.<br>● NO (Normally open): The door remains open all the time.<br>● NC (Normally close): The door remains closed all the time.<br>● Normal: The door access is controlled according to your settings. |
| Opening Method | Select a unlock method. |
| Hold Time (Sec.) | The duration in which the door is remain unlocked before it automatically locks again, and the range is 1 second –600 seconds. |
| Normally Open Time | Select the period that you set in **Time Section**. During the defined period, the door remains open. It is turned on by default. |
| Normally Close Time | Select the period that you set in **Time Section**. During the defined period, the door remains closed. It is turned on by default. |
| Timeout (Sec.) | A timeout alarm is triggered if the door remains unlocked for longer time than the defined time. |

Step 3 Enable the alarms.

The intrusion alarm and timeout alarm can be triggered only when **Door Sensor** is enabled.

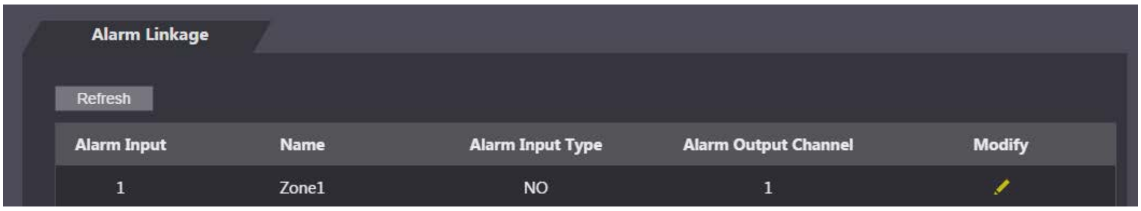
# 4.5 Alarm Linkage Configuration

## 4.5.1 Setting Alarm Linkage

Alarm input devices can be connected to the Standalone, and you can modify the alarm linkage parameters.

Step 1 Select **Alarm Linkage** > **Alarm Linkage**.

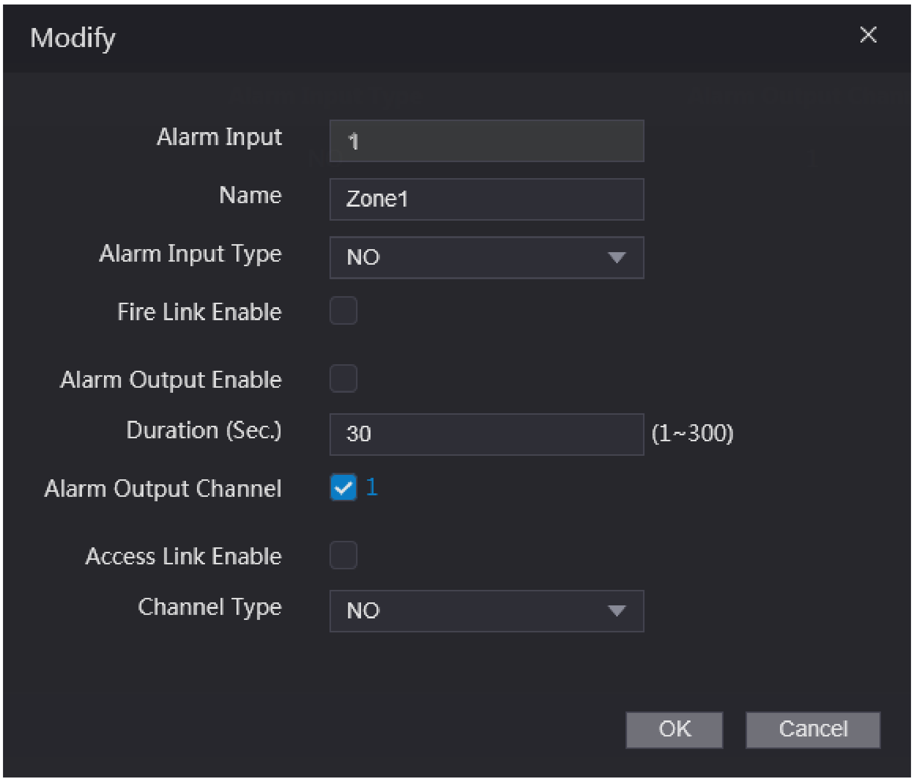
Figure 4-8 Alarm linkage



| Alarm Input | Name | Alarm Input Type | Alarm Output Channel | Modify |
|---|---|---|---|---|
| 1 | Zone1 | NO | 1 | ✏ |

Step 2 Click ✏ to configure alarm linkage.

Figure 4-9 Modifying alarm linkage parameter



Alarm Input: 1

Name: Zone1

Alarm Input Type: NO

Fire Link Enable: □

Alarm Output Enable: □

Duration (Sec.): 30 (1~300)

Alarm Output Channel: ☑ 1

Access Link Enable: □

Channel Type: NO

Table 4-2 Alarm linkage parameter description

| Parameter | Description |
|---|---|
| Alarm Input | You cannot modify the value. Keep it default. |
| Name | Enter a zone name. |

| Parameter | Description |
|---|---|
| Alarm Input Type | There are two options: **NO** and **NC**.<br>**NO**: The circuit of the alarm device is normally open, and it closes when an alarm is triggered.<br>**NC**: The circuit of the alarm device is normally closed, and it opens when an alarm is triggered. |
| Fire Link Enable | If fire link is enabled, the Standalone will output alarms when fire alarms are triggered. The alarm details are displayed in the alarm log.<br>Alarm output and access link are NO by default if fire link is enabled. |
| Alarm Output Enable | The relay can output alarm messages (will be sent to the management platform) if the **Alarm Output** is enabled. |
| Duration (Sec.) | The alarm duration, and the range is 1–300 seconds. |
| Alarm Output Channel | Select an alarm output channel according to the alarm device. Each alarm device can be regarded as a channel. |
| Access Link Enable | After the **Access Link** is enabled, the Standalone will be normally open or normally closed when there are input alarm signals. |
| Channel Type | There are two options: **NO** and **NC**. |

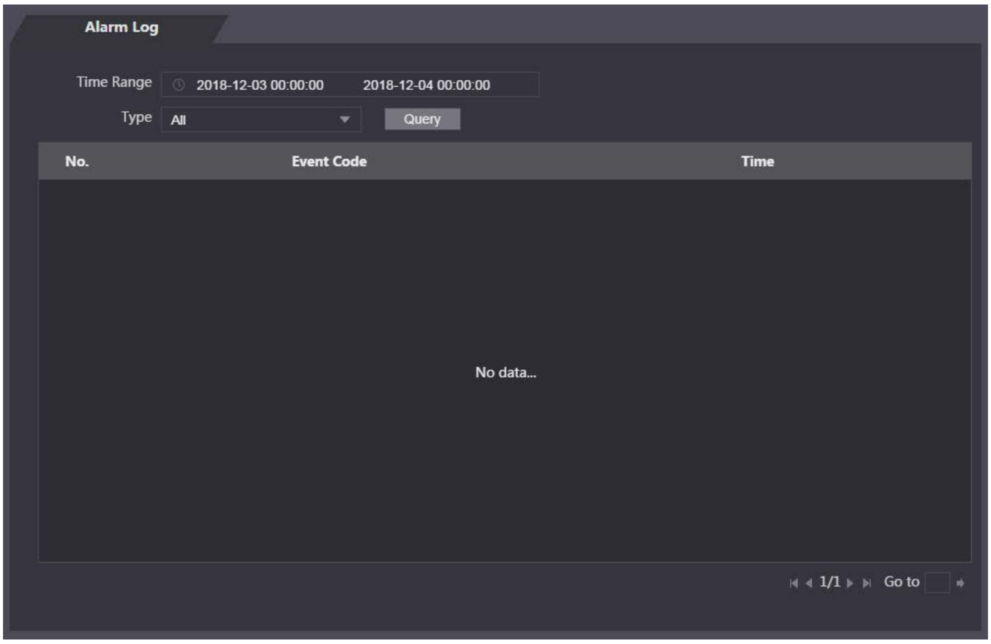
Step 3 Click **OK**.

The configurations on the web client will be synchronized with the desktop client if the Standalone is added to the desktop client.

## 4.5.2 Viewing Alarm Log

Step 1 Select **Alarm Linkage** > **Alarm Log**.

Figure 4-10 Alarm log



Time Range 2018-12-03 00:00:00 2018-12-04 00:00:00

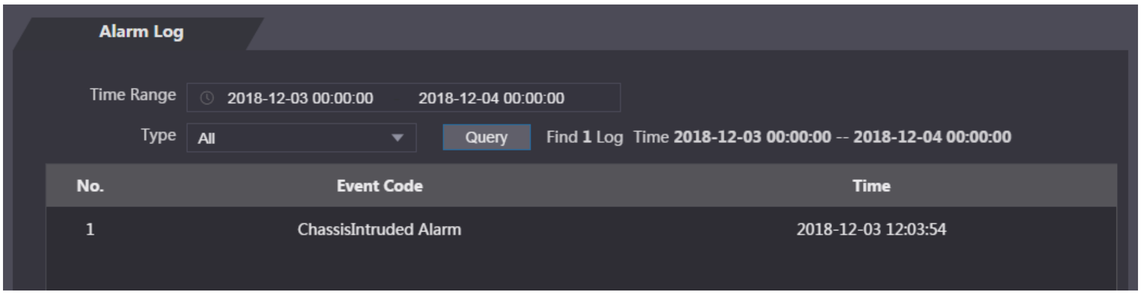
Type All

| No. | Event Code | Time |
|---|---|---|

No data...

Step 2 Select a time range and alarm type, and then click **Query**.

Figure 4-11 Query results



Time Range 2018-12-03 00:00:00 2018-12-04 00:00:00

Type All

Find 1 Log Time 2018-12-03 00:00:00 -- 2018-12-04 00:00:00

| No. | Event Code | Time |
|---|---|---|
| 1 | ChassisIntruded Alarm | 2018-12-03 12:03:54 |

## 4.6 Time Section Configuration

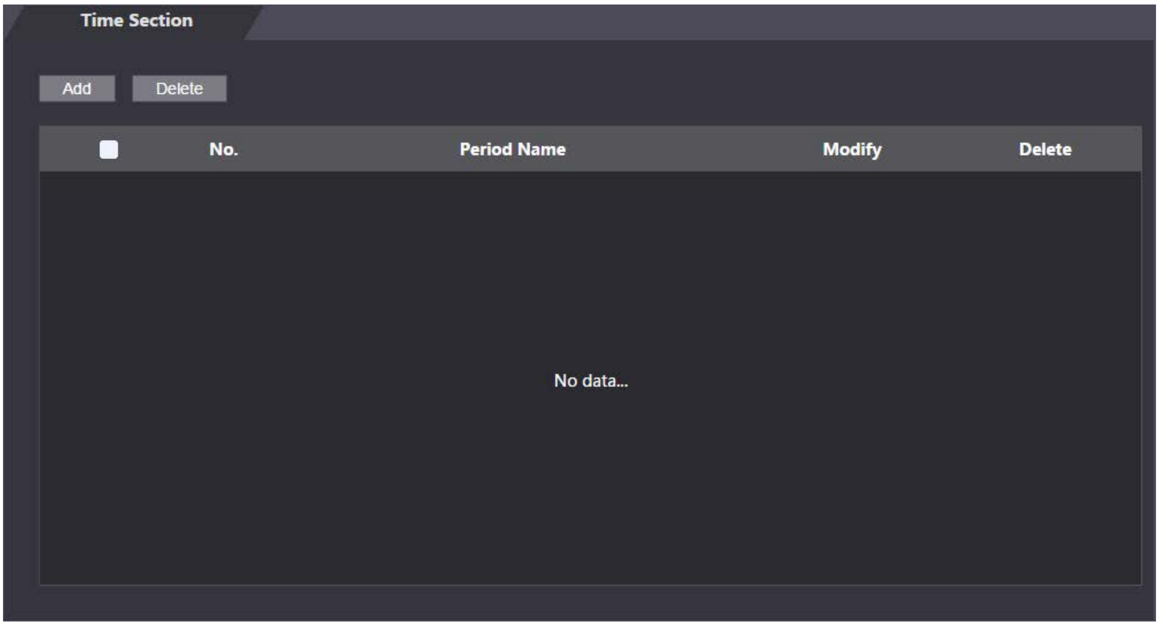
Configure time sections and holiday plans, and then you can define when a user has the permissions to unlock doors.

### 4.6.1 Setting Time Section

You can configure up to 128 groups (from No.0 through No.127) of time section. In each group, you need to configure door access schedules for a whole week. A user can only unlock the door during the scheduled time.

Step 1 Select **Time Section** > **Time Section**.

Figure 4-12 Time section

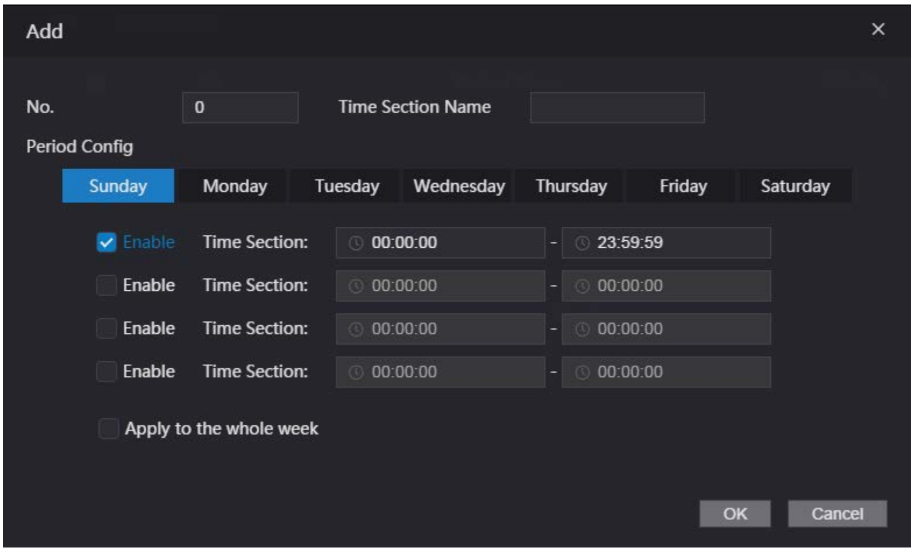


| □ | No. | Period Name | Modify | Delete |
|---|---|---|---|---|

No data...

Step 2 Click **Add**.

Figure 4-13 Add period


Add

No. 0  Time Section Name

Period Config

Sunday | Monday | Tuesday | Wednesday | Thursday | Friday | Saturday

☑ Enable Time Section: 00:00:00 - 23:59:59

□ Enable Time Section: 00:00:00 - 00:00:00

□ Enable Time Section: 00:00:00 - 00:00:00

□ Enable Time Section: 00:00:00 - 00:00:00

□ Apply to the whole week

Step 3 Enter No. and name for the time section.

- **No.**: Enter a section number. It ranges from 0 through 127.
- **Time Section Name**: Enter a name for each time section. You can enter a maximum of 32 characters (contain number, special characters and English characters).

Step 4 Configure time sections for each day.

You can configure up to four time sections for a single day.

Step 5 (Optional) Click **Apply to the whole week** to copy the configuration to the rest of days.

Step 6 Click **OK** to save the changes.

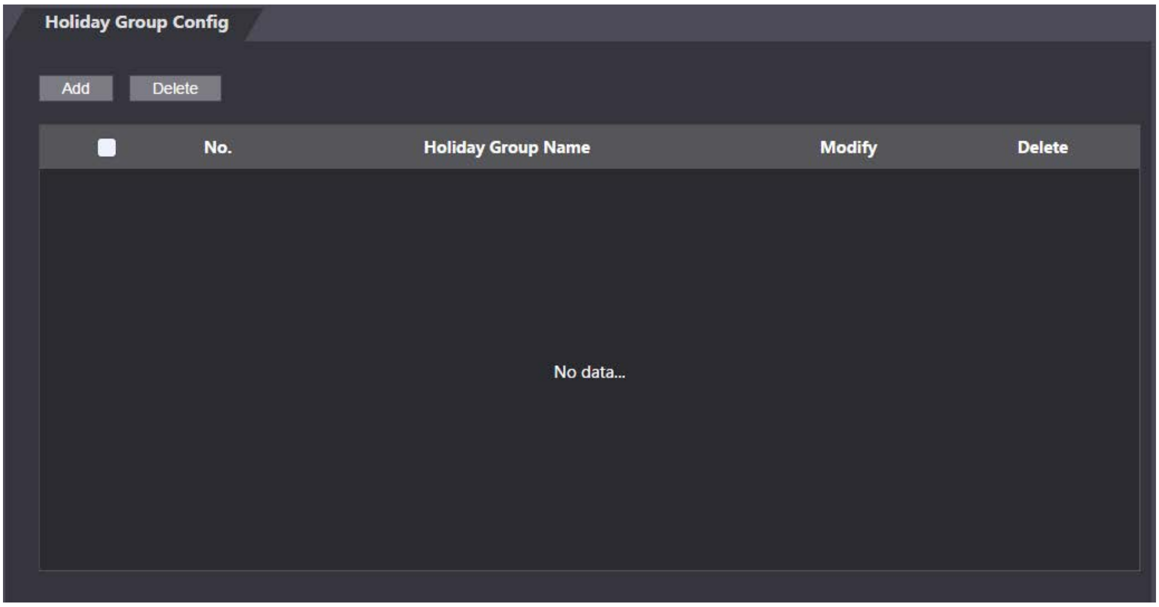
## 4.6.2 Setting Holiday Group

Configure the start time and end time of a holiday group, and then users cannot unlock the door in specified periods.

Set time sections for different holiday groups. You can configure up to 128 holiday groups (from No.0 through No.127). and up to 16 time sections for a single holiday group. Users can unlock doors in the defined time sections.

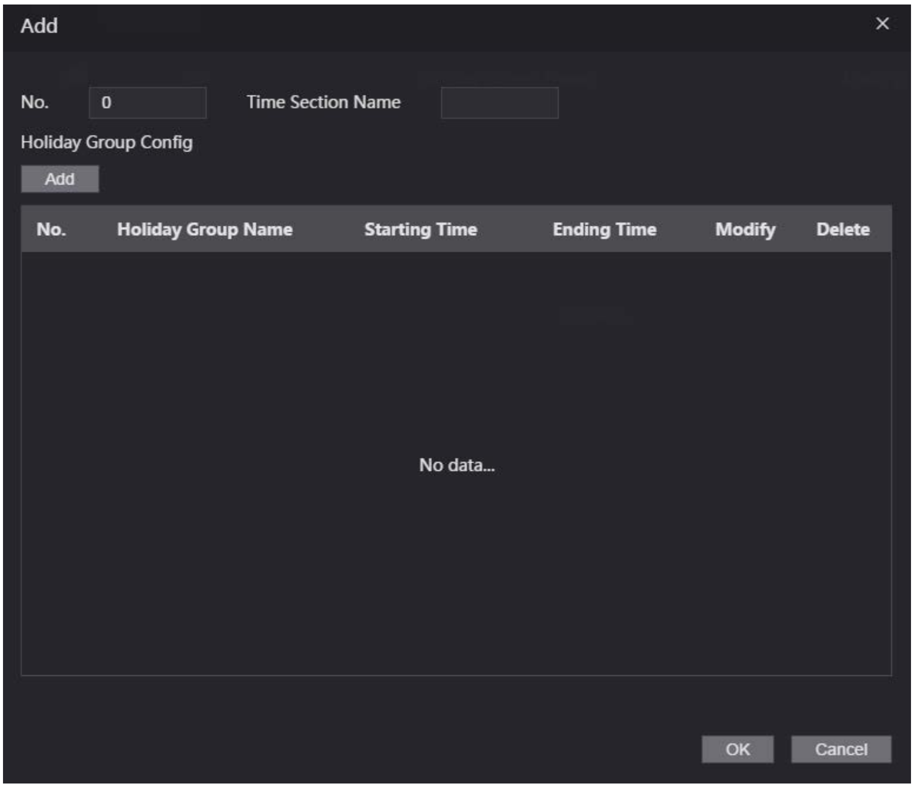
Step 1 Select **Time Section** > **Holiday Group Config**.

Figure 4-14 Holiday group configuration



Step 2 Click **Add**.

Figure 4-15 Add holiday group



Step 3 Enter a number and a name for the holiday group.

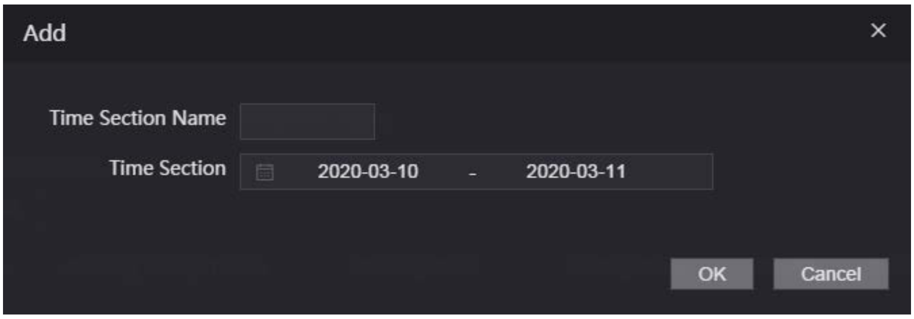
- **No.**: Enter a section number. It ranges from 0 through 127.
- **Time Section Name**: Enter a name for each time section. You can enter a maximum of 32 characters (contain numbers, special characters and English characters).

Step 4 Click **Add**.

Step 5 Enter a name in the **Time Section Name** box, select the start date and end date, and then click **OK**.

You can add multiple holidays for one holiday group.

Figure 4-16 Add holiday group configuration



Time Section Name

Time Section 2020-03-10 - 2020-03-11

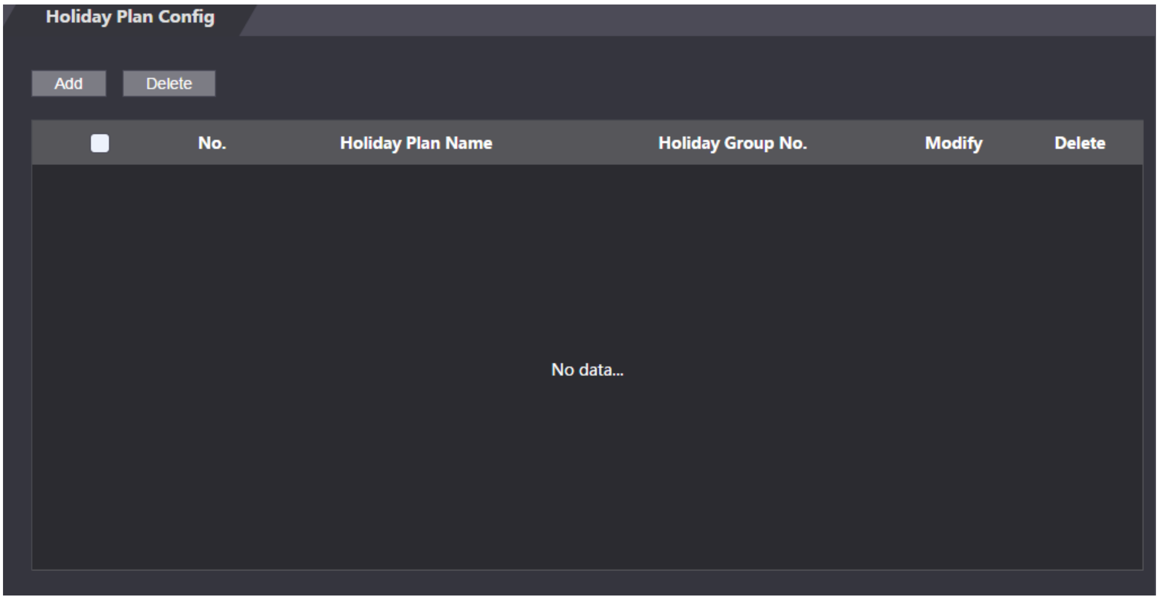
Step 6 Click **OK**.

### 4.6.3 Setting Holiday Plan

Assign the configured holiday groups to the holiday plan. Users can only unlock the door in the specified time in the holiday plan.

Step 1 Select **Time Section** > **Holiday Plan Config**.

Figure 4-17 Holiday plan configuration

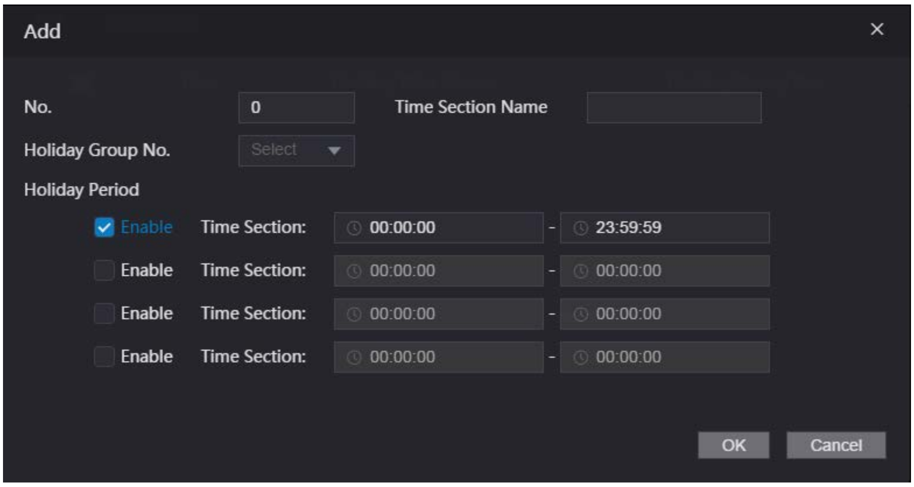


| □ | No. | Holiday Plan Name | Holiday Group No. | Modify | Delete |
|---|---|---|---|---|---|

No data...

Step 2 Click **Add**.

Figure 4-18 Add holiday plan



No. 0 Time Section Name

Holiday Group No. Select

Holiday Period

☑ Enable Time Section: 00:00:00 - 23:59:59

□ Enable Time Section: 00:00:00 - 00:00:00

□ Enable Time Section: 00:00:00 - 00:00:00

□ Enable Time Section: 00:00:00 - 00:00:00

Step 3 Enter a number and name for the holiday plan.

- **No.**: Enter a section number. It ranges from 0 through 127.
- **Time Section Name**: Enter a name for each time section. You can enter a maximum of 32 characters (contain numbers, special characters and English characters).

Step 4 In the **Holiday Group No.** list, select the holiday group that you have configured.

📖

Select **255** if you do not want to select a holiday group.

Step 5 In the **Holiday Period** area, configure time sections in the holiday group. You can configure up to four time sections.

Step 6 Click **OK**.

# 4.7 Data Capacity

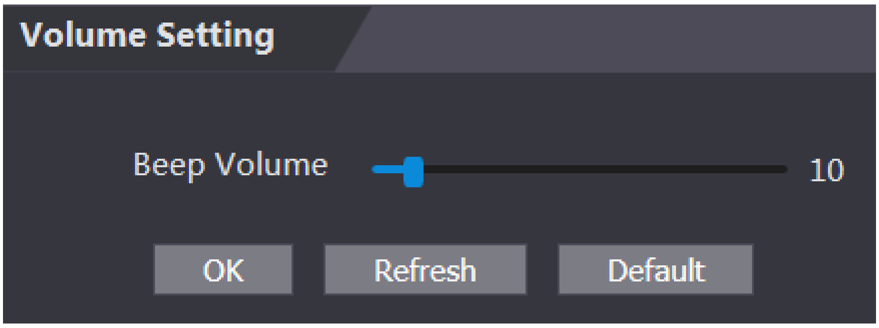
View data capacity such as users, cards, and fingerprints that the Standalone can store.

# 4.8 Setting Volume

Step 1 Log in to the web page.

Step 2 Click **Volume Setting**, and adjust the volume.

Figure 4-19 Volume setting



Beep Volume 10

# 4.9 Network Configuration

## 4.9.1 Setting TCP/IP

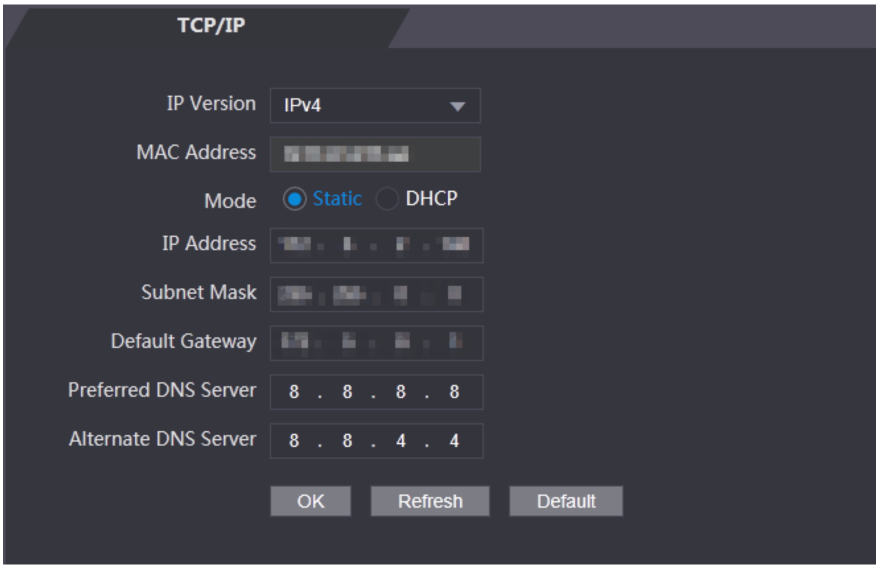
Configure IP address and DNS server so that the Standalone can communicate with other devices.

📖

Make sure that the Standalone is connected to the network.

Step 1 Select **Network Setting** > **TCP/IP**.

Figure 4-20 TCP/IP



TCP/IP

IP Version: IPv4

MAC Address: [redacted]

Mode: ● Static ○ DHCP

IP Address: [redacted]

Subnet Mask: [redacted]

Default Gateway: [redacted]

Preferred DNS Server: 8 . 8 . 8 . 8

Alternate DNS Server: 8 . 8 . 4 . 4

Step 2 Configure parameters.

Table 4-3 TCP/IP

| Parameter | Description |
|---|---|
| IP Version | IPv4. |
| MAC Address | MAC address of the Standalone. |
| Mode | ● **Static**: Set IP address, subnet mask, and gateway address manually.<br>● **DHCP**<br>◇ After DHCP is enabled, IP address, subnet mask, and gateway address cannot be configured.<br>◇ If DHCP is effective, IP address, subnet mask, and gateway address will be assigned by DHCP automatically.<br>◇ If you disable DHCP, the default IP will be displayed. |
| IP Address | Enter IP address, and then configure subnet mask and gateway address.<br>🕮<br>IP address and gateway address must be in the same network segment. |
| Subnet Mask | |
| Default Gateway | |
| Preferred/ Alternate DNS Server | Set IP address of the preferred DNS server. |

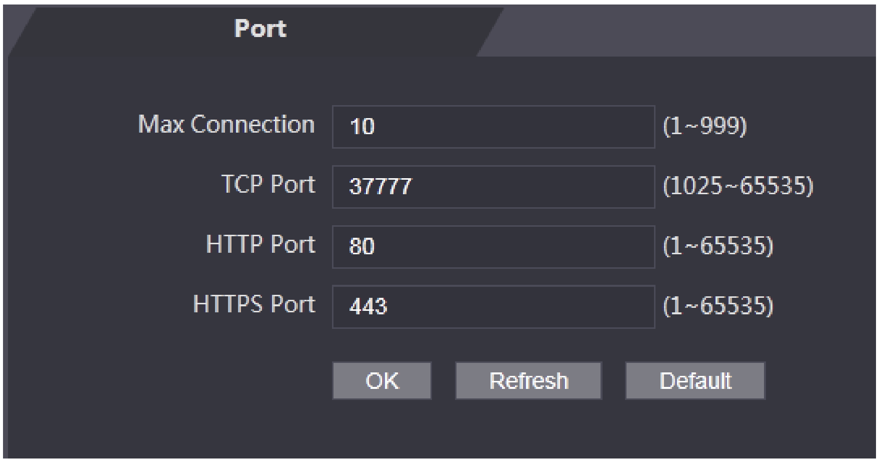
Step 3 Click **OK**.

## 4.9.2 Setting Port

You can limit access to the Standalone at the same time by computer and phone.

Step 1 Select **Network Setting** > **Port**.

Figure 4-21 Port



Port

Max Connection 10 (1~999)

TCP Port 37777 (1025~65535)

HTTP Port 80 (1~65535)

HTTPS Port 443 (1~65535)

Step 2 Configure port numbers.

Except **Max Connection**, you need to restart the Standalone to make your configurations effective.

Table 4-4 Port description

| Parameter | Description |
|---|---|
| Max Connection | Set the maximum access to the Standalone through clients.<br>Clients like SmartPSS are not counted. |
| TCP Port | The value is 37777 by default. |
| HTTP Port | The value is 80 by default. If you want to change the port number, add the changed port number after the address when you log in through a web browser. |
| HTTPS Port | The value is 443 by default. |

Step 3 Click **OK**.

### 4.9.3 Setting P2P

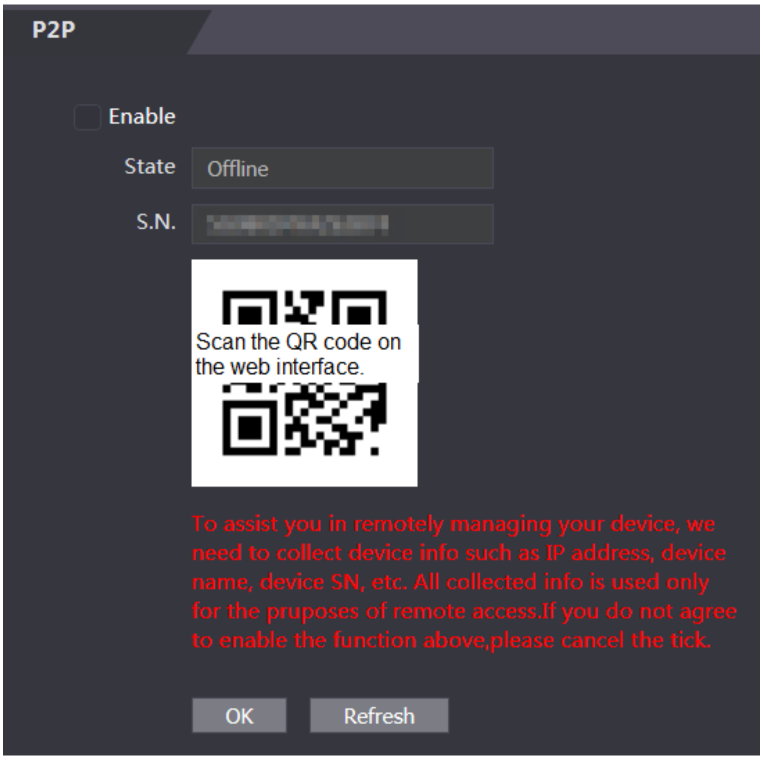
Peer-to-peer computing or networking is a distributed application architecture that partitions tasks or workloads between peers. Users can download mobile application by scanning QR code, and then register an account. You can manage multiple devices on the mobile application. Dynamic domain name, port mapping, and transit server are not required.

⚠

If you want to use P2P, connect the Standalone to the Internet; otherwise this function cannot work properly.

Step 1 Select **Network Setting** > **P2P**.

Figure 4-22 P2P


P2P

□ Enable

State: Offline

S.N.:

Scan the QR code on the web interface.

To assist you in remotely managing your device, we need to collect device info such as IP address, device name, device SN, etc. All collected info is used only for the pruposes of remote access.If you do not agree to enable the function above,please cancel the tick.

Step 2 Select **Enable** to enable P2P function.

Step 3 Click **OK**.

Scan the QR code on the P2P window to get the serial number of the Standalone.

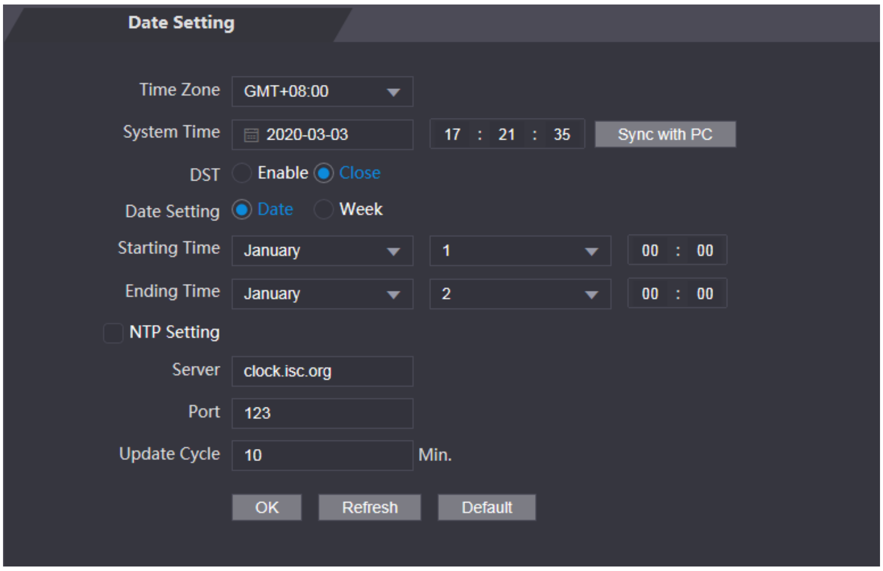
## 4.10 Setting Data

You can configure time zone, system time, DST (Daylight Saving Time) or NTP (Network Time Protocol).

Step 1 Log in to the web page.

Step 2 Click **Date Setting**.

Figure 4-23 Date setting


Date Setting

Time Zone: GMT+08:00

System Time: 2020-03-03 17 : 21 : 35 Sync with PC

DST: ○ Enable ● Close

Date Setting: ● Date ○ Week

Starting Time: January 1 00 : 00

Ending Time: January 2 00 : 00

□ NTP Setting

Server: clock.isc.org

Port: 123

Update Cycle: 10 Min.

Table 4-5 Data setting description

| Parameter | Description |
|---|---|
| Time Zone | Configure the time zone. |
| System Time | Configure system time.<br>Click **Sync with PC**, and the system time changes to the PC time. |
| DST | 1. (Optional) Enable DST.<br>2. Select **Date** or **Week** in **Sate Setting**.<br>3. Configure start time and end time. |
| NTP Setting | 1. Select the **NTP Setting** checkbox.<br>2. Configure parameters.<br>● **Server**: Enter the domain of a NTP server, and the Standalone will automatically sync time with NTP server.<br>● **Port**: Enter the port of the NTP server.<br>● **Update Cycle**: Enter time synchronization interval. |

Step 3 Click **OK**.

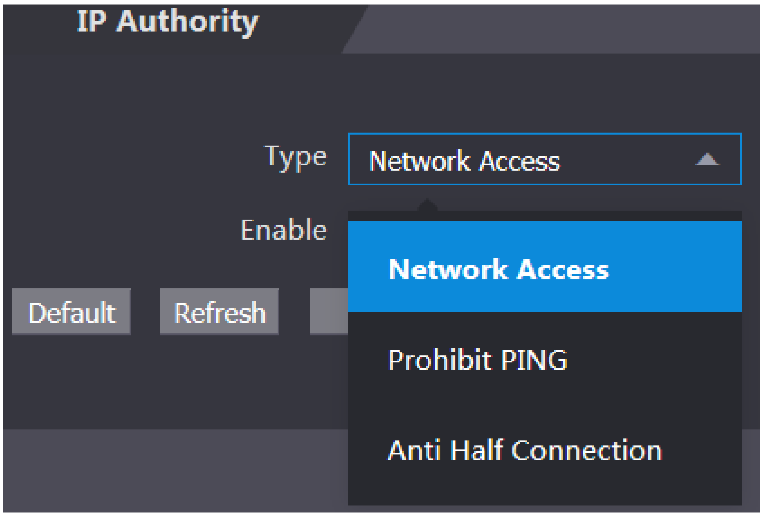
# 4.11 Safety Management

## 4.11.1 Configuring IP Authority

Step 1 Log in to the web page.

Step 2 Click **Safety Mgmt.** > **IP Authority**.

Figure 4-24 IP authority



Step 3 Select a cybersecurity mode in the **Type** list.

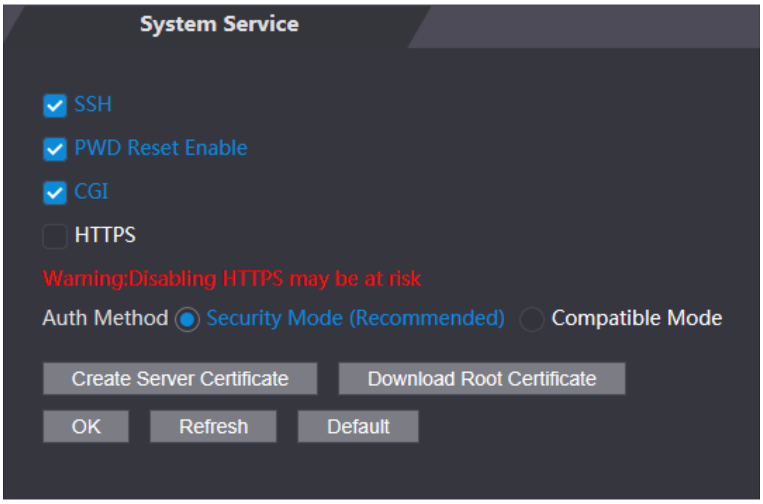
- **Network Access**: Set allowlist and blocklist to control access to the Standalone.
  - ◇ **Allowlist**: a list of trusted IP/MAC addresses that has access to the Standalone.
  - ◇ **Blocklist**: a list of blocked IP/MAC addresses that has no access to Standalone.
- **Prohibit PING**: Enable **PING prohibited** function, and the Standalone will not respond to the Ping request.
- **Anti Half Connection**: Enable **Anti Half Connection** function, and the Standalone can still function properly under half connection attack.

### 4.11.2 Configuring System Service

There are four options: SSH, PWD Reset Enable, CGI, and HTTPS. For details, see "3.9.4 Privacy Setting."

The system service configurations on the web client will be synchronized with the configurations on the **Privacy Setting** of the Standalone.

Figure 4-25 System service



System Service

☑ SSH

☑ PWD Reset Enable

☑ CGI

□ HTTPS

Warning:Disabling HTTPS may be at risk

Auth Method ● Security Mode (Recommended) ○ Compatible Mode

Table 4-6 Description of system service

| Parameter | Description |
|---|---|
| SSH | Secure Shell (SSH) is a cryptographic network protocol for operating network services securely over an unsecured network.<br>When SSH is enabled, SSH provides cryptographic service for the data transmission. |
| PWD Reset Enable | If enabled, you can reset the password. This function is enabled by default. |
| CGI | Common Gateway Interface (CGI) offers a standard protocol for web servers to execute programs similarly to console applications running on a server that dynamically generates web pages.<br>When CGI is enabled, CGI commands can be used. The CGI is enabled by default. |
| HTTPS | Hypertext Transfer Protocol Secure (HTTPS) is a protocol for secure communication over a computer network.<br>When HTTPS is enabled, HTTPS will be used to access CGI commands; otherwise HTTP will be used.<br>When HTTPS is enabled, the Device will restart automatically. |
| Auth Method | ● **Security Mode (recommended)**: Supports logging in with Digest authentication.<br>● **Compatible Mode**: Compatible with the login method of old devices. |

## 4.11.3 User Management

You can add or delete users, change users' passwords, and link your email address for resetting the password when you forget it.

### 4.11.3.1 Adding Users

Step 1 Click **Add** on the **User Mgmt.** window

Step 2 Enter username, password, confirmation password, and remark.

Step 3 Click **OK**.

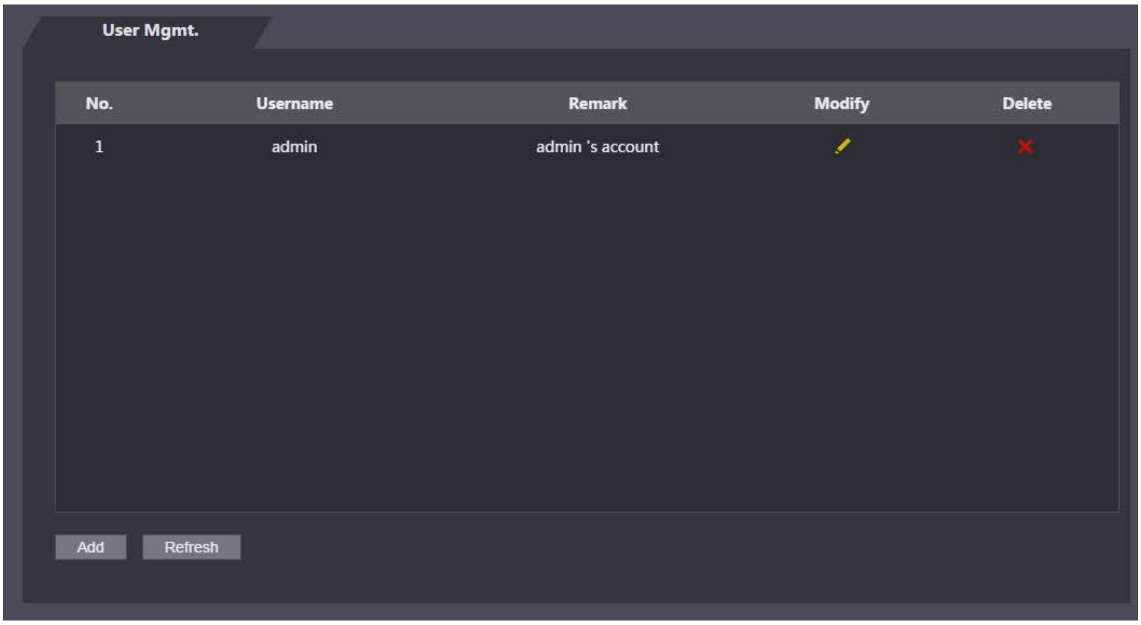
### 4.11.3.2 Changing Password

Step 1 Log in to the web page.

Step 2 Select **User Mgmt.** > **User Mgmt**.

Step 3 Click ✎.

Figure 4-26 User management



| No. | Username | Remark | Modify | Delete |
|---|---|---|---|---|
| 1 | admin | admin 's account | ✎ | ✕ |

Step 4 Select **Bind Email** and enter the email address.

Step 5 Select **Modify Password**, and then enter the old password, new password and confirm password.

Step 6 Click **OK**.

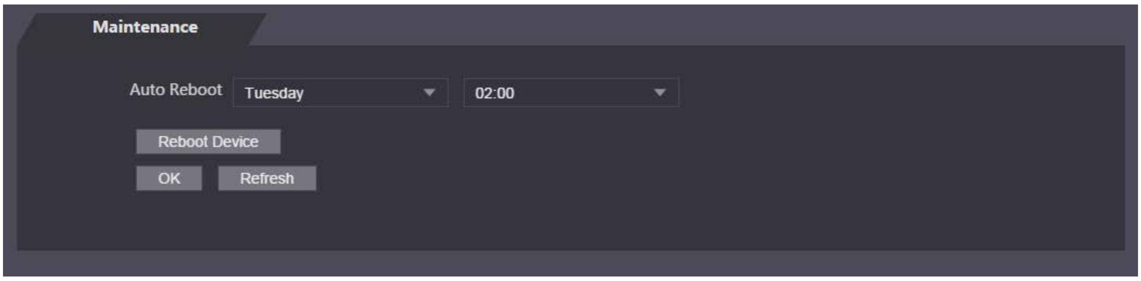
## 4.11.4 Maintenance

You can regularly restart the Standalone during idle time to improve its performance.

Step 1 Log in to the web page.

Step 2 Select **Maintenance**.

Figure 4-27 Maintenance



Step 3 Set the time, and then click **OK**.

The Device will restart at the defined the time.

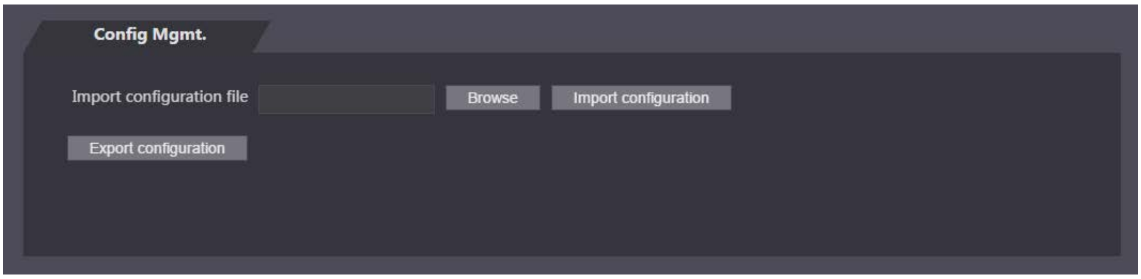
It is **Never** by default.

Step 4 (Optional) Click **Reboot Device**, and the Standalone will restart immediately.

### 4.11.5 Configuration Management

When more than one access controllers need the same configurations, you can configure parameters for them by importing or exporting configuration files.

Figure 4-28 Configuration management



### 4.11.6 Updating System

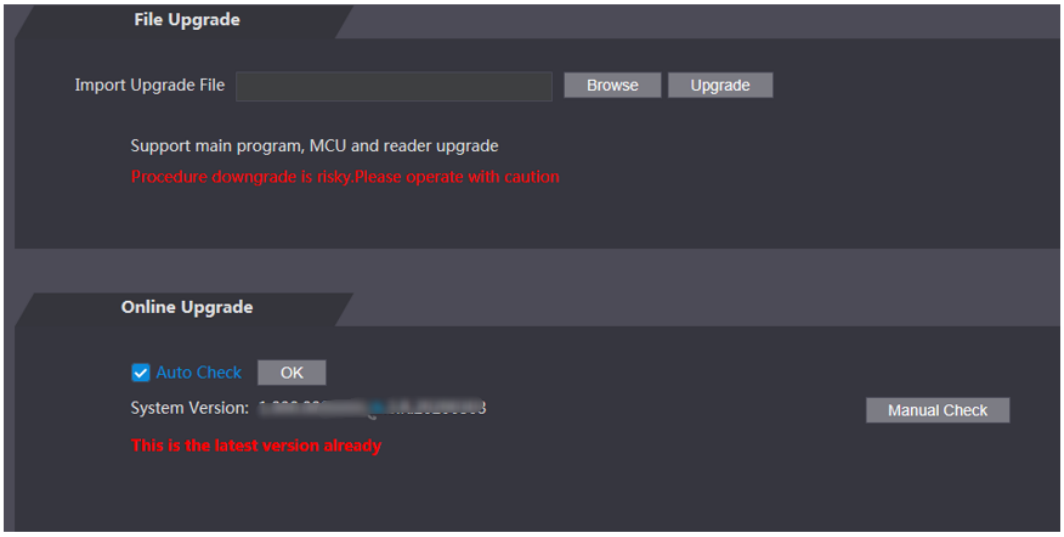
- Export the configuration file for backup before updating, and then import the file after the update completes.
- Use the correct update file. Make sure to get the correct update file from the technical support.

Do not disconnect the power or network, or restart or shut down the Standalone during the update.

Step 1 Log in to the web page.

Step 2 Select **Upgrade**.

Figure 4-29 Upgrade



Support main program, MCU and reader upgrade

Procedure downgrade is risky.Please operate with caution

System Version: [redacted]

This is the latest version already

Step 3 Select the update method.

- File Update

1) Click **Browse**, and then upload upgrade file.

   The upgrade file should be a .bin file.

2) Click **Upgrade**.

   The Device will restart after the update completes.

- Online Update

1) Select the **Auto-check** checkbox, and then click **OK**.

   The system checks for new version automatically.

   We need to collect the data such as device name, firmware version, and device serial number to proceed auto-check. The collected information is only used for verifying the legality of cameras and giving upgrade notification.

2) If there is any new version available, click **Upgrade**.

   The Standalone will restart after the update completes.

   Click **Manual Check** to check for new version manually.

## 4.11.7 Version Information

View information including MAC address, serial number, MCU version, web version, security baseline version, system version and firmware version.

Step 1 Log in to the web page.

Step 2 Select **Version Info** to view version information.

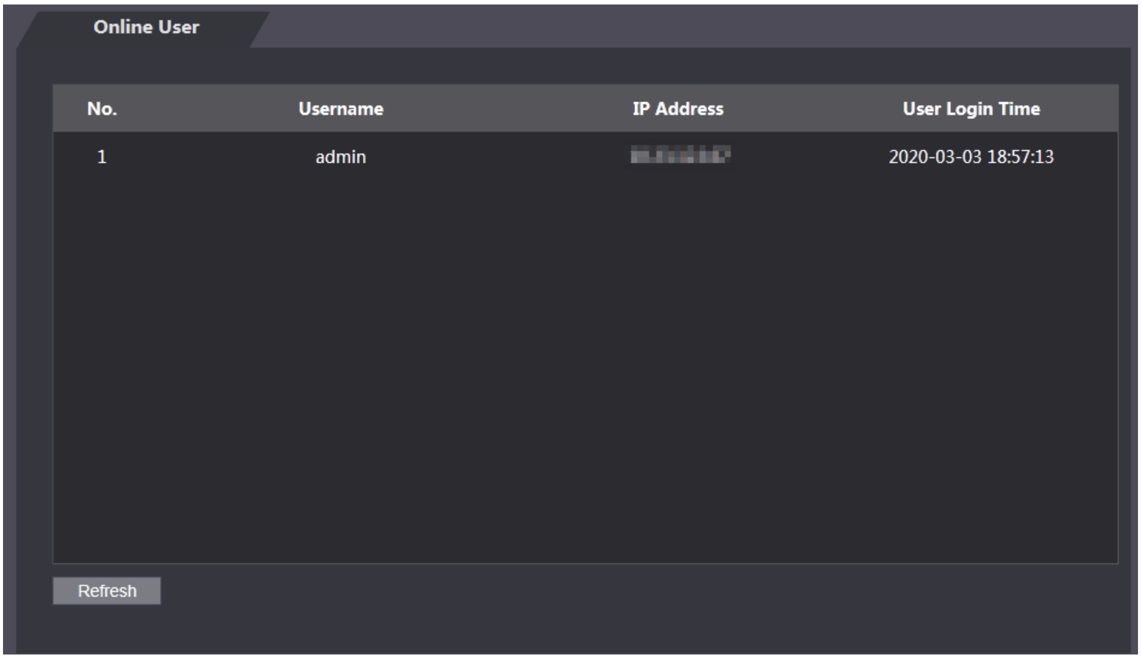
## 4.11.8 Viewing Online Users

You can view online users who log in to web, including their username, IP address, and login time.

Step 1 Log in to the web page.

Step 2 Select **Online User**.

Figure 4-30 Online user



| No. | Username | IP Address | User Login Time |
|---|---|---|---|
| 1 | admin | [redacted] | 2020-03-03 18:57:13 |

## 4.11.9 Viewing System Log

View and back up system logs, admin logs, and unlock records.

### 4.11.9.1 System Log

View and search for system logs.

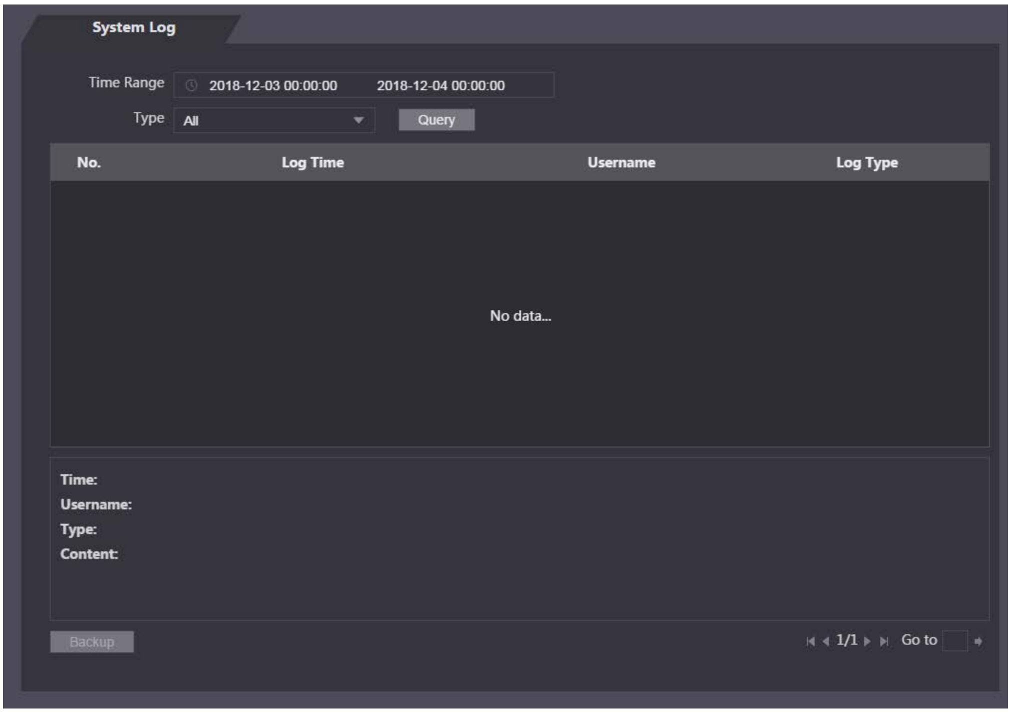
Step 1 Log in to the web page.

Step 2 Select **System Log** > **System Log**.

Step 3 Select the time range and the log type, and then click **Query**.

Click **Backup** to download the results.

Figure 4-31 System log



System Log

Time Range 2018-12-03 00:00:00 2018-12-04 00:00:00

Type All

Query

| No. | Log Time | Username | Log Type |
|---|---|---|---|

No data...

Time:
Username:
Type:
Content:

Backup

1/1 Go to

### 4.11.9.2 Admin Log

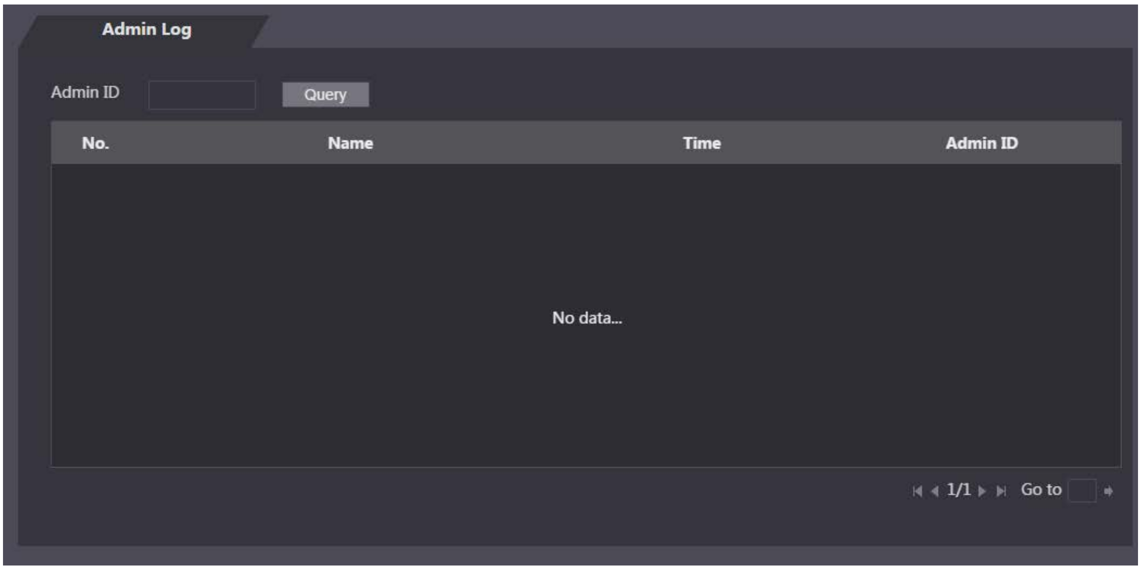
Search for admin logs by using admin ID.

Step 1 Log in to the web page.

Step 2 Select **System Log** > **Admin Log**.

Step 3 Enter the admin ID, and then click **Query**.

Figure 4-32 Admin log



Admin Log

Admin ID

Query

| No. | Name | Time | Admin ID |
|---|---|---|---|

No data...

1/1 Go to

## 4.12 Logging Out

Click ⇥ at the upper-left corner, and then click **OK** to log out of the web page.

# 5 Phone Configuration

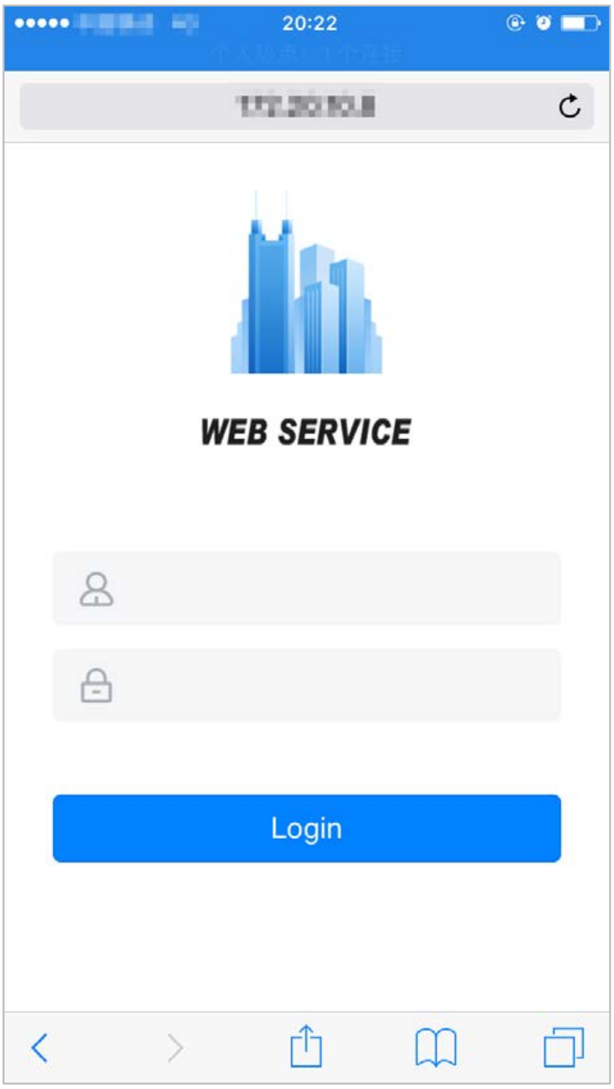
You can also log in to the web page of the Standalone through your phone.

📖

Make sure the Standalone is on the same LAN as your phone.

Step 1 Open the browser on the phone, go to the IP address (192.168.1.108 by default) of the Standalone.

Figure 5-1 Login



Step 2 Enter the username and password.

📖

The default username of administrator is admin, and the password is the login password after initializing the Standalone. We recommend you change the administrator password regularly to increase security.

Step 3 Click **Login**.

# 6 DSS Configuration

This chapter introduces how to manage and configure the Standalone through DSS client. For details, see "*DSS Professional User's Manual*".

📖

The windows of DSS Pro in the user manual are only for reference, and might differ from the actual product.

Download and install DSS client first. For details, see "*DSS Professional User's Manual*".

## 6.1 Adding Device

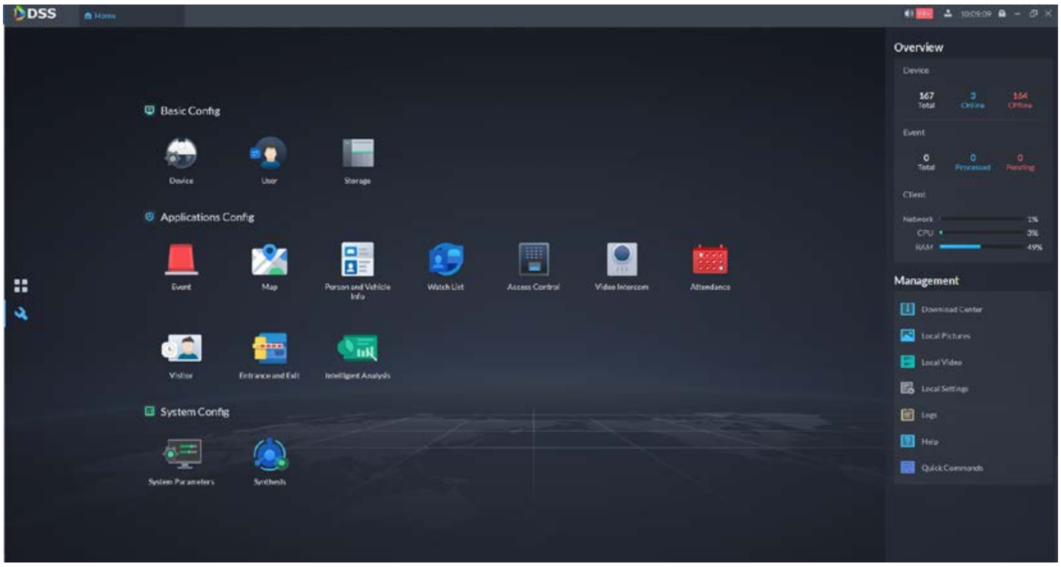
### Prerequisite

Log in to the DSS client. For details. For details, see "*DSS Professional User's Manual*".

### Procedure

Step 1 On the **Home** page, click 🔧, and select **Device**.

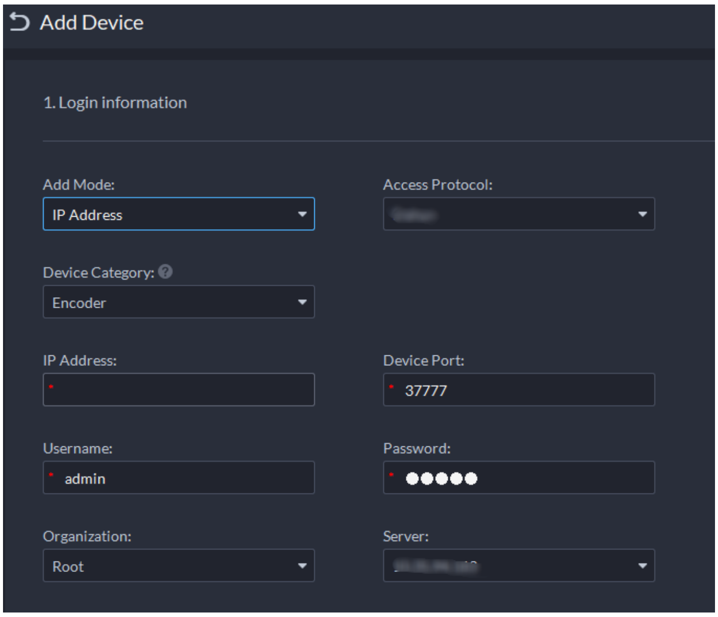
Figure 6-1 Homepage



Step 2 Select **Add Device** and click **Add**.

Step 3 Enter the login information, and then click **Add**.

Figure 6-2 Add device



Add Device

1. Login information

Add Mode: IP Address

Access Protocol: [redacted]

Device Category: Encoder

IP Address: *

Device Port: * 37777

Username: * admin

Password: * ●●●●●

Organization: Root

Server: [redacted]

Step 4 Enter the information of the Standalone and click **OK**.

## 6.2 Access Control Management

You can configure access control of the Standalone such as door status, alarm and unlock methods.

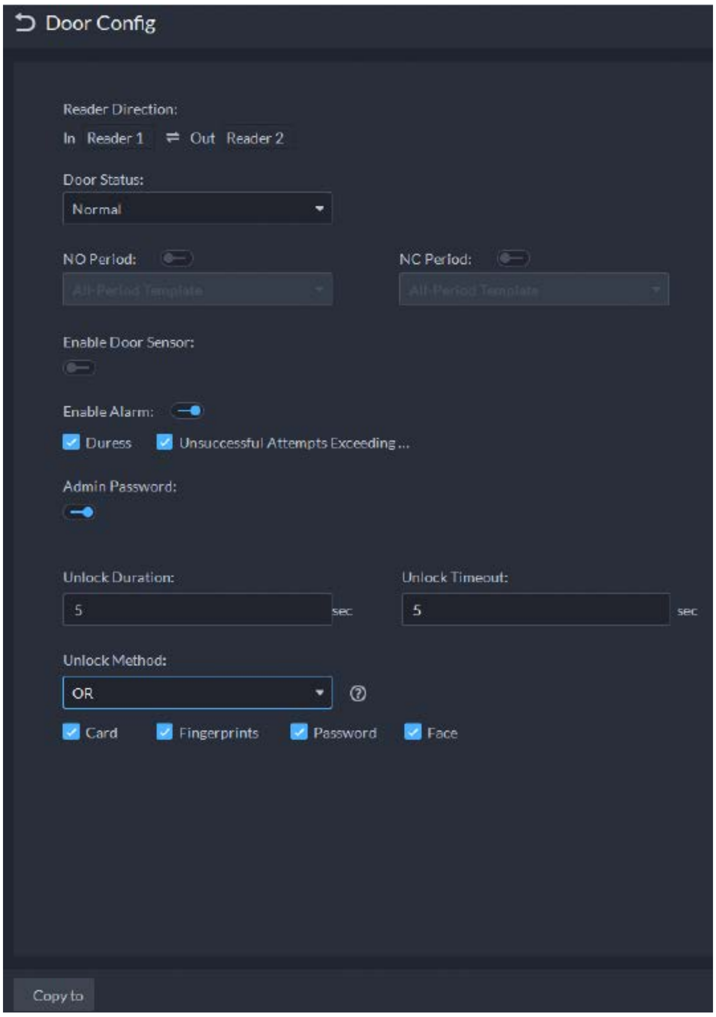
### 6.2.1 Configuring Door

Step 1 On the **Home** page, click 🔧, and select **Device**.

Step 2 Select a door channel in the device tree, and then click **Door Config**.

Step 3 Configure door information, and then click **OK**.

Figure 6-3 Door configuration



Door Config

Reader Direction:

In Reader 1 ⇄ Out Reader 2

Door Status:

Normal

NO Period: All-Period Template

NC Period: All-Period Template

Enable Door Sensor:

Enable Alarm:

☑ Duress ☑ Unsuccessful Attempts Exceeding...

Admin Password:

Unlock Duration: 5 sec

Unlock Timeout: 5 sec

Unlock Method: OR

☑ Card ☑ Fingerprints ☑ Password ☑ Face

Table 6-1 Door configuration description

| **Parameter** | **Description** |
|---|---|
| Set reader direction | Indicates the in/out reader. |
| Door Status | Set access control status to **Normal**, **Always Open**, or **Always Close**. |
| NO Period | If enabled, you can set up a period during which the door is always open. |
| NC Period | If enabled, you can set up a period during which the door is always closed. |
| Door Sensor Enable | You can only enable intrusion and timeout alarms when the door sensor is enabled. |
| Enable Alarm | ● **Duress**: A duress alarm is triggered when entry with the duress card, duress password, or duress fingerprint.<br>● **Unsuccessful Attempts Exceeding Limit**: An alarm is triggered when a person failed to unlock the door after a few attempts. |
| Admin Password | Enable this function, and then you can use the admin password to unlock the door. |
| Unlock Duration | The door remains unlocked during specified time before it locks automatically again. |
| Unlock Timeout | A timeout alarm is triggered if the door remains unlocked for longer time than the defined time. |

| Parameter | Description |
|---|---|
| Unlock Method | You can use any one of the methods, card, fingerprint, face, and password, or their combinations to unlock the door.<br>● Select **And**, and select unlock methods. You can only open the door using all the selected unlock methods.<br>● Select **Or** and select unlock methods. You can open the door in one of the ways that you configured.<br>● Select **Unlock by period** and select unlock mode for each time period. The door can only be opened by the selected method(s) within the defined period. |

## 6.2.2 Creating Door Group

Group doors for easier management of access permissions.

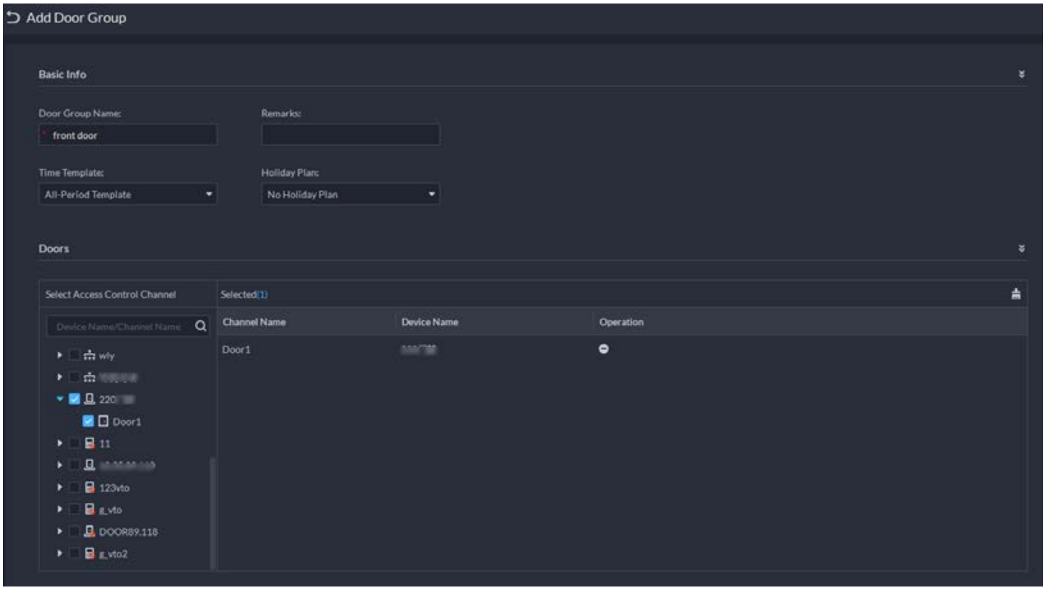
Step 1 On the **Home** page, click , and then in the **Applications Config** section, select **Access Control**.

Step 2 Click .

Step 3 Create a door group.

1) Click **Add**.
2) Enter the group name, select a time template and a holiday schedule, select a device channel, and then click **Add**.

Figure 6-4 Door group



Add Door Group

Basic Info

Door Group Name: front door

Remarks:

Time Template: All-Period Template

Holiday Plan: No Holiday Plan

Doors

Select Access Control Channel

Selected(1)

| Channel Name | Device Name | Operation |
|---|---|---|
| Door1 | [redacted] | ⊖ |

## 6.2.3 Configuring Access Permission Group

Configure access permission groups to assign access permissions by door groups.

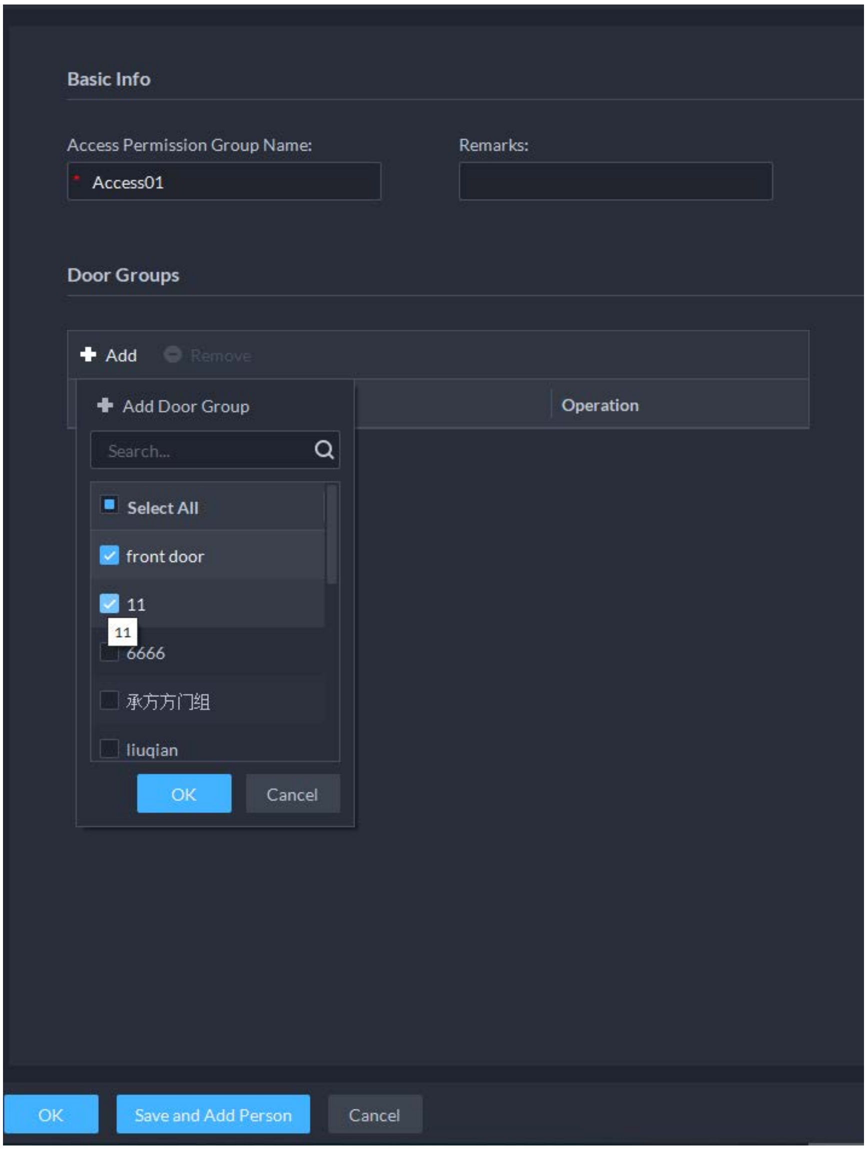
Step 1 On the **Home** page, click , and then select **Access Control**.

Step 2 Click

Step 3 Create an access permission group.

1) Click **Add** at the upper-left corner.

Figure 6-5 Add basic information



Basic Info

Access Permission Group Name: * Access01

Remarks:

Door Groups

☑ front door

☑ 11

☐ 6666

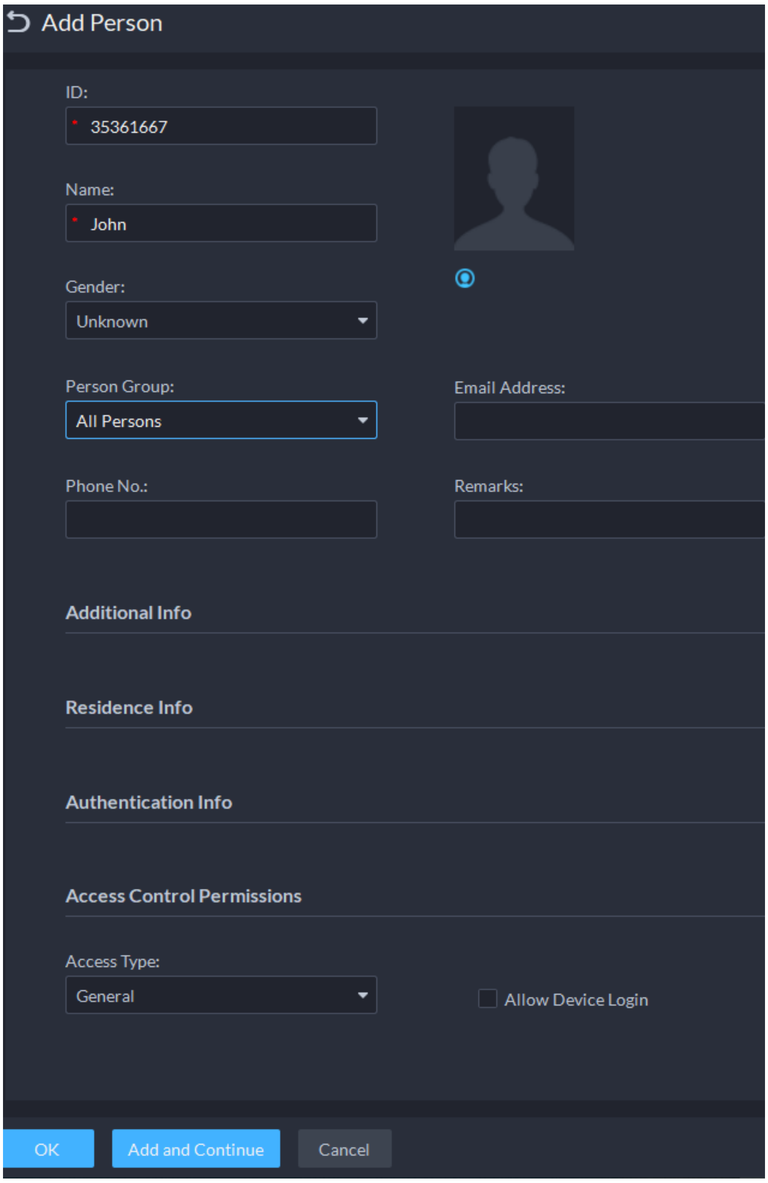
☐ 承方方门组

☐ liuqian

2) Enter the group name, and then select the door groups.

3) Click **Save** and **Add Person**.

Figure 6-6 Add person



Add Person

ID:
35361667

Name:
John

Gender:
Unknown

Person Group:
All Persons

Email Address:

Phone No.:

Remarks:

Additional Info

Residence Info

Authentication Info

Access Control Permissions

Access Type:
General

□ Allow Device Login

4) Enter the user information.

5) Click **Add and Continue**, and then click **OK**.

## 6.2.4 Configuring Advanced Function

## 6.2.5 First Card Unlock

Users can unlock the door only after the specified first-cards holders swipe their cards. You can set multiple first-card holders.

Step 1 On the **Home** page, click and then select **Access Control**.

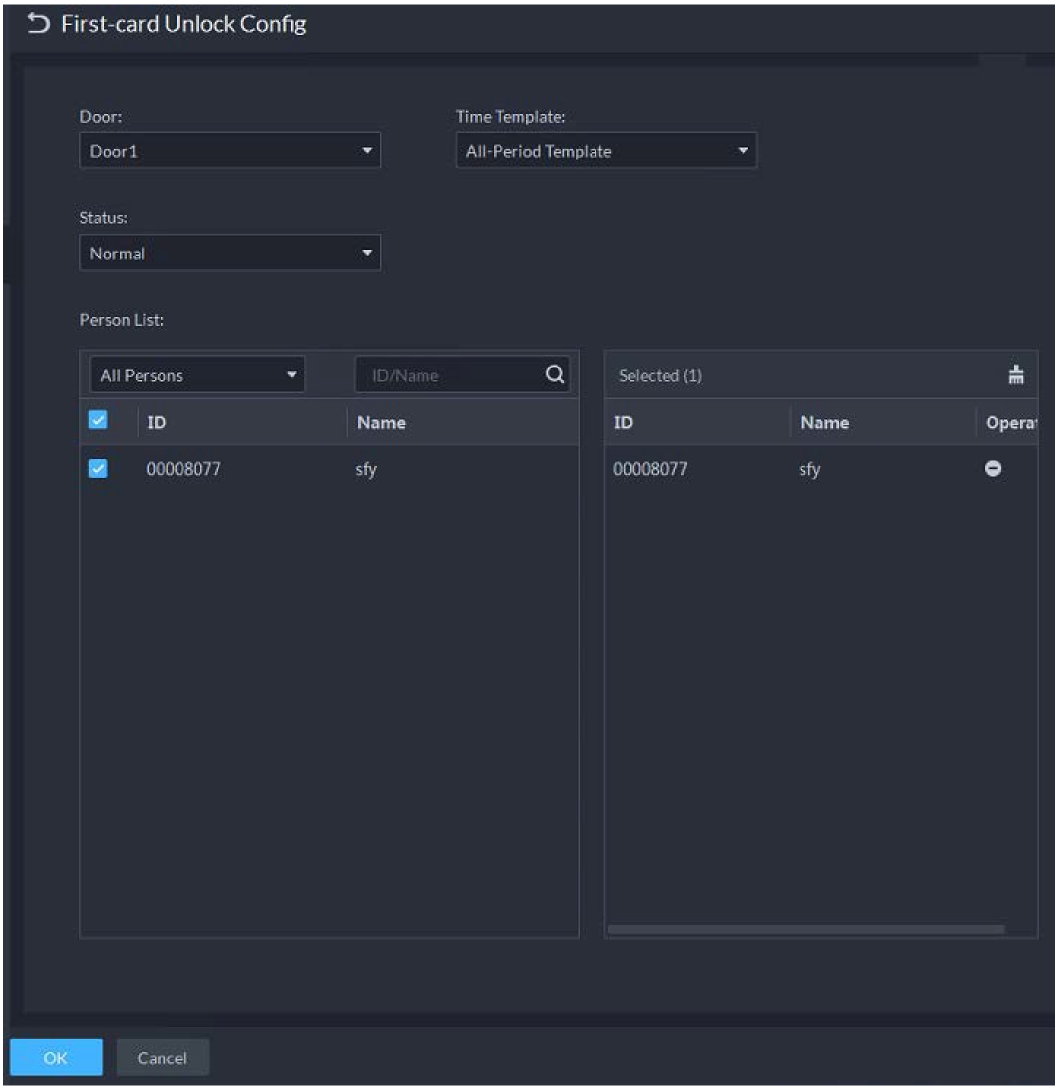
Step 2 click .

Step 3 Click the **First Card Unlock** tab.

Step 4 Click **Add**.

Step 5 Configure the parameters, and then click **OK**.

Figure 6-7 First card configuration



First-card Unlock Config

Door: Door1

Time Template: All-Period Template

Status: Normal

Person List:

All Persons

| ☑ | ID | Name |
|---|---|---|
| ☑ | 00008077 | sfy |

Selected (1)

| ID | Name | Opera |
|---|---|---|
| 00008077 | sfy | ⊖ |

Table 6-2 First card parameters

| Parameter | Description |
|---|---|
| Door | Enable the first-card function for selected doors. |
| Time Template | First-card unlock is valid during the defined periods in the selected time template. |
| Status | After first-card unlock is enabled, the door is in either the **Normal** mode or Always Open mode. |
| Person List | You can select more than one users to be first-card holders. Any one of them must swipe the card first, and then other users can unlock the door. |

### 6.2.5.2 Multi-Card Unlock

You can configure a door to be opened by a number of people in a defined order.

Step 1 On the **Home** page, click and then select **Access Control**.

Step 2 Click and then click **Multi-card Unlock**.

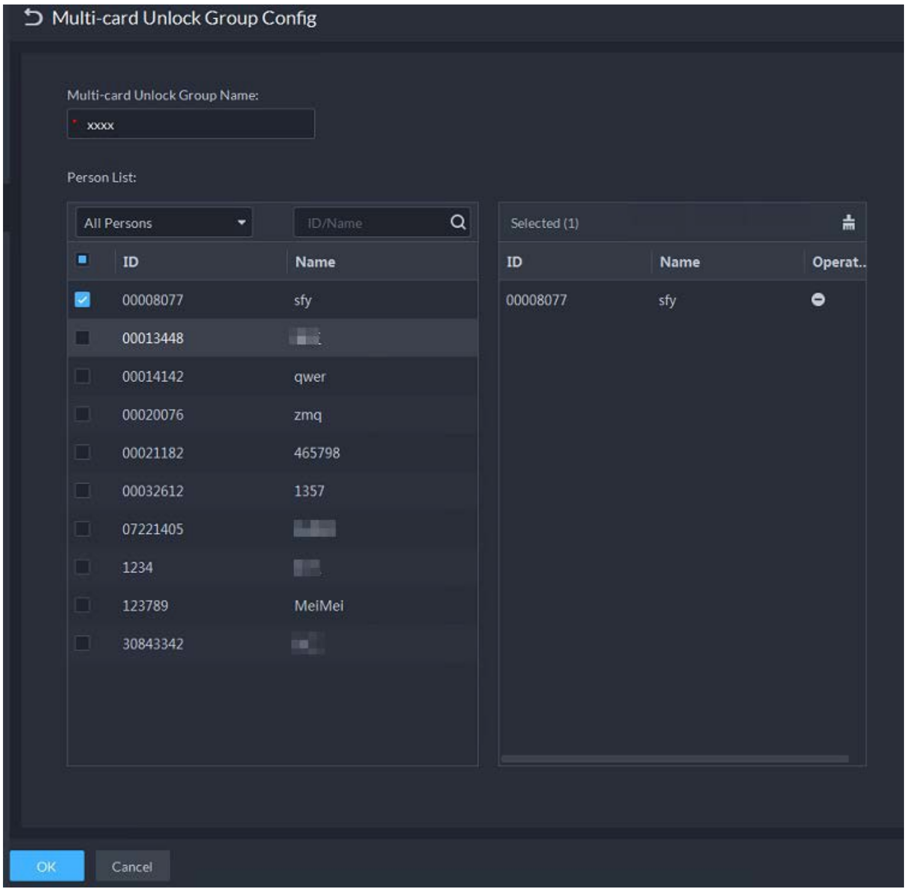
Step 3 Add a user group.

1) Click **Multi-card Unlock Group**.

2) Click **Add**.

3) Enter the group name, select users from **User List** and then click **OK**. You can select up to 50 users.

Figure 6-8 Multi-card unlock group configuration



Multi-card Unlock Group Config

Multi-card Unlock Group Name: xxxx

Person List:

All Persons | ID/Name

| ☑ | ID | Name |
|---|---|---|
| ☑ | 00008077 | sfy |
| □ | 00013448 | [redacted] |
| □ | 00014142 | qwer |
| □ | 00020076 | zmq |
| □ | 00021182 | 465798 |
| □ | 00032612 | 1357 |
| □ | 07221405 | [redacted] |
| □ | 1234 | [redacted] |
| □ | 123789 | MeiMei |
| □ | 30843342 | [redacted] |

Selected (1)

| ID | Name | Operat.. |
|---|---|---|
| 00008077 | sfy | ⊖ |

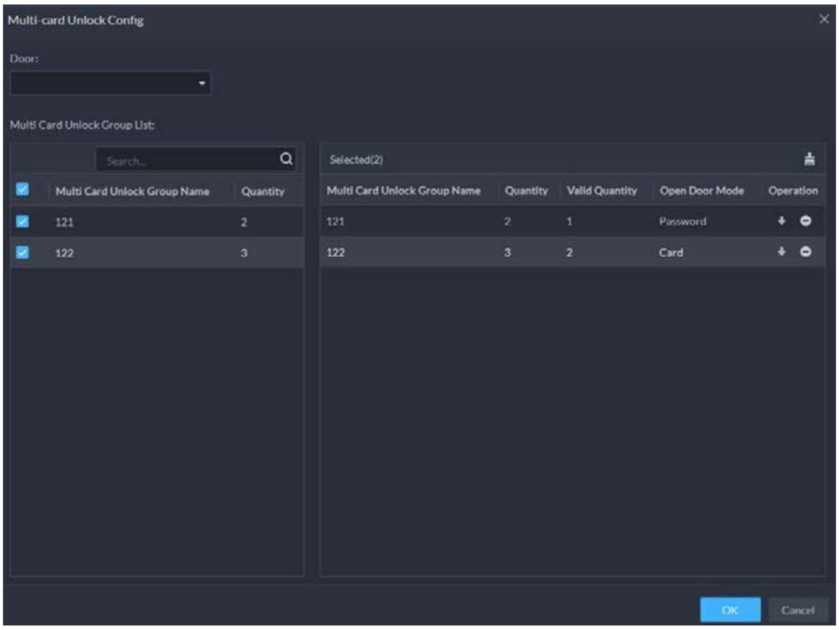
Step 4 Configure the multi-card unlock function.

1) Go back to the **Multi-card Unlock** window, and click **Add**.

2) Select the door.

3) Select the user group. You can select up to four groups.

Figure 6-9 User group information



Multi-card Unlock Config

Door:

Multi Card Unlock Group List:

Search...

| ☑ | Multi Card Unlock Group Name | Quantity |
|---|---|---|
| ☑ | 121 | 2 |
| ☑ | 122 | 3 |

Selected(2)

| Multi Card Unlock Group Name | Quantity | Valid Quantity | Open Door Mode | Operation |
|---|---|---|---|---|
| 121 | 2 | 1 | Password | ↓ ⊖ |
| 122 | 3 | 2 | Card | ↓ ⊖ |

4) Enter **Valid Quantity** and select **Open DoorMode**.

The valid quantity refers to the number of people that must be present to grant access by swiping their cards, entering their passwords, or using their fingerprints.

- Click ↑ or ↓ to adjust the card swiping sequence.
- Up to five valid users are allowed.

Step 5 Click **OK**.

means the function is enabled.

### 6.2.5.3 Anti-passback

Anti-passback can prevent users from passing their credentials such as access card back to a second person to enter a controlled area. It can also stop users from entering the controlled area by tailgating another person. Users must use access cards in a specific sequence, and access readers at both the entry and the exit are required.

For example, if you swipe an access card on the entrance access reader, then you must swipe the access card on the exit access reader before using the entrance access reader again. The "in-out" sequence should be followed.

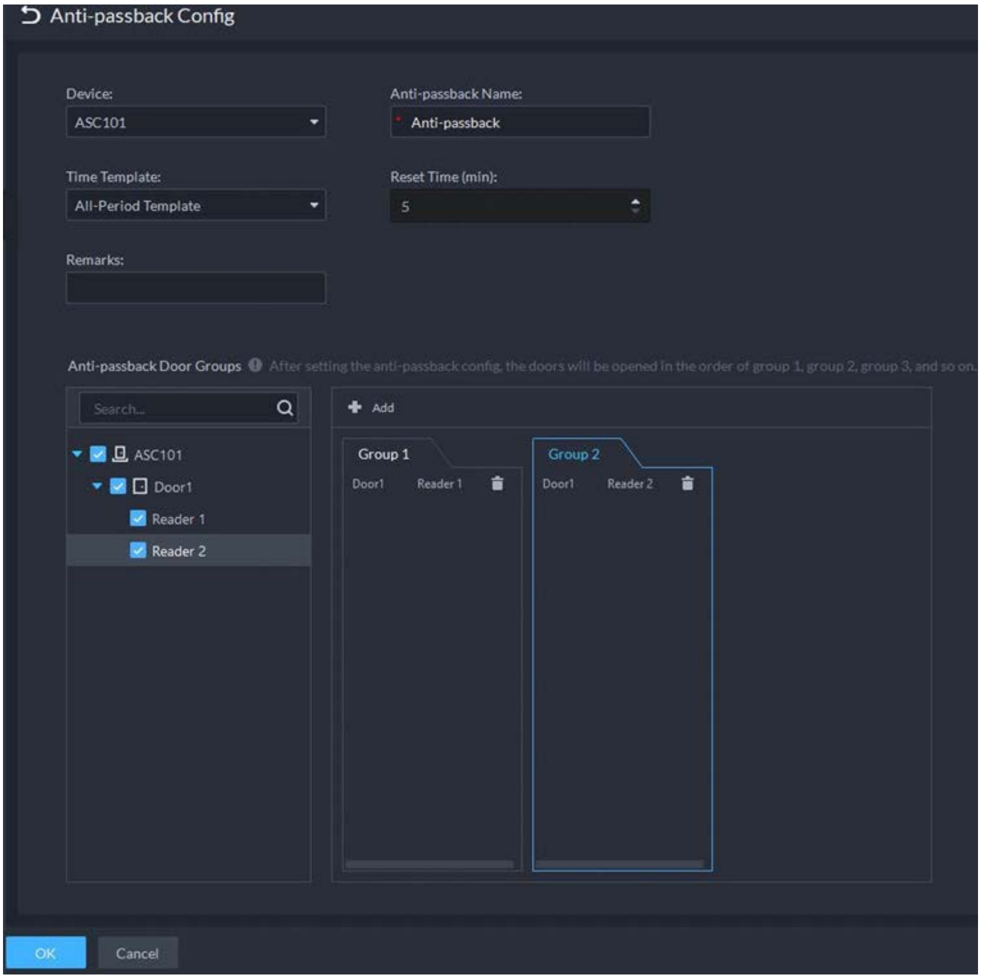
Step 1 On the **Home** page, click and then select **Access Control**.

Step 2 Click and then click **Anti-passback**.

Step 3 Click **Add**.

Step 4 Configure anti-passback parameters, and then click **OK**.

Figure 6-10 Anti-passback parameters



Anti-passback Config

Device: ASC101

Anti-passback Name: Anti-passback

Time Template: All-Period Template

Reset Time (min): 5

Remarks:

Anti-passback Door Groups After setting the anti-passback config, the doors will be opened in the order of group 1, group 2, group 3, and so on.

- ☑ ASC101
  - ☑ Door1
    - ☑ Reader 1
    - ☑ Reader 2

| Group 1 | | Group 2 | |
|---|---|---|---|
| Door1 | Reader 1 | Door1 | Reader 2 |

Table 6-3 User selection information description

| Parameter | Description |
|---|---|
| Device | Apply the anti-passback function to the selected device. |
| Anti-passback name | Enter a name for the anti-passback rule. |
| Reset Time(min) | The reset time is the duration during which the access card becomes invalid after an anti-passback rule is violated. |
| Time Template | Anti-passback rules is effective during defined periods in the selected time template. |
| Remark | Description information. |
| Group X<br>(X is a number) | You can add up to 16 readers for each group. For example, if you swipe a card on the reader 1 to enter a controlled area, then you must exit the controlled area by swiping your card on reader 2 as shown in Fig 6-10. |

### 6.2.5.4 Multi-door Interlock

You cannot open a door until the other door is locked.

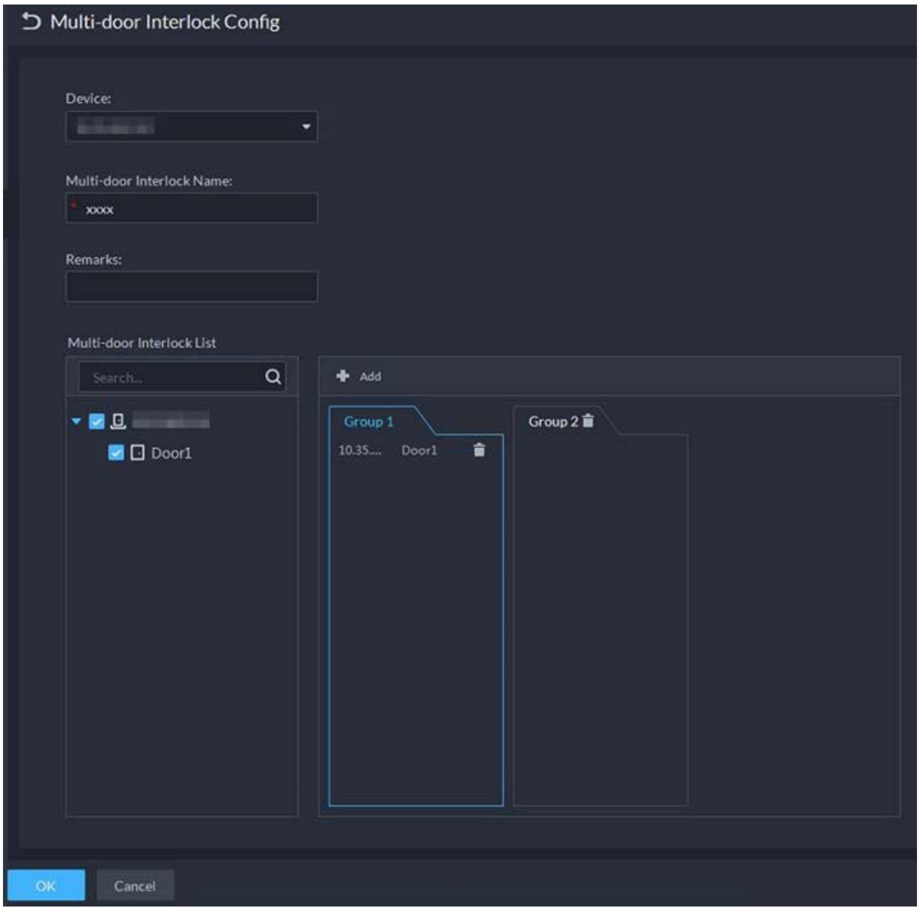
Step 1 On the **Home** page, click and then select **Access Control**.

Step 2 Click , and then click **Multi-door Interlock**.

Step 3 Click **Add**.

Step 4 Configure the parameters, and then click **OK**.

Figure 6-11 Multi-door interlock



Multi-door Interlock Config

Device:

Multi-door Interlock Name: xxxx

Remarks:

Multi-door Interlock List

| Group 1 | Group 2 |
|---|---|
| 10.35.... Door1 | |

Table 6-4 Parameters of multi-door interlock

| Parameter | Description |
|---|---|
| Device | Apply the multi-door interlock functioin for the selected device. |
| Multi-door Interlock Name | Enter a name for the inter-lock rule. |
| Remark | Description information. |
| Multi-door Interlock List | You can set up inter-lock across different door groups. If a door in Group 1 is open, doors cannot be unlocked in Group 2 until all doors in Group 1 are closed.<br>Supports up to 16 door groups, with up to 16 doors in each group. |

### 6.2.5.5 Remote Verification

When a person attempts to unlock the door with card, fingerprint, or password during a specified period, authorization from the management platform is required before the door opens.

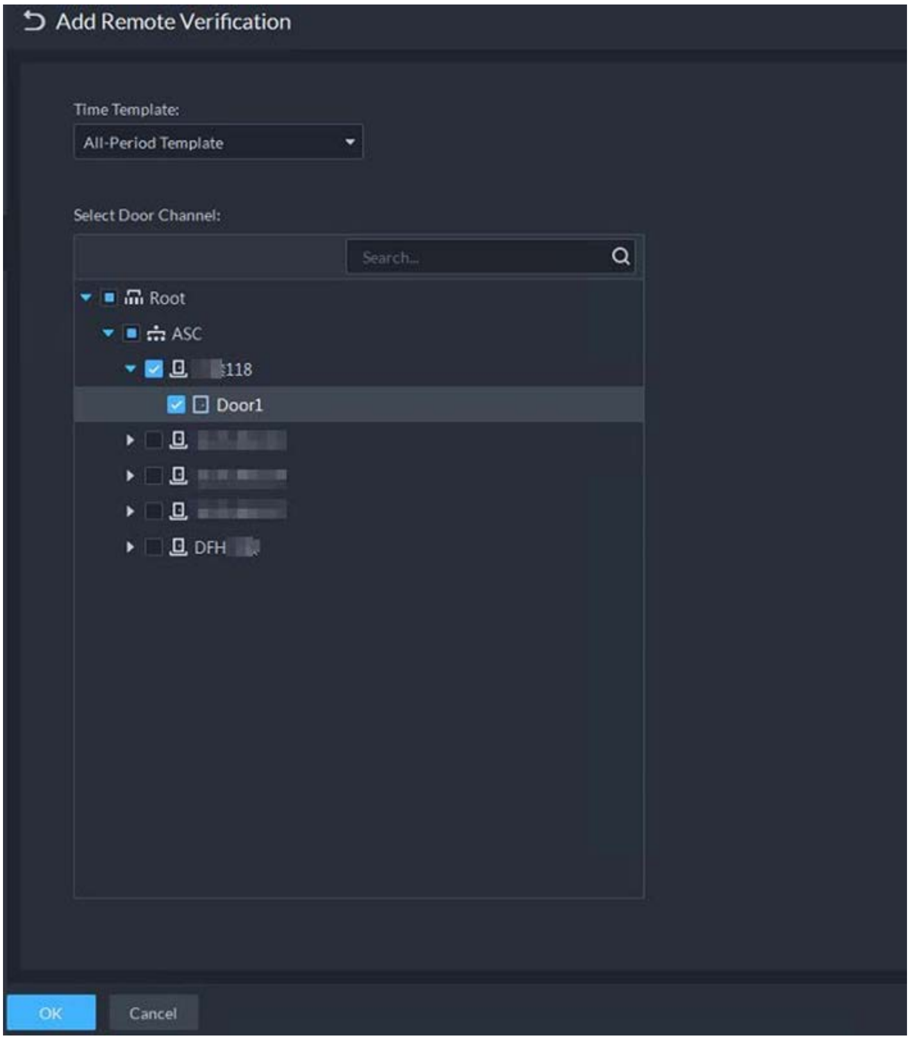
Step 1 On the **Home** page, click , and then in the **Applications Config** section, select **Access Control**.

Step 2 On the **Access Control** page, click .

Step 3 Click the **Remote Verification** tab.

Step 4 Click **Add**.

Figure 6-12 Add remote verification



Add Remote Verification

Time Template: All-Period Template

Select Door Channel:

Step 5 Select **Time Template** and access control channel, and click **OK**.

Step 6 Click ⊂⊃, and then it changes to ⊂●. The function is enabled.

## 6.2.6 Viewing Access Control Record

You can view access control records on the platform or on the device.

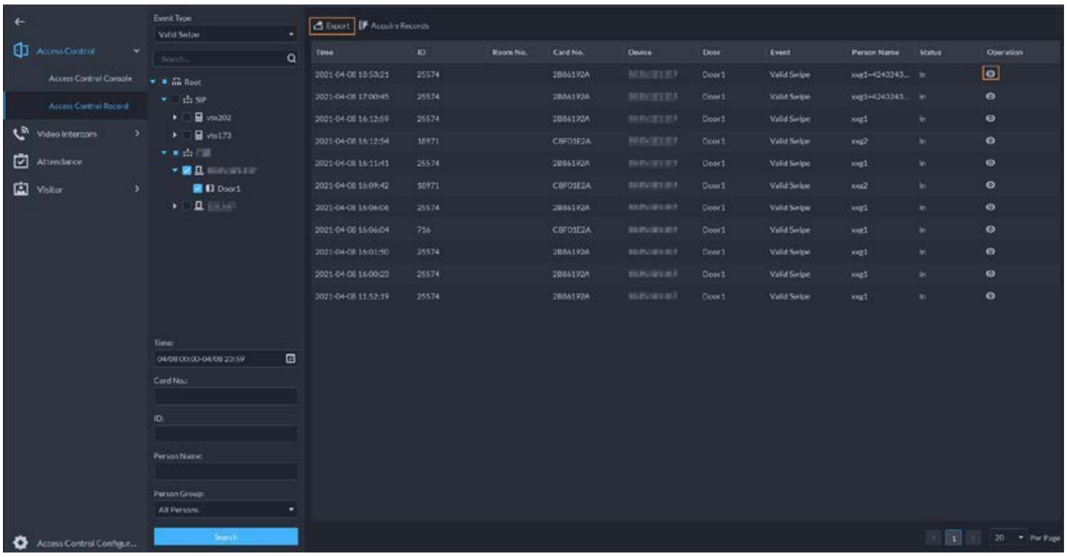
### 6.2.6.1.1 Online Record

The access control records stored on the platform.

Step 1 On the **Home** page, click ⊞ > **Access Management** > ◫ > **Access Control Record**.

Step 2 Set search conditions, and then click **Search**.

Figure 6-13 Search results



Event Type: Valid Swipe

Root
SIP
vto202
vto173
☑ Door1

Time: 04/08 00:00-04/08 23:59

Card No.:

ID:

Person Name:

Person Group: All Persons

Search

| Time | ID | Room No. | Card No. | Device | Door | Event | Person Name | Status | Operation |
|---|---|---|---|---|---|---|---|---|---|
| 2021-04-08 18:53:21 | 25574 | | 2B86192A | [redacted] | Door1 | Valid Swipe | xxg1~4243243... | In | ◉ |
| 2021-04-08 17:00:45 | 25574 | | 2B86192A | [redacted] | Door1 | Valid Swipe | xxg1~4243243... | In | ◉ |
| 2021-04-08 16:12:59 | 25574 | | 2B86192A | [redacted] | Door1 | Valid Swipe | xxg1 | In | ◉ |
| 2021-04-08 16:12:54 | 10971 | | CBF01E2A | [redacted] | Door1 | Valid Swipe | xxg2 | In | ◉ |
| 2021-04-08 16:11:41 | 25574 | | 2B86192A | [redacted] | Door1 | Valid Swipe | xxg1 | In | ◉ |
| 2021-04-08 16:09:42 | 10971 | | CBF01E2A | [redacted] | Door1 | Valid Swipe | xxg2 | In | ◉ |
| 2021-04-08 16:06:06 | 25574 | | 2B86192A | [redacted] | Door1 | Valid Swipe | xxg1 | In | ◉ |
| 2021-04-08 16:06:04 | 716 | | CBF01E2A | [redacted] | Door1 | Valid Swipe | xxg1 | In | ◉ |
| 2021-04-08 16:01:50 | 25574 | | 2B86192A | [redacted] | Door1 | Valid Swipe | xxg1 | In | ◉ |
| 2021-04-08 16:00:20 | 25574 | | 2B86192A | [redacted] | Door1 | Valid Swipe | xxg1 | In | ◉ |
| 2021-04-08 11:52:19 | 25574 | | 2B86192A | [redacted] | Door1 | Valid Swipe | xxg1 | In | ◉ |

Step 3 Manage event records.

- Click ◉ to view live view, snapshot and unlock records, and more.
- Click **Export** to export records.

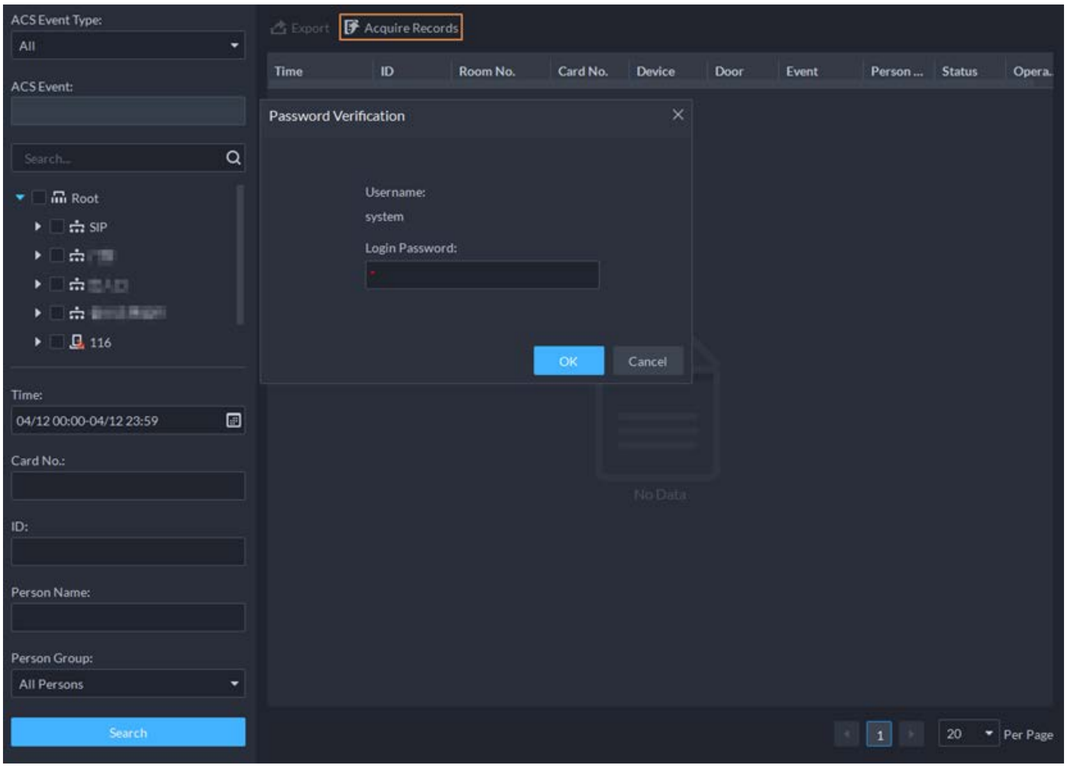
### 6.2.6.1.2 Offline Record

The access control records are stored in the Standalone when it is disconnected from the platform. After the Standalone reconnects to the platform, you can retrieve the records generated during the disconnection.

Step 1 On the **Home** page, click ⊞ > **Access Management** > ◫ > **Access Control Record**.

Step 2 Click **Acquire Records**.

Figure 6-14 Extract records during disconnection



Username: system

Login Password:

Time: 04/12 00:00-04/12 23:59

Step 3 Enter the login password for verification.

Step 4 Click ▦ to set period, select **Card-swiping Records** or **Alarm Log**, and then select device..

Step 5 Click **OK**.

# 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.