Поставщик систем безопасности TELECAMERA.RU

Access Standalone

User’s Manual

V1.0.1

Foreword

General

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

Safety Instructions

The following categorized signal words with defined meaning 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
V1.0.0	First release.	March 2020
V1.0.1	Add recommended installation height.	June 2020

About the Manual

- The manual is for reference only. If there is inconsistency between the manual and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the manual.
- The manual would be updated according to the latest laws and regulations of related regions. For detailed information, see the paper manual, CD-ROM, QR code or our official website. If there is inconsistency between paper manual and the electronic version, the electronic version shall prevail.
- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the manual. Please contact the customer service for the latest program and supplementary documentation.
- There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, please refer to our 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 the company names in the manual are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurred when using the device.
- If there is any uncertainty or controversy, please refer to our final explanation.

Important Safeguards and Warnings

This Chapter describes the contents covering proper handling of the standalone, hazard prevention, and prevention of property damage. Read these contents carefully before using the standalone, comply with them when using, and keep it well for future reference.

Operation Requirement

- Do not place or install the standalone in a place exposed to sunlight or near the heat source.
- Keep the standalone away from dampness, dust or soot.
- Keep the standalone installed horizontally on the stable place to prevent it from falling.
- Do not drop or splash liquid onto the standalone, and make sure there is no object filled with liquid on the standalone to prevent liquid from flowing into the standalone.
- Install the standalone in a well-ventilated place, and do not block the ventilation of the standalone.
- Operate the standalone within the rated range of power input and output.
- Do not dissemble the standalone.
- Transport, use and store the standalone under the allowed humidity and temperature conditions.

Electrical Safety

- Improper battery use might result in fire, explosion, or inflammation.
- When replacing battery, make sure the same model is used.
- Use the recommended power cables in the region and conform to the rated power specification.
- Use the power adapter provided with the standalone; otherwise, it might result in people injury and device damage.
- The power source shall conform to the requirement of the Safety Extra Low Voltage (SELV) standard, and supply power with rated voltage which conforms to Limited power Source requirement according to IEC60950-1. Please note that the power supply requirement is subject to the device label.
- Connect the device (I-type structure) to the power socket with protective earthing.
- The appliance coupler is a disconnection device. When using the coupler, keep the angle for easy operation.

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 Connections 3
2.2 Device Installation 3
3 System Operation **6**
3.1 Button Description 6
3.2 Initialization 6
3.3 Standby Interface 7
3.4 Unlocking Methods 8
3.4.1 User Passwords 8
3.4.2 Administrator Password 9
3.5 Main Menu 9
3.6 User Management 10
3.6.1 Adding New Users 10
3.6.2 Viewing User information 12
3.7 Access Management 12
3.7.1 Unlock Mode 12
3.7.2 Door Status 13
3.7.3 Lock Holding Time 14
3.7.4 Door Sensor Type 14
3.7.5 Remote Verification 14
3.8 Network Communication 14
3.8.1 IP Address 14
3.8.2 Wiegand Configuration 16
3.8.3 TCP Port 17
3.8.4 Serial Port Settings 17
3.9 System 18
3.9.1 Time 18
3.9.2 Volume Adjustment 18
3.9.3 ScreenSaver 18
3.9.4 Privacy Setting 19
3.9.5 Card No. Reverse 19
3.9.6 Auto Test 20
3.9.7 Restore to Factory Settings 20
3.9.8 Reboot 20
3.10 USB 21
3.10.1 USB Export 21
3.10.2 USB Import 22
3.10.3 USB Update 22

3.10.4 Screensaver 22
3.10.5 Exporting Record 23
3.11 System Information 23
4 Web Operation 24
4.1 Initialization 24
4.2 Login 26
4.3 Resetting the Password 26
4.4 Door Parameter 28
4.5 Alarm Linkage 29
4.5.1 Setting Alarm Linkage 29
4.5.2 Alarm Log 31
4.6 Time Section Configuration 31
4.6.1 Time Section 32
4.6.2 Holiday Group Configuration 33
4.6.3 Holiday Plan Configuration 34
4.7 Data Capacity 35
4.8 Volume Setting 35
4.9 Network Setting 36
4.9.1 TCP/IP 36
4.9.2 Port 37
4.9.3 P2P 38
4.10 Data Setting 39
4.11 Safety Management 39
4.11.1 IP Authority 39
4.11.2 System 40
4.11.3 User Management 40
4.11.4 Maintenance 41
4.11.5 Configuration Management 42
4.11.6 Upgrade 42
4.11.7 Version Information 43
4.11.8 Online User 43
4.12 System Log 43
4.12.1 Query Logs 44
4.12.2 Backup Logs 44
4.13 Admin Log 44
4.14 Exit 45
5 Mobile phone Operation 46
6 Configuration on DSS Pro 48
6.1 Adding Devices 48
6.2 Access Control Management 51
6.2.1 Door Configuration 51
6.2.2 Creating Door Groups 54
6.2.3 Issuing Access Cards 55
6.2.4 First Card Unlock 59
6.2.5 Multi-Card Unlock 62
6.2.6 Anti-passback 67
6.2.7 Remote Verification 69

6.2.8 Viewing Access Control Records..... 71
6.2.9 Viewing Device Logs 73
Appendix 1 Cybersecurity Recommendations 75

1 Overview

1.1 Introduction

The access standalone is an access control panel that supports unlock through fingerprint, passwords, and card, and supports their combinations.

1.2 Features

- Support card unlock, fingerprint unlock and password unlock (unlock button and remote unlock).
- Support 30,000 users, 30,000 cards, and 3000 fingerprints.
- Store 150,000 access records and 1000 alarm records.
- Support duress alarm, tamper alarm, and report the alarm; support 1 alarm input and 1 alarm output.
- Support general users, restricted users, guest users, patrol users, VIP users, and other users.
- Voice prompt function.
- The timer can work normally for one year after power off.
- NTP auto test function.

1.3 Dimensions and Components

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

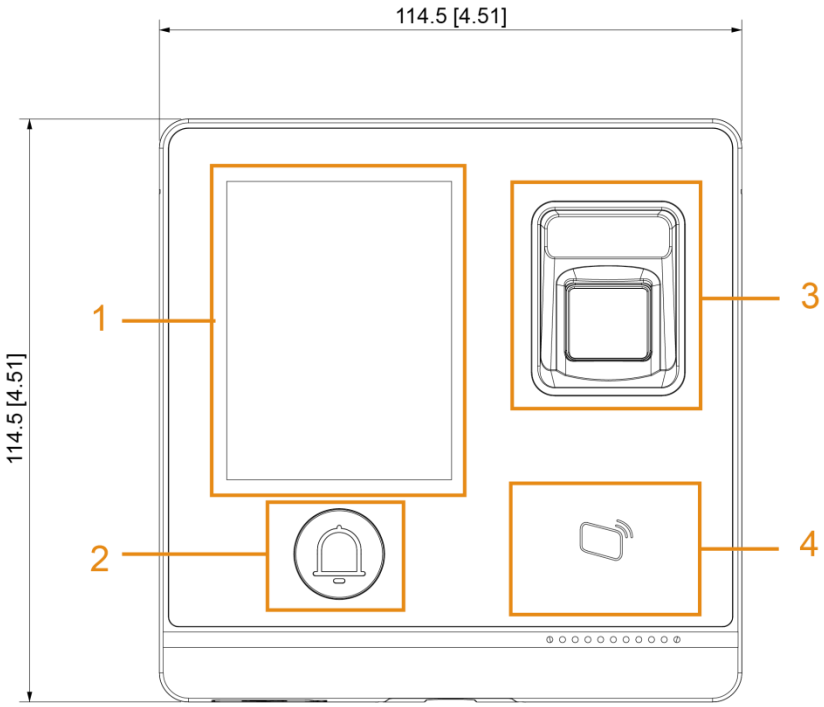


Figure 1-2 Back view (mm [inch])

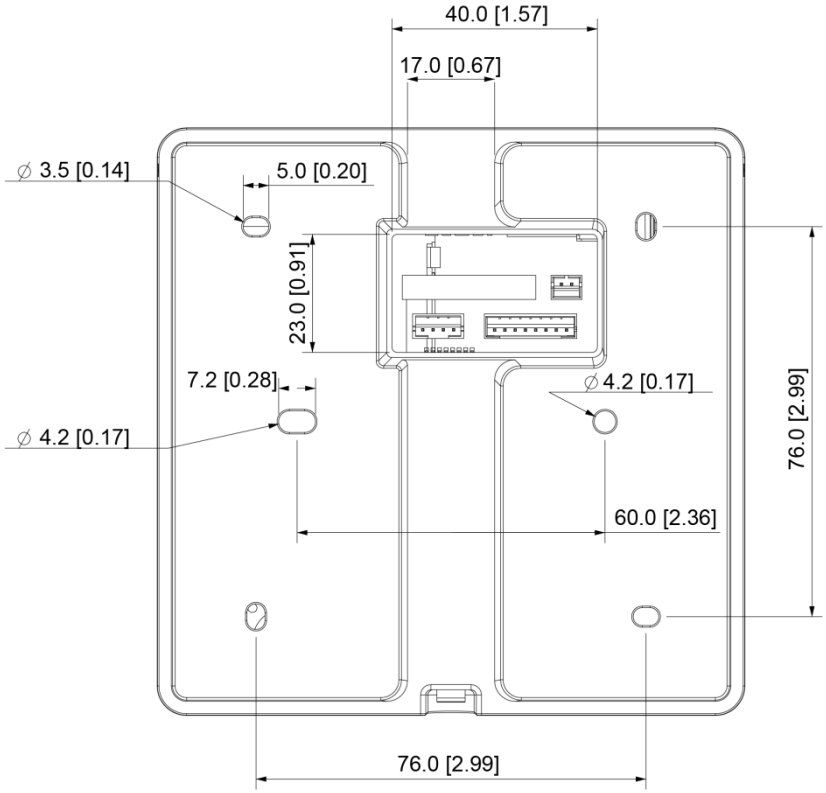


Figure 1-3 Side and bottom view (mm [inch])

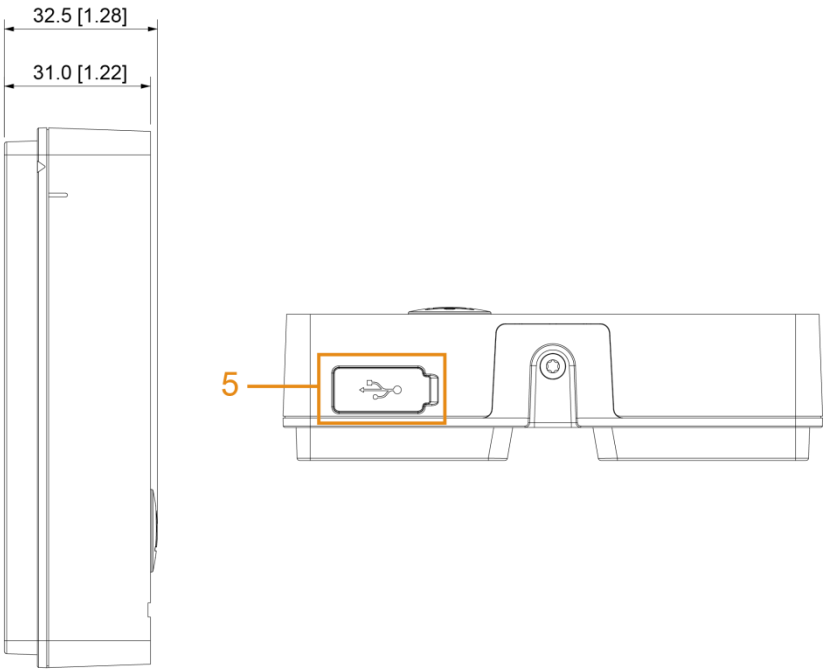


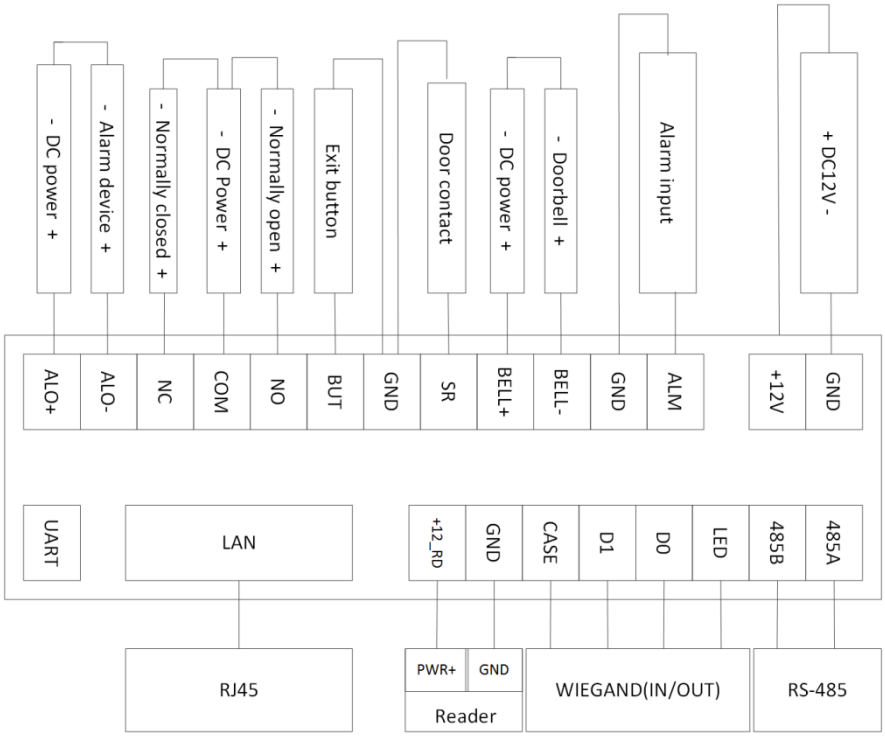
Table 1-1 Component description

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

2 Installation

2.1 Cable Connections

Figure 2-1 Cable connection



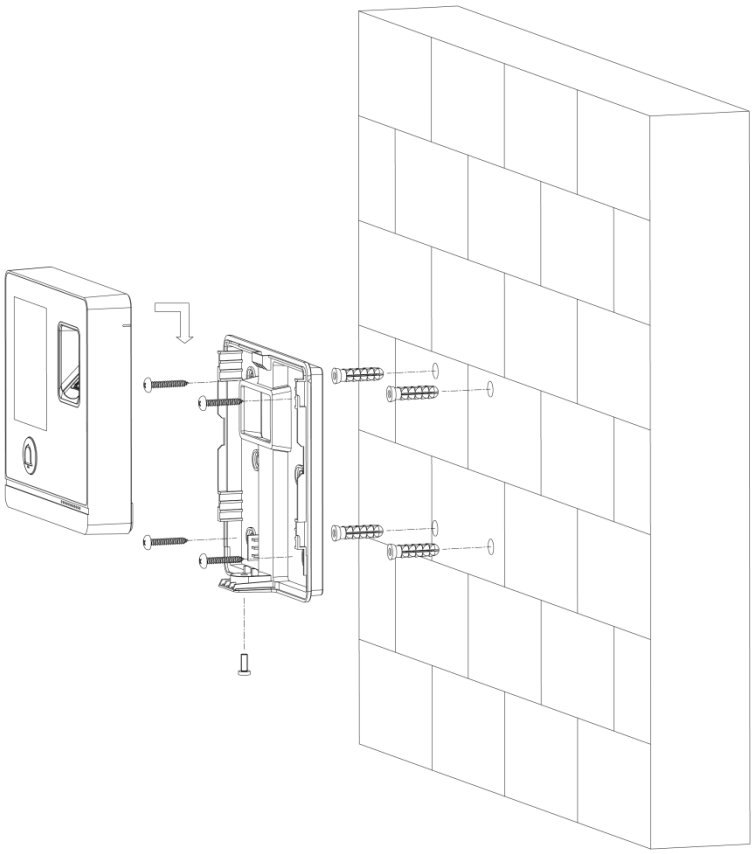
2.2 Device Installation

The recommended installation height is 1.4–1.6 meters.

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.

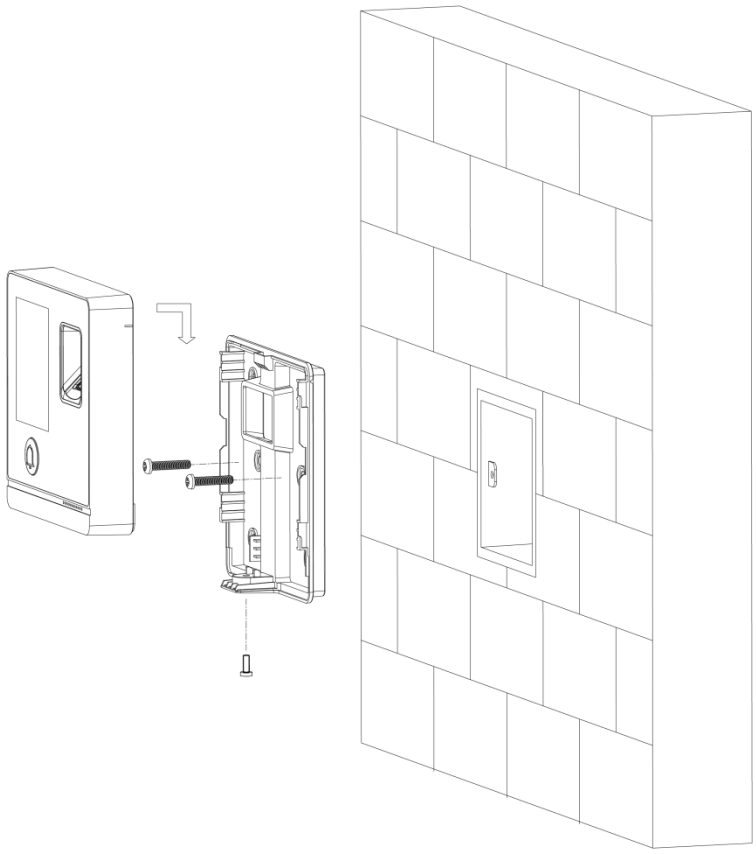
Step 2 Insert expansion bolt into installation holes.

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 System Operation

3.1 Button Description

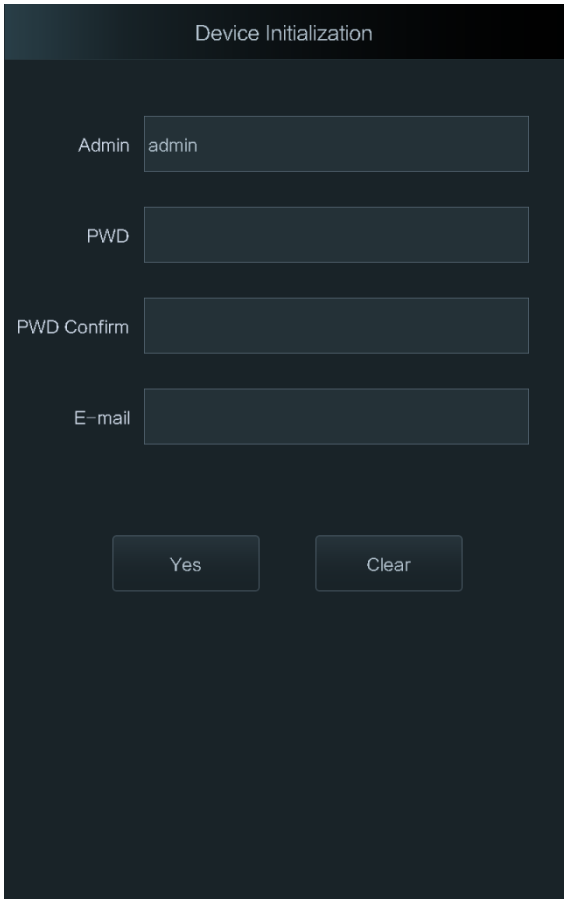
Table 3-1 Button description

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

Administrator password and an email should be set the first time the standalone is turned on; otherwise the standalone cannot be used.

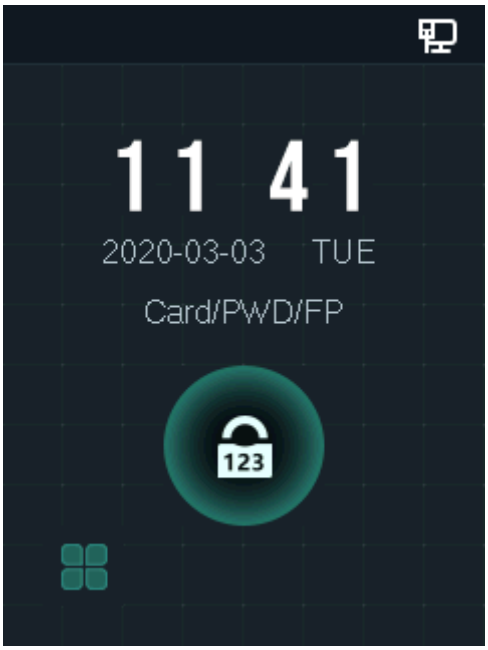
Figure 3-1 Initialization



- Administrator and password set on this interface are used to log in to the web management platform.
- The administrator password can be reset through the email address you entered if the administrator forgets 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 interface is displayed.

Figure 3-2 Standby interface



3.3 Standby Interface

You can unlock the door through fingerprint, passwords, and card. For details, see Table 3-2.

- If there are no operations in 30 seconds, the standalone will go to screensaver mode when the screensaver is enabled and pictures have been imported for screensaver play; After 30 seconds screensaver play, the standalone go to the standby mode.
- The following figures are for reference only, and the actual interface shall prevail.

Figure 3-3 Standby interface

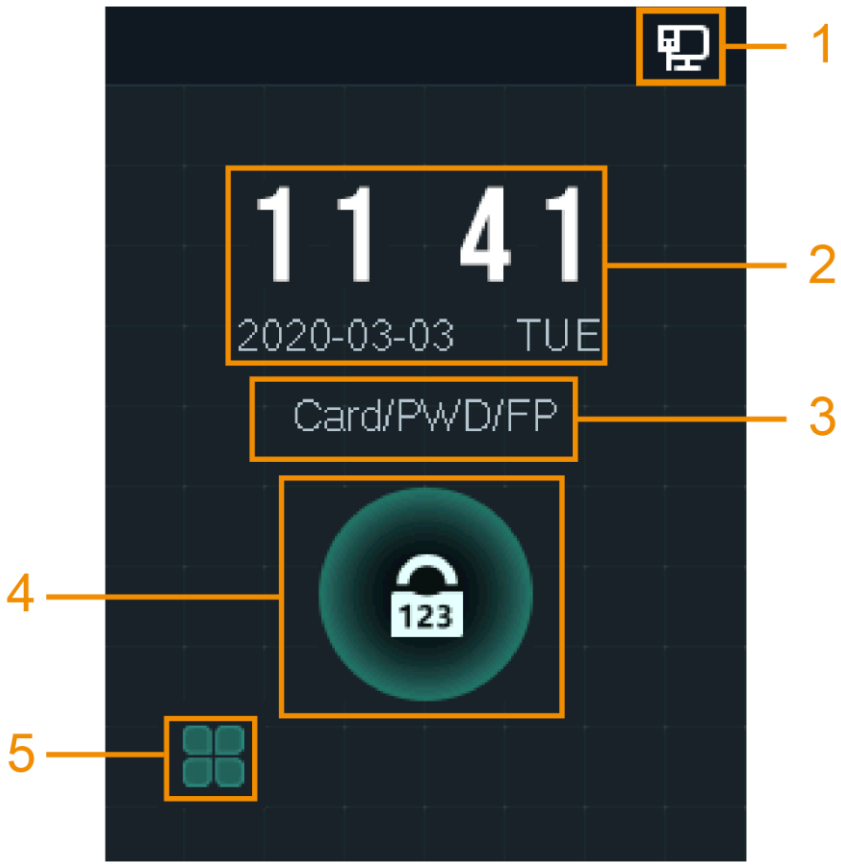


Table 3-2 Homepage description

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. Only the administrator can enter the main menu.

3.4 Unlocking Methods

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

3.4.1 User Passwords

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

Step 1 Tap on the standby interface.

Step 2 Tap

, 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 one standalone.
- DSS Pro can issue 100 passwords for one standalone at most.
- Administrator is not the password that was set during initialization.

Step 1 Tap

on the homepage.

Step 2 Tap

.

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

The door is unlocked.

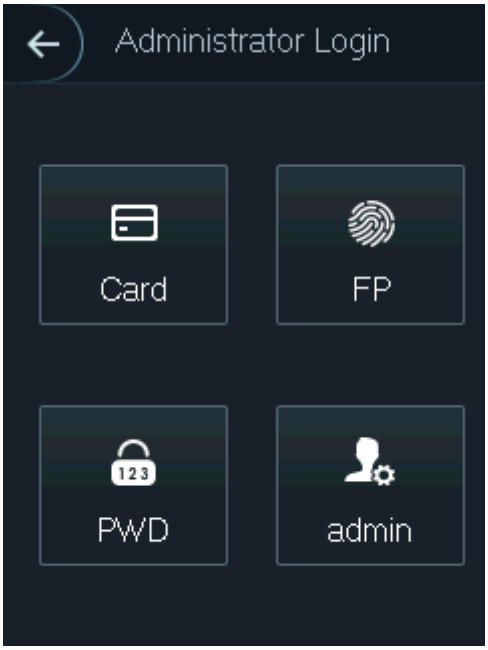
You can set and enable Administrator PWD on the **Administrator PWD** interface.

3.5 Main Menu

Administrators can add users of different levels, set access-related parameters, do network configuration, view access records and system information, and more in the main menu.

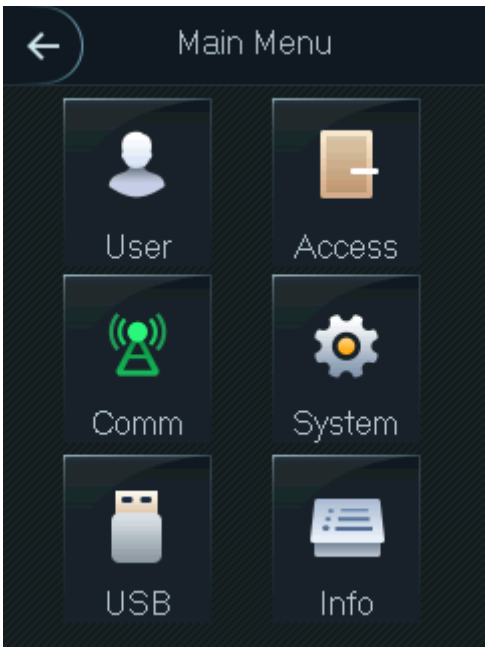
Step 1 Tap on the standby interface.

Figure 3-4 Administrator login



Step 2 Select a main menu entering method.

Figure 3-5 Main menu



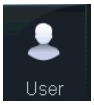
3.6 User Management

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

3.6.1 Adding New Users

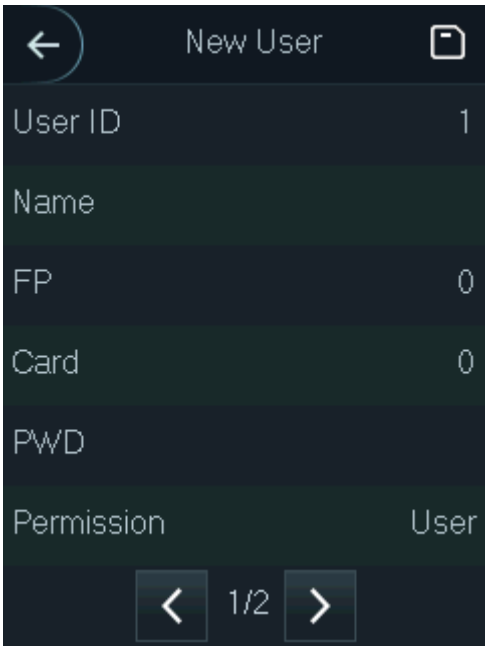
You can add new users by entering user IDs, names, importing fingerprints, cards, passwords, selecting user levels, and more.

The following figures are for reference only, and the actual interface shall prevail.

Step 1 Tap 

, and then tap .

Figure 3-6 New user info



Step 2 Configure parameters on the interface.

Table 3-3 New user parameter description

Parameter	Description
User ID	You can enter user IDs. The IDs consist of 18 characters (including numbers and letters, but not special characters), and each ID is unique. The ID will be allocated when you do not enter one.
Name	You can enter names with at most 32 characters (including numbers, symbols, and letters).
FP	Fingerprint registration. Record the user's fingerprints.
Card	Card registration. Record the card information.
PWD	The door unlocking password. The maximum length of the ID digits is 8.
Permission	Set the user's permission: **User** or **Admin**. ● User: **User** only has the permission to unlock the door. ● Admin: **Admin** has the permission to unlock the door and configure the parameters.
Period	You can set a period in which the user can unlock the door.
Holiday Plan	You can set a holiday plan in which the user can unlock the door.
Valid Date	You can set a period during which the unlocking information of the user is valid.

Parameter	Description
User Type	● General: General users can unlock the door normally. ● Restricted: When users in the blacklist unlock the door, service personnel will get a prompt. ● Guest: Guests are allowed to unlock the door certain times in certain periods. Once they exceed the maximum times and periods, they cannot unlock the door again. ● Patrol: Patrolling users can get their attendance tracked, but they have no unlock authority. ● VIP: When VIP unlocks the door, service personnel will get a prompt. ● Other: When special users (such as disabled people and pregnant people) unlock the door, there will be a delay of 5 seconds before the door is closed.
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 After you have configured all the parameters, tap to save the configuration.

3.6.2 Viewing User information

You can search user, view user list, admin list, enable administrator password and edit and delete user information through the **User** interface.

3.7 Access Management

You can do access management on unlock mode, door status, lock holding time, door sensor type, and remote verification.

Tap

to go to the access management interface.

3.7.1 Unlock Mode

When the **Unlock Mode** is on, users can unlock card, password, fingerprint, and the combination mode.

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

Figure 3-7 Element (multiple choice)

Step 2 Select unlock mode(s).

Tap a selected unlock mode again, the unlock mode will be deleted.

Step 3 Select a combination mode.

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

Step 4 Tap to save the settings.

And then the **Access** interface is displayed.

Step 5 Enable the **Unlock Mode**.

- means enabled.
- means not enabled.

3.7.2 Door Status

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

- NO: If **NO** is selected, the door status is normally open, which means the door will never be closed.
- NC: If **NC** is selected, the door status is normally closed, which means the door will not be unlocked.
- Normal: If **Normal** is selected, the door will be unlocked and locked depending on your settings.

3.7.3 Lock Holding Time

Lock Holding Time is the duration in which the door is unlocked. If the door has been unlocked for a period that exceeds the duration, the door will be automatically locked.

3.7.4 Door Sensor Type

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

3.7.5 Remote Verification

Tap **Remote Verification** to set the effective time, and then tap to enable it. Remote verification is required when unlock doors. To unlock the door, a door unlock instruction sent by the management platform is needed.

- means enabled.
- means not enabled.

3.8 Network Communication

To make the standalone work normally, you need to configure parameters for network, serial ports and Wiegand ports.

3.8.1 IP Address

3.8.1.1 IP Configuration

Configure an IP address for the standalone to make it be connected to the network. For details, see Table 3-4.

Figure 3-8 IP address configuration

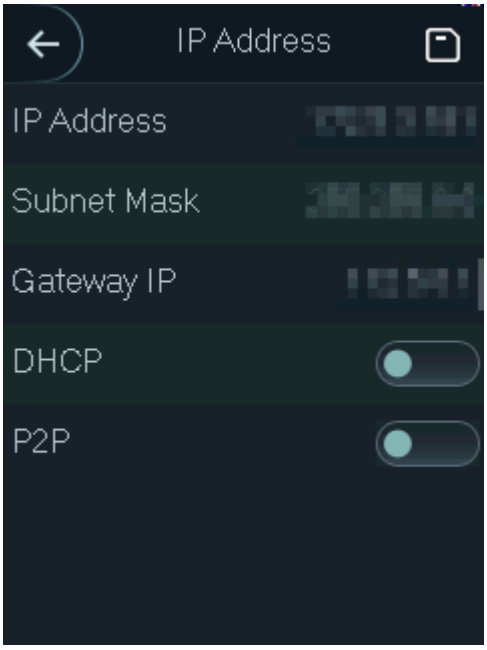


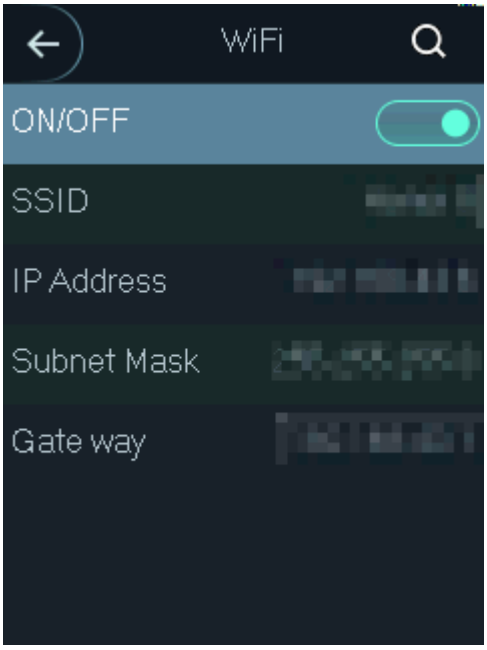
Table 3-4 IP configuration parameters

Parameter	Description
IP Address/Subnet Mask/Gateway IP Address	The IP address, subnet mask, and gateway IP address should be on the same network segment. After configuration, tap to save the configurations.
DHCP	DHCP (Dynamic Host Configuration Protocol). When the DHCP is enabled, the IP address can be automatically acquired, 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 requiring DDNS, port mapping or transit server.

3.8.1.2 Wi-Fi

You can connect the standalone to the network through Wi-Fi when the Wi-Fi function is enabled.

Figure 3-9 Wi-Fi

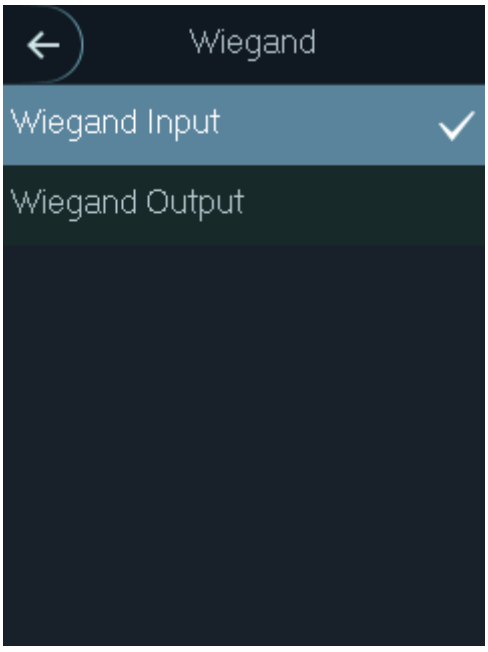


3.8.2 Wiegand Configuration

Select **Wiegand Input** or **Wiegand Output** according to the entering direction and exiting direction.

Select **Comm > Wiegand**, and then the **Wiegand** interface is displayed.

Figure 3-10 Wiegand



- Select **Wiegand Input** when an external card swipe mechanism is connected to the standalone.
- Select **Wiegand Output** when the standalone works as a reader that can be connected to the controller. See Table 3-5.

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 recognized by the standalone. ● Wiegand26, three bytes, six digits. ● Wiegand34, four bytes, eight digits. ● Wiegand66, eight bytes, sixteen digits.
Pulse Width	You can set pulse width and pulse interval.
Pulse Interval	
Output Data Type	You can select the types of output data. ● User ID: If User ID is selected, and then user ID will be output. ● Card No.: If Card No. is selected, and then card number will be output.

3.8.3 TCP Port

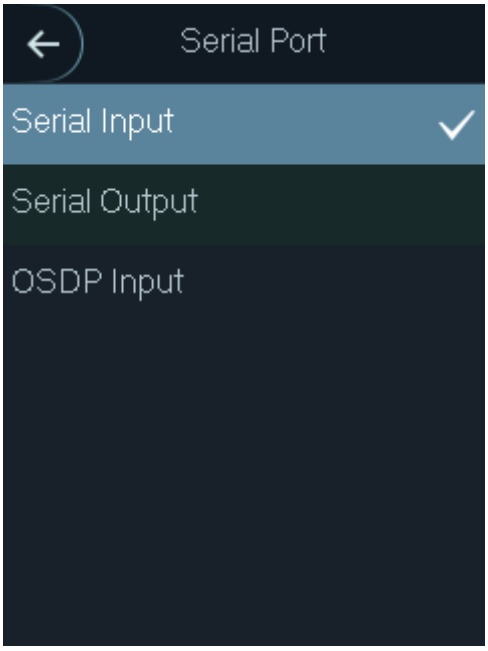
The range is 1025-65535, and it is 37777 by default. If you modify the port, the system will restart automatically.

3.8.4 Serial Port Settings

Select serial input or serial output according to the entering direction and exiting direction.

Select **Comm > Serial Port**.

Figure 3-11 Serial port



- Select **Serial Input** when external devices that are with card reading and writing functions are connected to the standalone. **Serial Input** is selected to enable access card information to be sent to the standalone and the management platform.
- For standalones with fingerprint recognition, card reading and writing functions, if you select **Serial Output**, standalone will send card number or user ID to the controller.

- Select **OSDP Input** when card reader of OSDP protocol is connected to the standalone.

3.9 System

3.9.1 Time

You can enable **24-hour System**, and do date format setting, date setting, time setting, and time zone settings.

3.9.2 Volume Adjustment

Tap or to adjust the volume.

3.9.3 ScreenSaver

Enable **ScreenSaver**, the screen saver will be displayed if there is no operation in 30 seconds.

- 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 Privacy Setting

Figure 3-12 Privacy setting

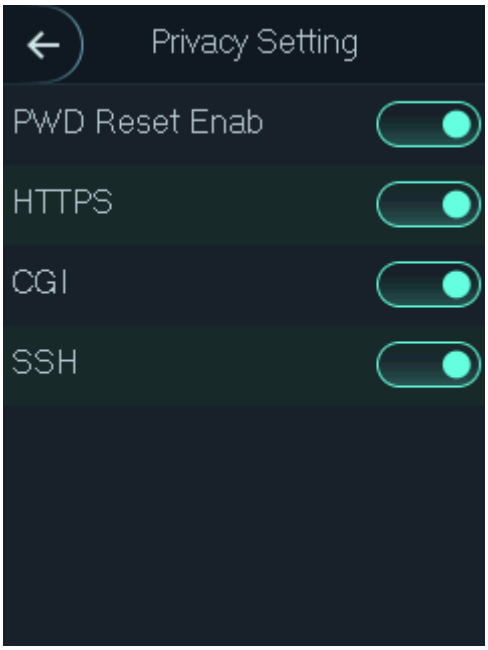


Table 3-6 Features

Parameter	Description
PWD Reset Enable	If the **PWD Reset Enable** function is enabled, you can reset the password. The PWD Reset function is enabled by default.
HTTPS	Hypertext Transfer Protocol Secure (HTTPS) is a protocol for secure communication over a computer network. 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. 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. When SSH is enabled, SSH provides cryptographic service for the data transmission.

When HTTPS is enabled, the standalone will restart automatically.

3.9.5 Card No. Reverse

If the third party card reader needs to be connected to the terminal through the Wiegand output port, you need to enable the Card No. Reverse function; otherwise the communication between the terminal and the third party card reader might fail due to protocol discrepancy.

3.9.6 Auto Test

When you use the standalone for the first time or when the standalone malfunctioned, you can use auto test function to check whether the standalone can work normally. Do actions according to the prompts.

When you select **Auto Test**, the standalone will guide you to do all the auto tests.

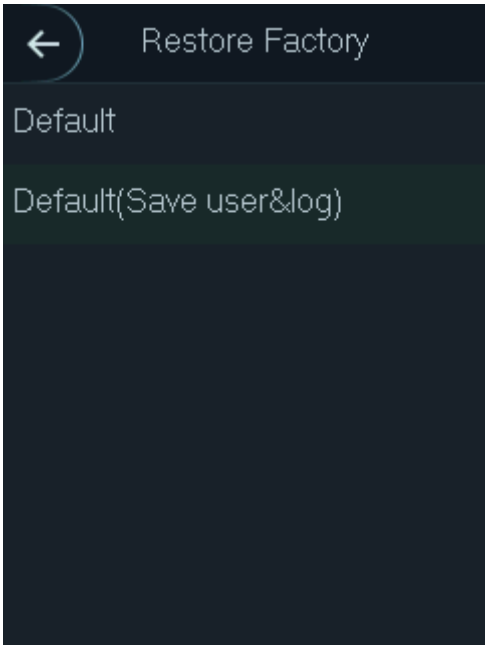
3.9.7 Restore to Factory Settings

Data will be lost if you restore the access controller to the factory settings.

You can select whether to retain user information and logs.

- Tap **Default** to restore the standalone to the factory settings with all user information and device information deleted.
- Tap **Default (Save user&log)** to restore the standalone to the factory settings with user information and device information retained.

Figure 3-13 Restore factory



3.9.8 Reboot

Select **System > Reboot**, tap **Yes**, and the standalone will be rebooted.

3.10 USB

- Make sure that the USB is inserted before exporting user information and updating. During exporting or updating, do not pull out the USB or do other operations; otherwise the exporting or updating will fail.
- You need to import information from one standalone to the USB before using USB to import information to another standalone.
- USB can also be used to update the program.

3.10.1 USB Export

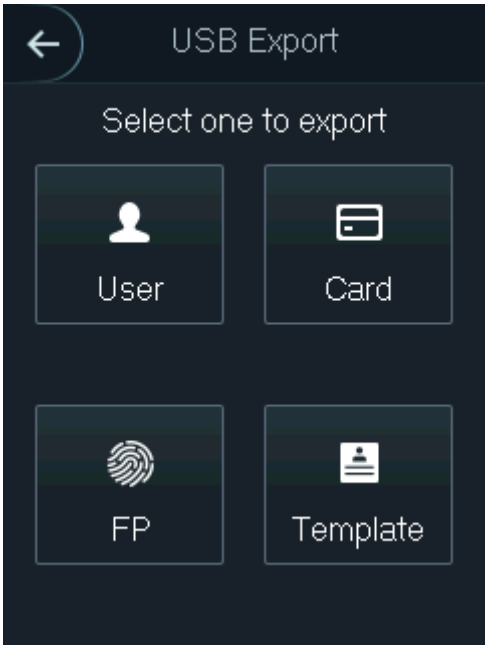
You can export data from the standalone to the USB after inserting the USB. The exported template is in .xml format, and you can edit user information and import it to the standalone. The first three pieces of information are encrypted and cannot be edited.

Only the FAT32 file system is supported.

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

The **USB Export** interface is displayed.

Figure 3-14 USB export



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

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

Step 3 Tap **OK**.

Data exported will be saved in the USB.

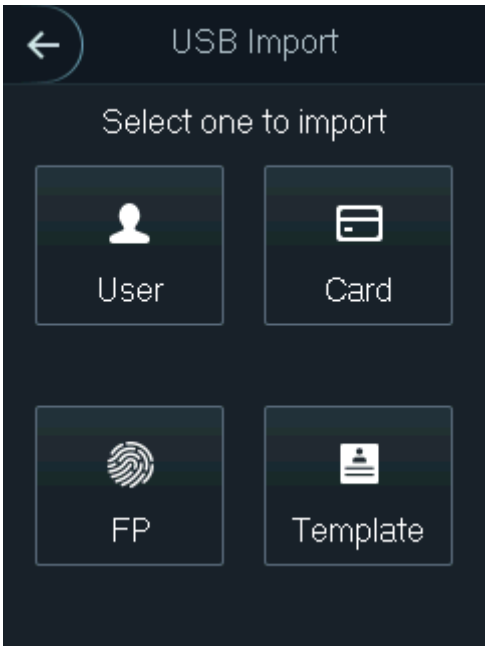
3.10.2 USB Import

Edit the user information in the exported template, and then import it to the standalone.

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

The **USB Import** interface is displayed.

Figure 3-15 USB import



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

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

Step 3 Tap **OK**.

Data in the USB will be imported into the standalone.

3.10.3 USB Update

USB can be used to update the system.

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 update starts, and the standalone reboots after the update is finished.

3.10.4 Screensaver

Insert a USB with pictures, and tap **ScreenSaver** to import pictures from the USB as the screen saver.

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

3.10.5 Exporting Record

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 of the standalone on the **System Info** interface.

4 Web Operation

The standalone can be configured and operated on the web. Through the web you can set network parameters, video parameters, and standalone parameters; and you can also maintain and update the system.

4.1 Initialization

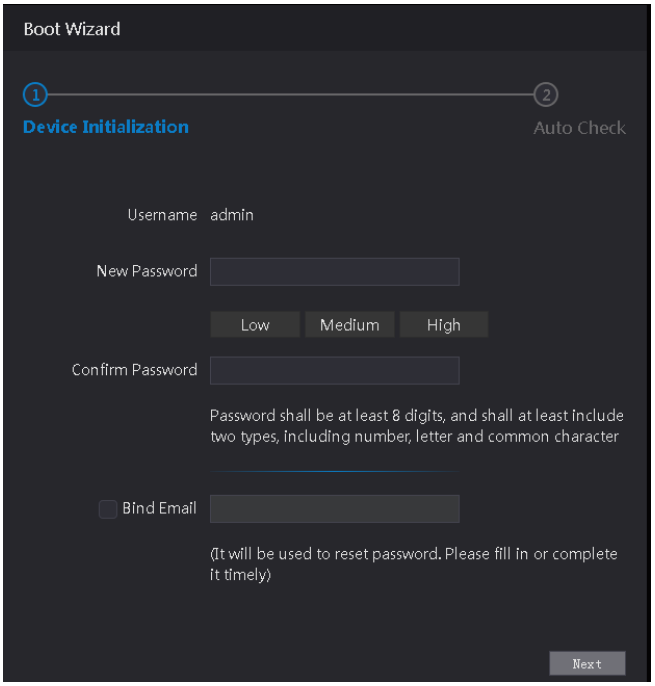
You need to set a password and an email address before logging in to the web for the first time.

Step 1 Open IE web browser, enter the IP address (the default address is 192.168.1.108) of the standalone in the address bar, and then press Enter key.

The **Initialization** interface is displayed.

Use browser newer than IE 8, otherwise you might not log in to the web.

Figure 4-1 Initialization



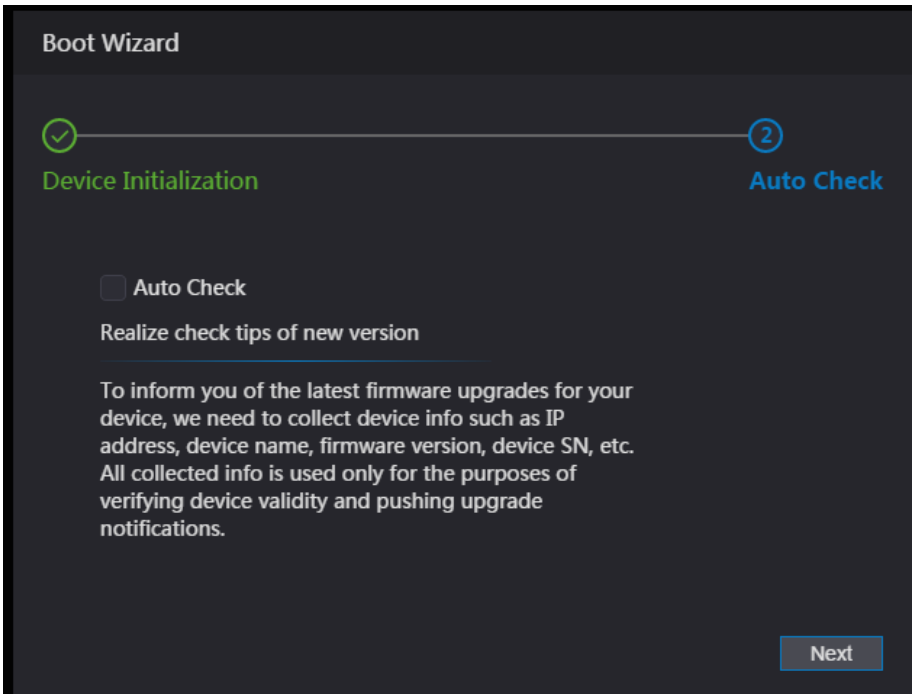
Step 2 Enter the new password, confirm password, enter an email address, and then tap **Next**.

- For security, keep the password properly after initialization and change the password regularly.
- 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 ' " ; : &). Set a password of high security level according to the password strength prompt.
- When you need to reset the administrator password by scanning the QR code, you need an email address to receive the security code.

Step 3 Click **Next**.

The auto check interface is displayed.

Figure 4-2 Auto Test



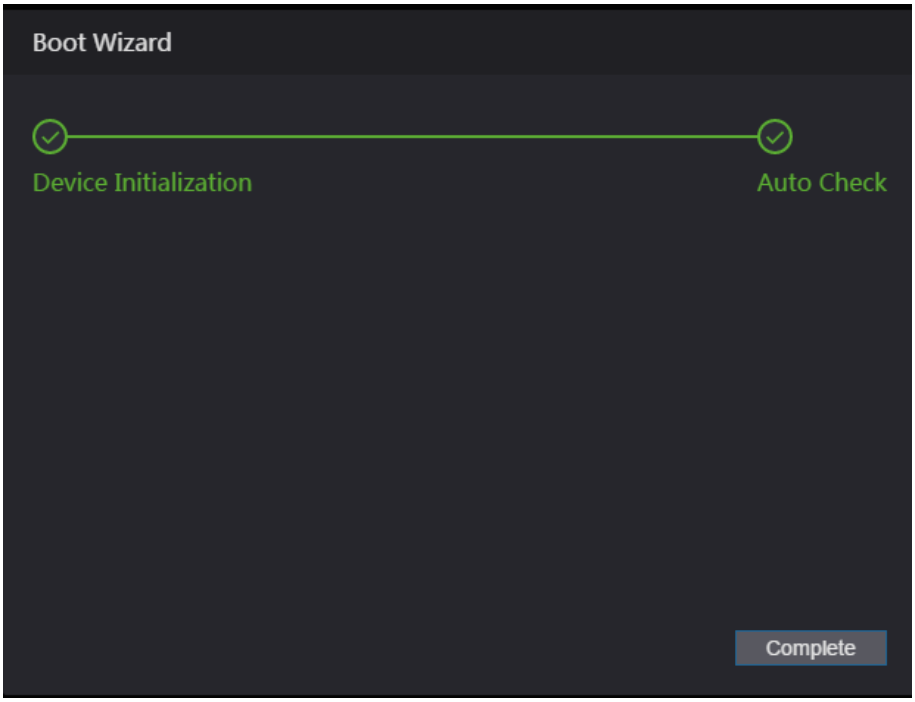
Step 4 You can decide whether to select **Auto Check**.

It is recommended that **Auto Check** be selected to get the latest program in time.

Step 5 Click **Next**.

The configuration is finished.

Figure 4-3 Finished configuration



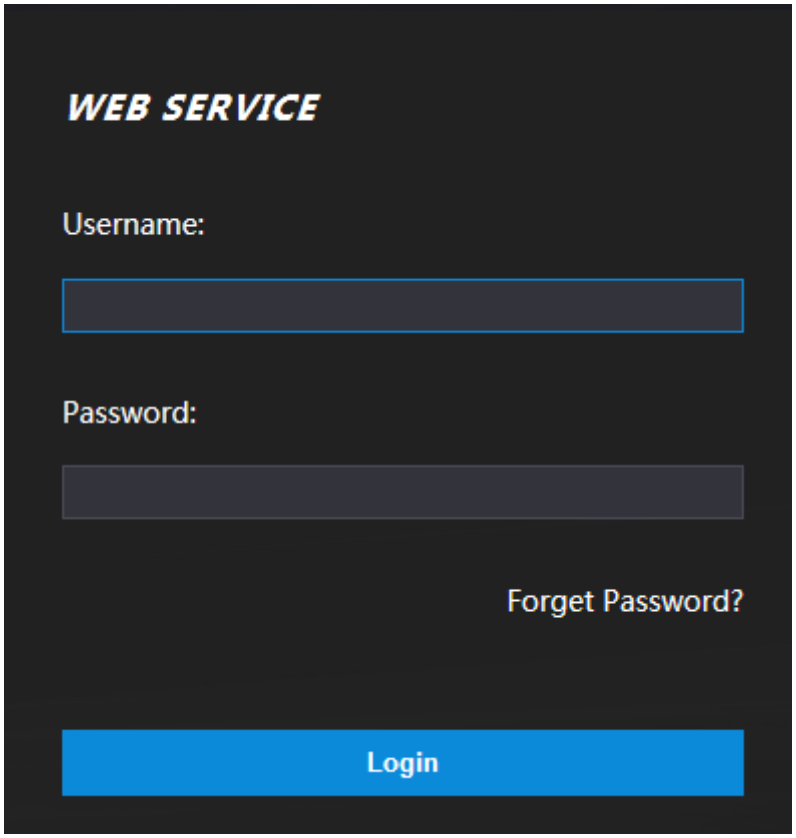
Step 6 Click **Complete**, and the initialization is completed.

The web login interface is displayed.

4.2 Login

Step 1 Open IE web browser, enter the IP address of the standalone in the address bar, and then press Enter. The login interface is displayed.

Figure 4-4 Login



Step 2 Enter the username and password.

- The default administrator name is admin, and the password is the login password after initializing the standalone. Modify the password regularly and keep it properly for the sake of security.
- If you forget the administrator login password, you can click **Forget password?** to reset it. See "4.3 Resetting the Password."

Step 3 Click **Login**.

The web interface is logged in.

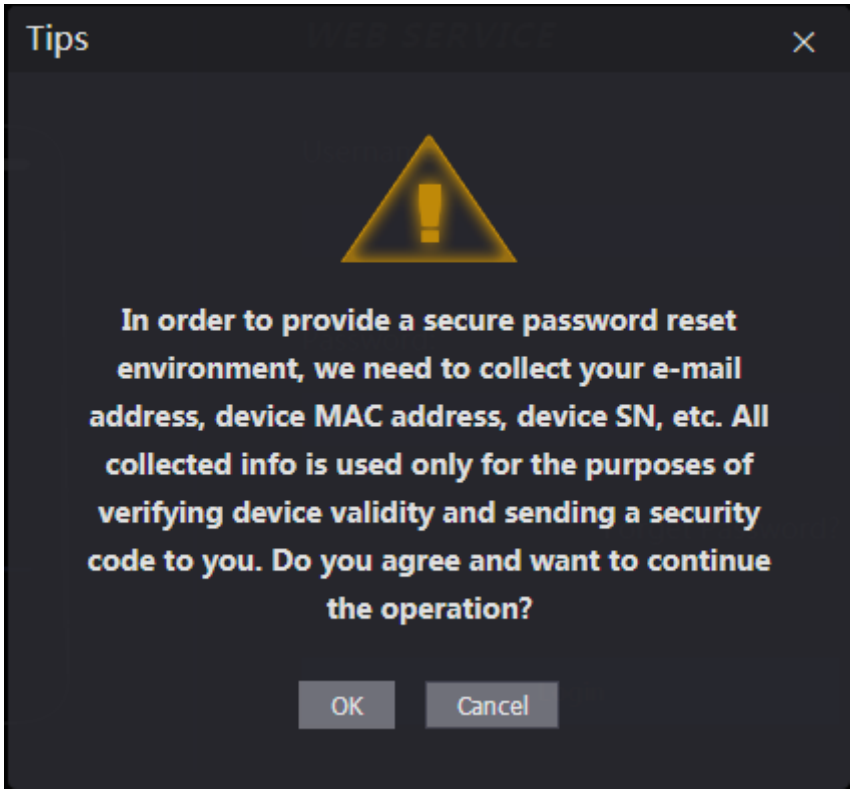
4.3 Resetting the Password

When resetting the password of the admin account, your email address will be needed.

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

The **Tips** interface is displayed.

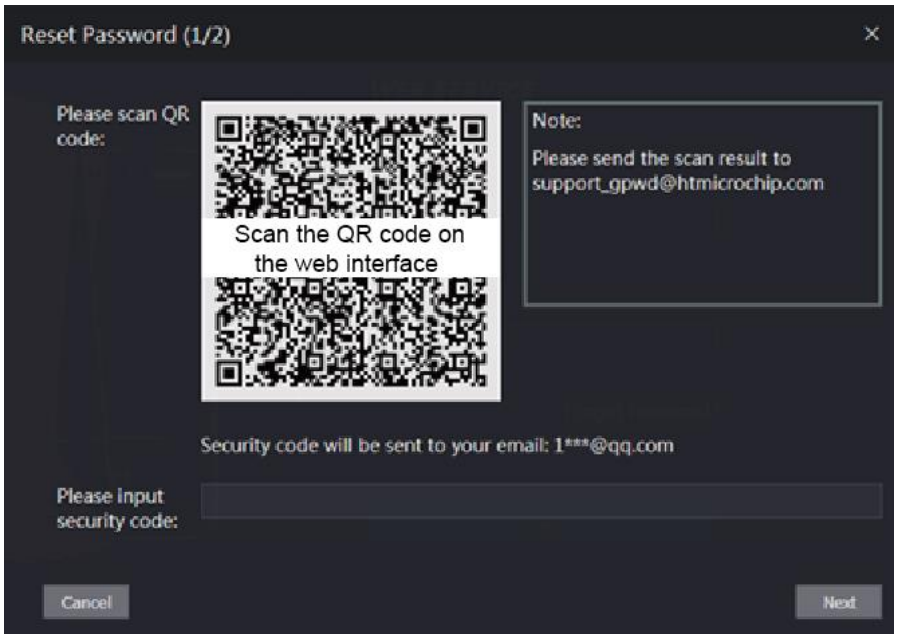
Figure 4-5 Tips



Step 2 Read the tips, and click **OK**.

The **Reset Password** interface is displayed.

Figure 4-6 Reset password



Step 3 Scan the QR code on the interface, and you will get the security code.

- At most two security codes will be generated by scanning the same QR code. To get more security code, refresh the QR code.
- You need to send the content you get after you scanned the QR code to the designated email address, and then you will get the security code.

- Please 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** interface is displayed.

Step 6 Reset and confirm the new 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 ' " ; : &).

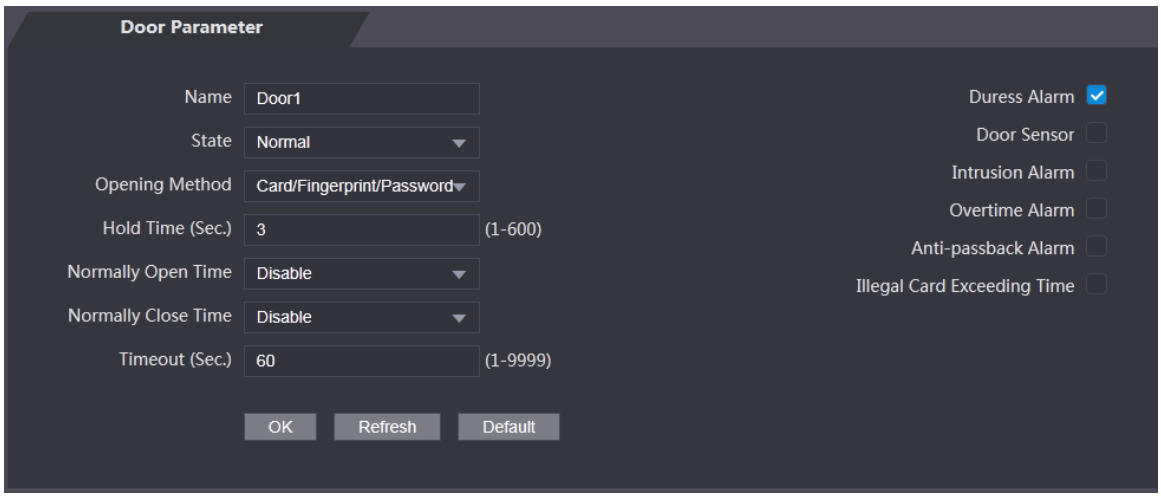
Step 7 Click **OK**, and the reset is completed.

4.4 Door Parameter

Set the door parameters including name, state, opening method, hole time, normally open time, normally close time, timeout, and enable the alarms that might be triggered during unlocking the door.

Step 1 Click **Door Parameter**.

Figure 4-7 Door parameter



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**. ● Normal: If **Normal** is selected, the door will be unlocked and locked depending on your settings. ● NC: If **NC** is selected, the door status is normally closed, which means the door will not be unlocked. ● NO: If **NO** is selected, the door status is normally open, which means the door will never be closed.

Parameter	Description
Opening Method	Select a unlock method.
Hold Time (Sec.)	The duration in which the door is unlocked. If the door has been unlocked for a period that exceeds the duration, the door will be automatically locked., and the range is 1–600 seconds.
Normally Open Time	Select the period that you set in **Time Section**. During the selected period, the door is normally open. And it is disabled by default.
Normally Close Time	Select the period that you set in **Time Section**. During the selected period, the door is normally closed. And it is disabled by default.
Timeout (Sec.)	When the door opens longer than the configured time, the overtime alarm will be triggered.

Step 3 Enable the alarms as needed.

Only when **Door Sensor** is enabled, can I**ntrusion Alarm** and **Overtime Alarm** be triggered.

4.5 Alarm Linkage

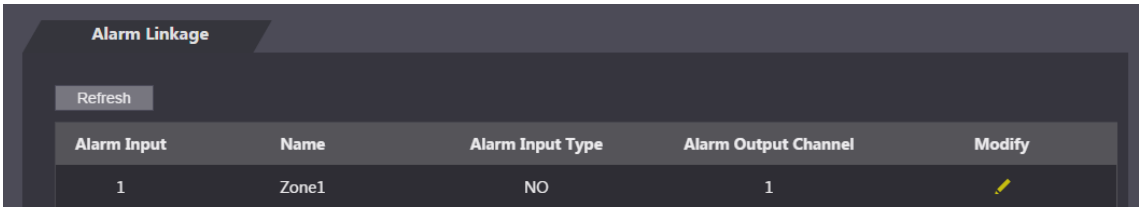
4.5.1 Setting Alarm Linkage

Alarm input devices can be connected to the standalone, and you can modify the alarm linkage parameter as needed.

Step 1 Select **Alarm Linkage > Alarm Linkage** on the navigation bar.

The **Alarm Linkage** interface is displayed.

Figure 4-8 Alarm linkage



Step 2 Click , and then you can modify alarm linkage parameters.

Figure 4-9 Modifying alarm linkage parameter

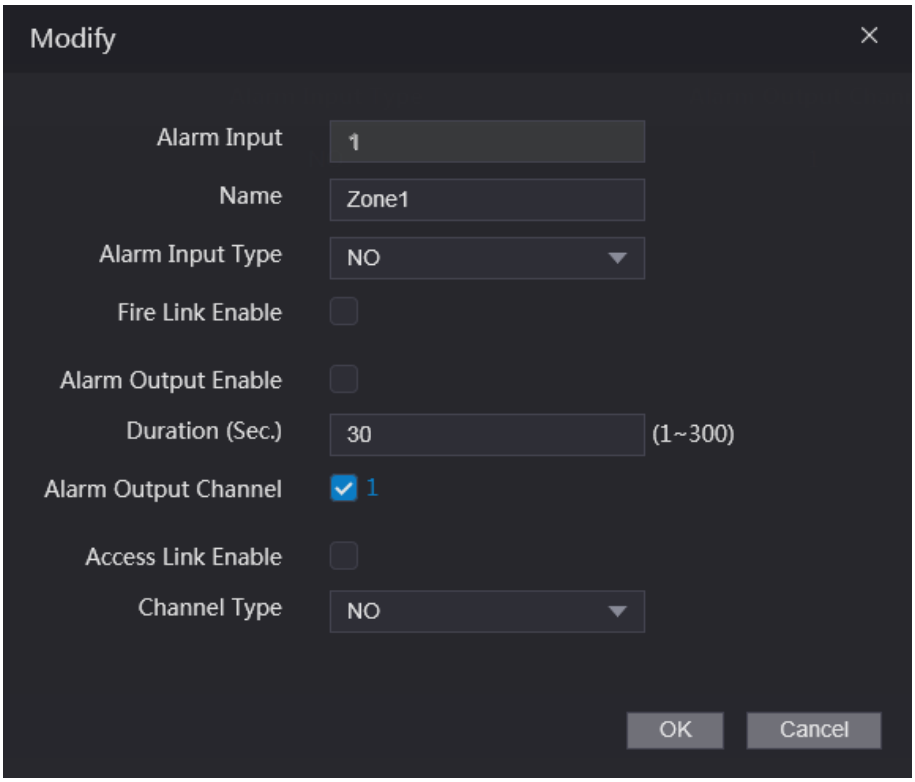


Table 4-2 Alarm linkage parameter description

Parameter	Description
Alarm Input	You cannot modify the value. Keep it default.
Name	Enter a zone name.
Alarm Input Type	There are two options: **NO** and **NC**. If alarm input type of the alarm device you purchased is **NO**, then you should select **NO**; otherwise you should select **NC**.
Fire Link Enable	If fire link is enabled, the standalone will output alarms when fire alarms are triggered. The alarm details will be displayed in the alarm log. Alarm output and access link are NO by default if fire link is enabled.
Alarm Output Enable	The relay can output alarm information (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	You can select an alarm output channel according to the alarming device that you have installed. 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**, and then the configuration is completed.

The configuration on the web will be synchronized with the configuration in the client if the standalone is added to a client.

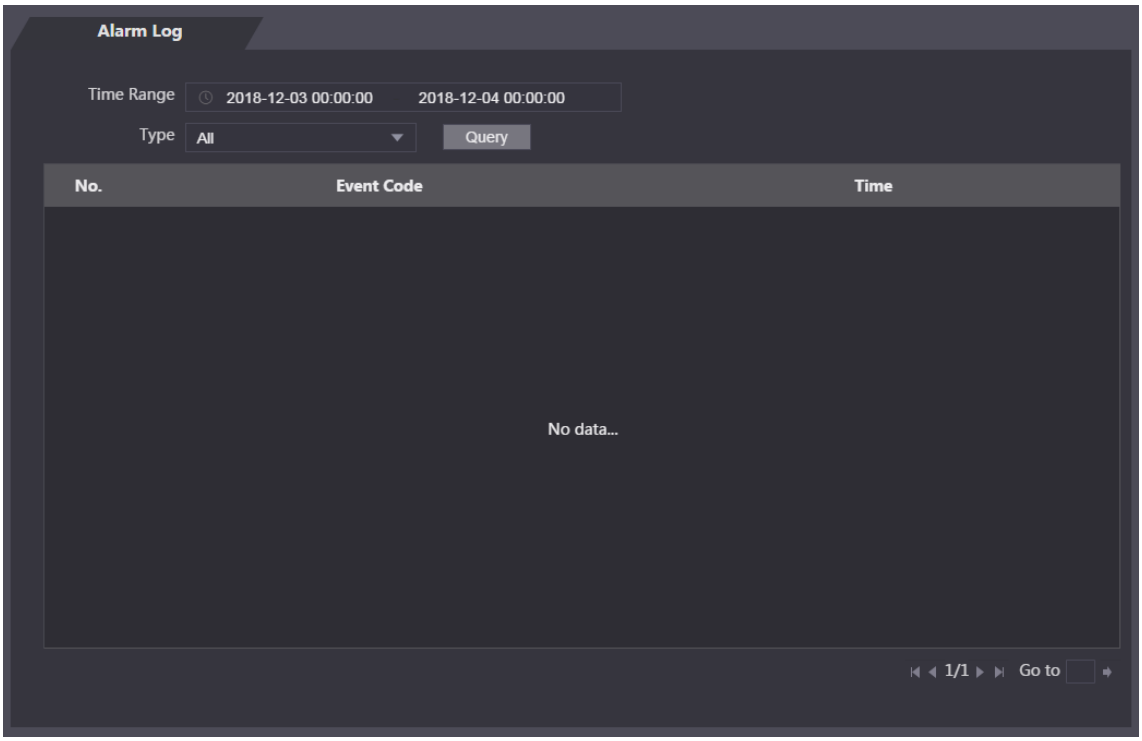
4.5.2 Alarm Log

You can view the alarm type and time range on the **Alarm Log** interface.

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

The **Alarm Log** interface is displayed.

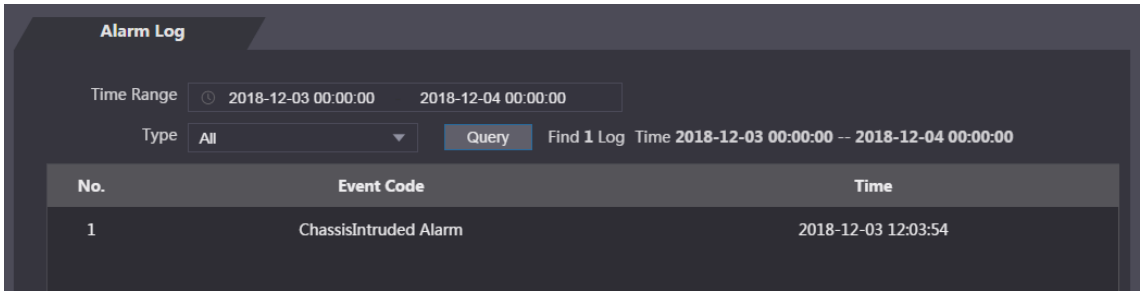
Figure 4-10 Alarm log



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

The query results are displayed.

Figure 4-11 Query results



4.6 Time Section Configuration

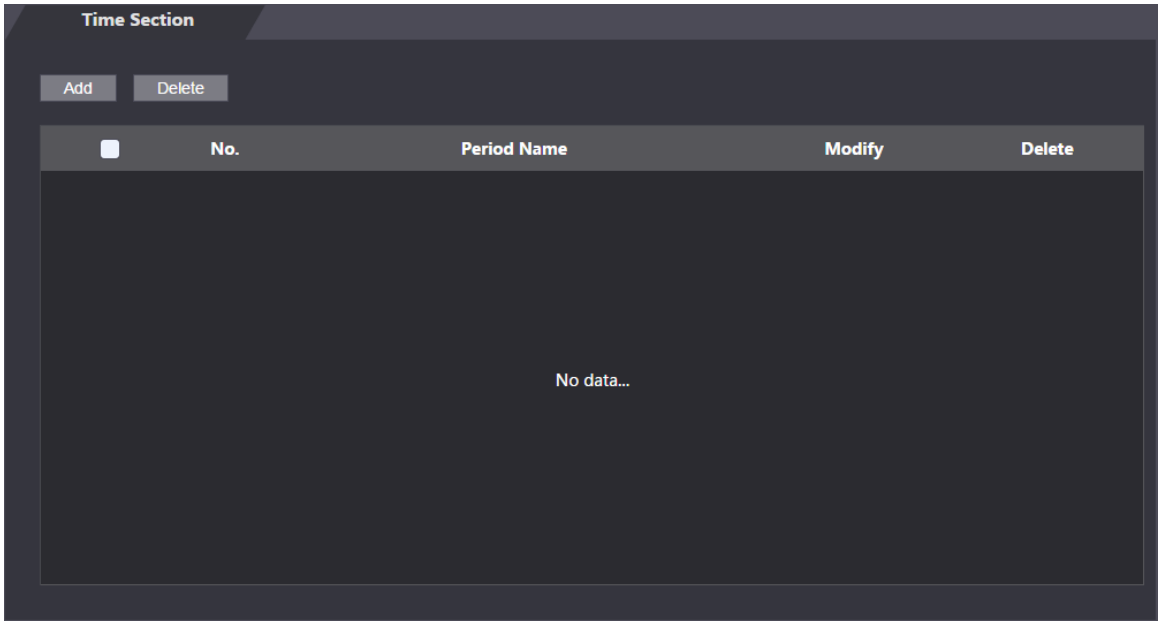
You can set periods, holiday periods, and holiday plan periods.

4.6.1 Time Section

After setting the period, users can only unlock the door in the periods that you have set.

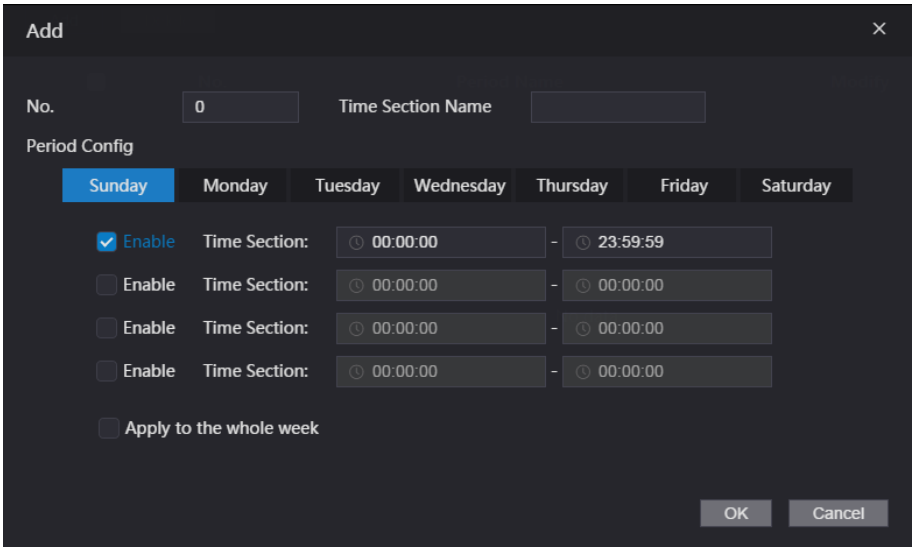
Step 1 Select **Time Section > Time Section**.

Figure 4-12 Time section



Step 2 Click **Add**.

Figure 4-13 Add period



Step 3 Set the period number and time section name. Select the **Enable** check box, and the time section as needed.

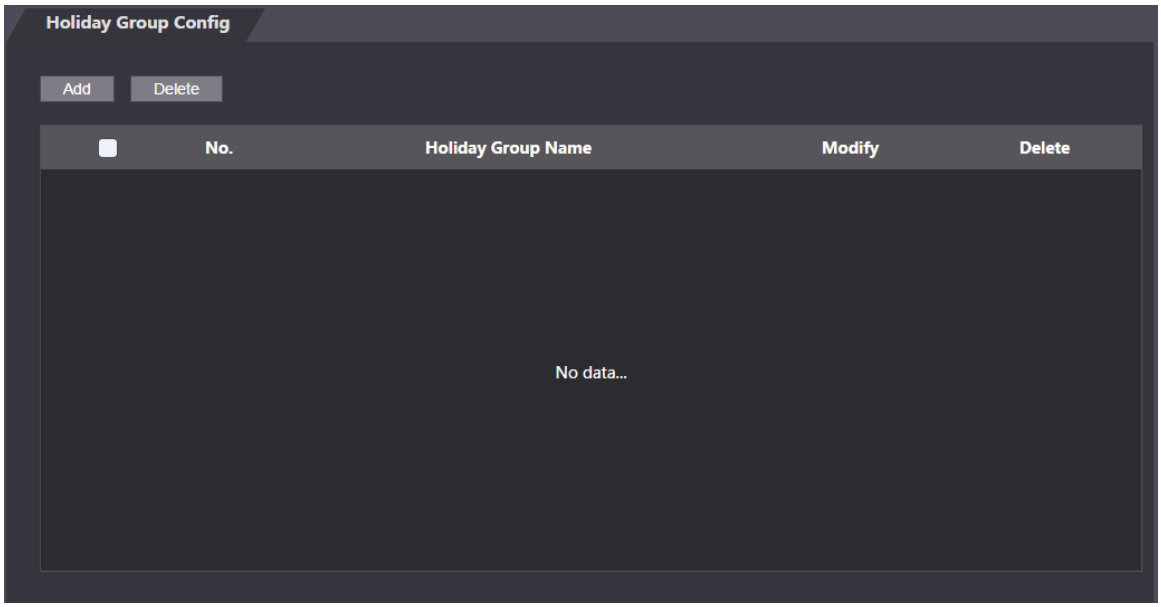
You can configure 128 periods (weeks) whose number range is 0–127, and set four periods on each day of a period (week). The default is 255, which indicates that the period is not configured; 0–127 is the period configured manually. You can edit the configured period in the **User List** on the standalone.

4.6.2 Holiday Group Configuration

Configure the start time and end time of a holiday group, and then users cannot unlock the door in the periods that you have set.

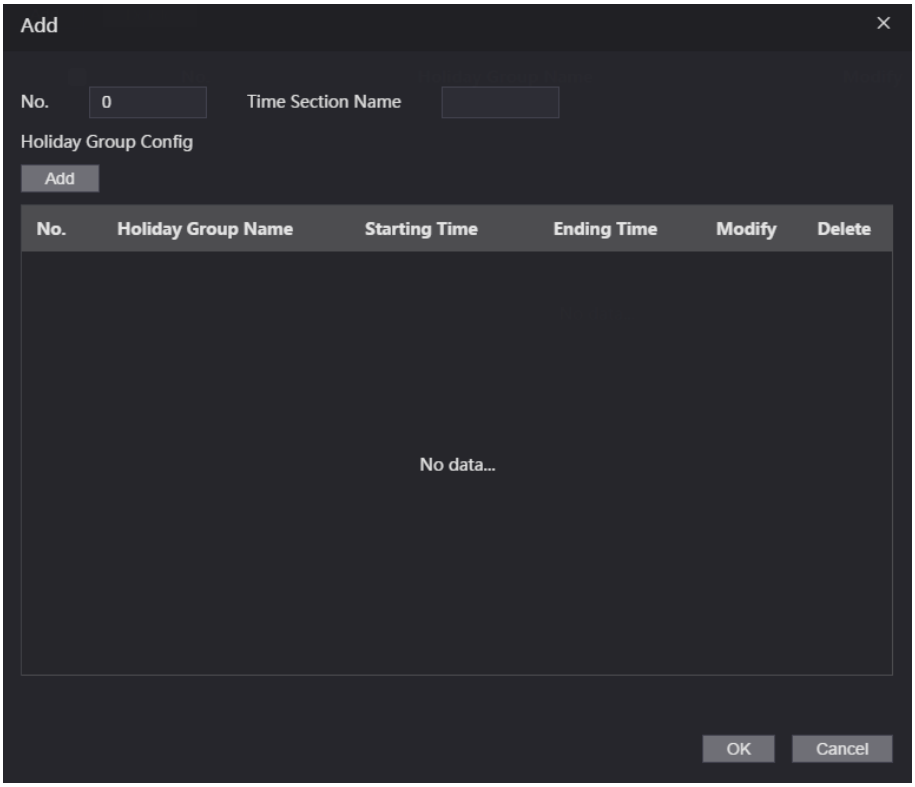
Step 1 Select **Time Section > Holiday Group Config**.

Figure 4-14 Holiday group configuration



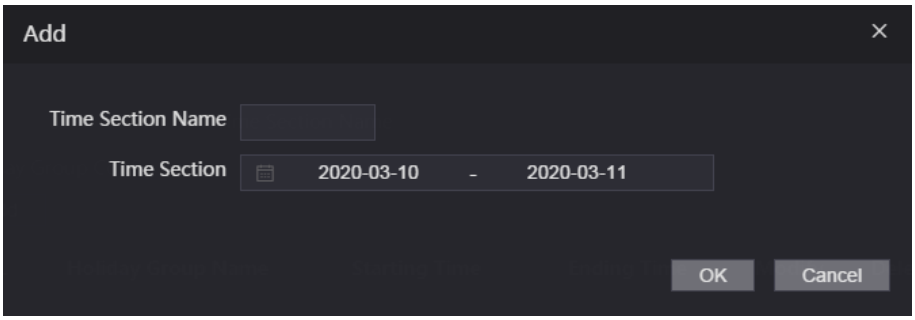
Step 2 Click **Add**.

Figure 4-15 Add holiday group



Step 3 Set the period number and time section name, and then click **Add**.

Figure 4-16 Add holiday group configuration



Step 4 Set time section name and the time section as needed.

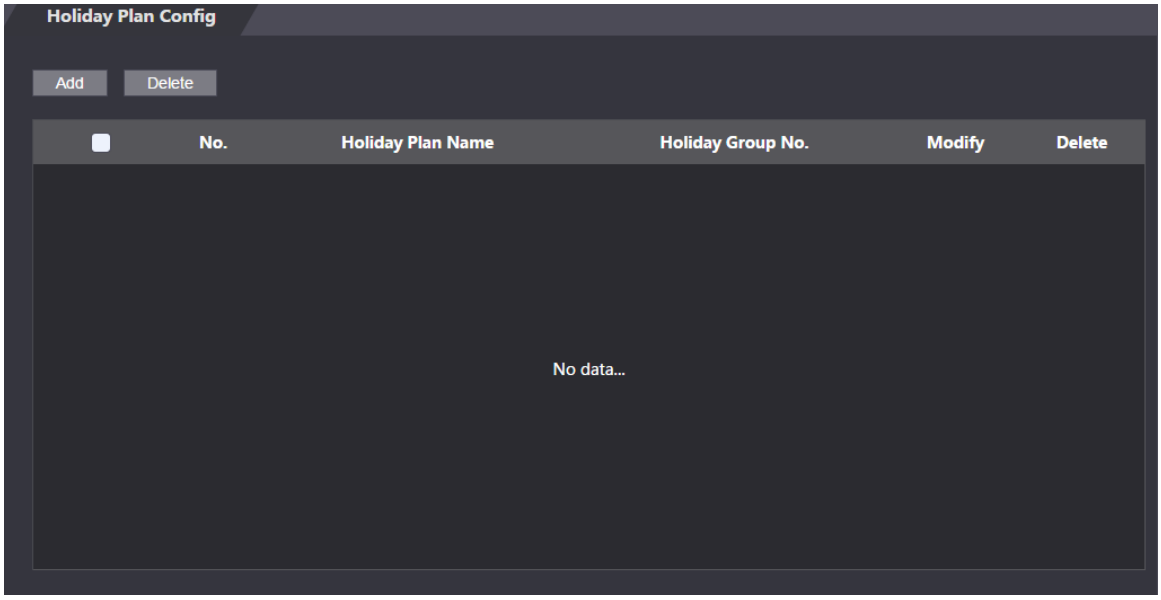
You can set group holidays, and then you can set plans for holiday groups. You can configure 128 groups whose number range is 0–127. You can add 16 holidays into a group.

4.6.3 Holiday Plan Configuration

You can add holiday groups into holiday plans, and users can only unlock the door in the period that you set.

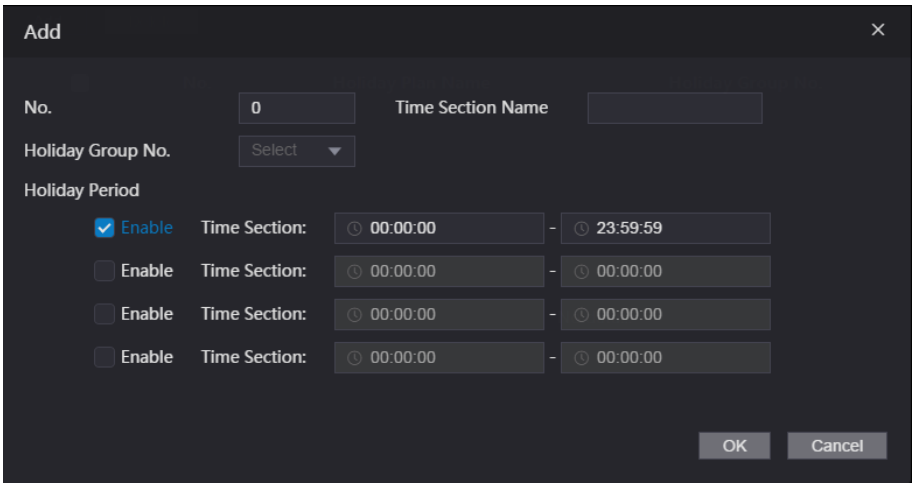
Step 1 Select **Time Section > Holiday Plan Config**.

Figure 4-17 Holiday plan configuration



Step 2 Click **Add**.

Figure 4-18 Add holiday plan



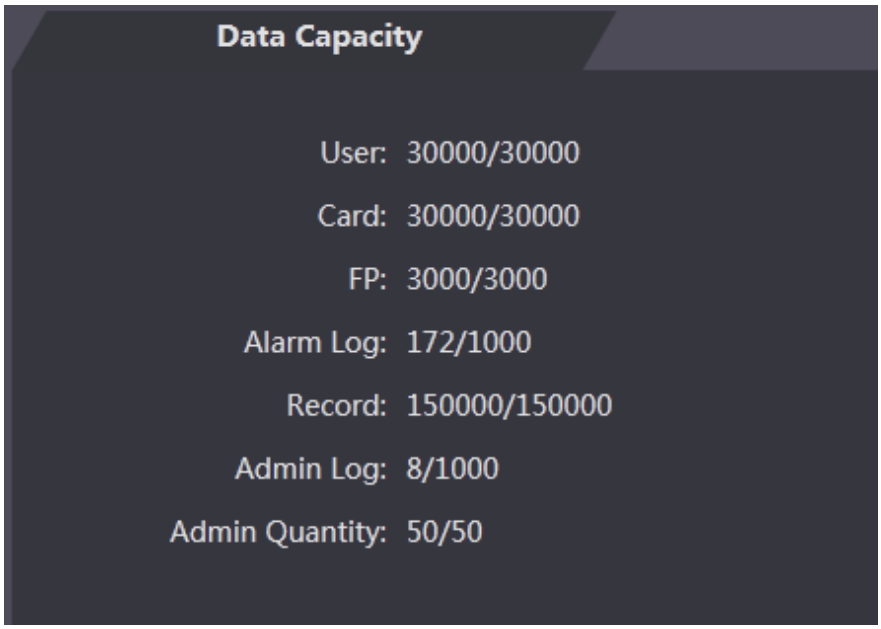
Step 3 Set the period number and time section name, select the holiday group number, select the **Enable** check box, and then set the time section.

Step 4 Click **OK**.

4.7 Data Capacity

You can see how many users, cards, fingerprints, alarm logs, records, admin logs and admin quantity the standalone can hold on the **Data Capacity** interface.

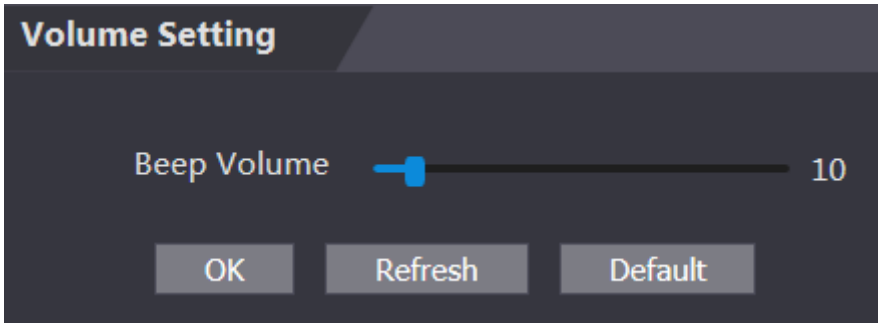
Figure 4-19 Data capacity



4.8 Volume Setting

You can set beep volume on the **Volume Setting** interface.

Figure 4-20 Volume setting



4.9 Network Setting

4.9.1 TCP/IP

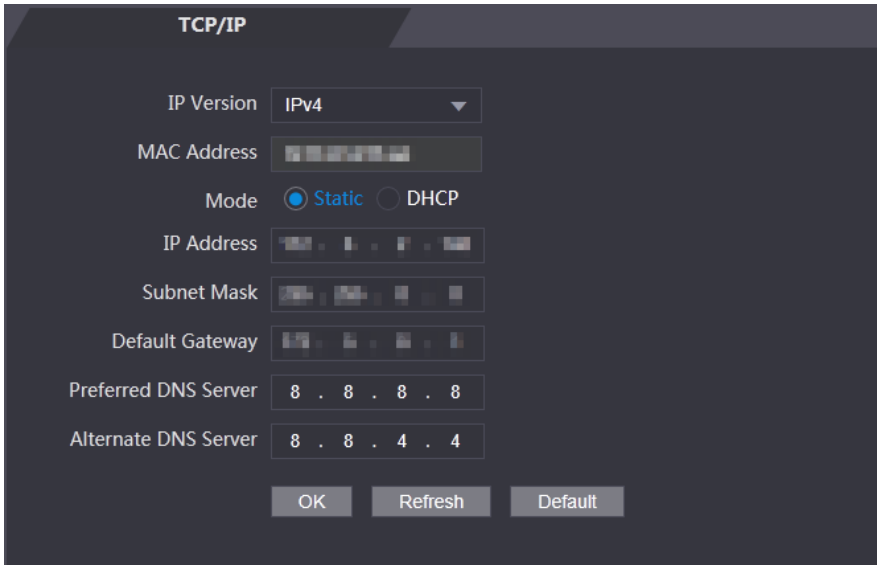
You need to configure IP address and DNS server to make sure that the standalone can communicate with other devices.

Precondition

Make sure that the standalone is connected to the network correctly.

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

Figure 4-21 TCP/IP



Step 2 Configure parameters.

Table 4-3 TCP/IP

Parameter	Description
IP Version	There is one option: IPv4.
MAC	MAC address of the standalone is displayed.
Mode	● Static Set IP address, subnet mask, and gateway address manually. ● DHCP ◇ After DHCP is enabled, IP address, subnet mask, and gateway address cannot be configured. ◇ If DHCP is effective, IP address, subnet mask, and gateway address will be displayed automatically; if DHCP is not effective, IP address, subnet mask, and gateway address will all be zero.
IP Address	Enter IP address, and then configure subnet mask and gateway address. IP address and gateway address must be in the same network segment.
Subnet Mask	
Gateway	
Preferred DNS Server	Set IP address of the preferred DNS server.
Alternate DNS Server	Set IP address of the alternate DNS server.

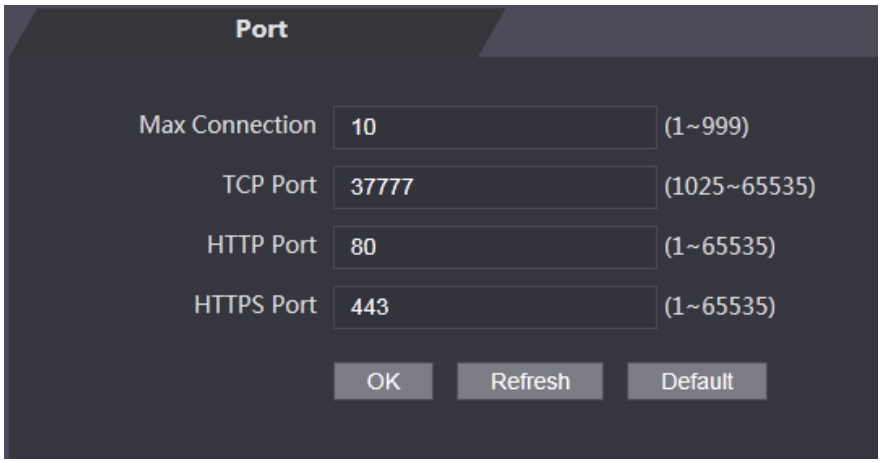
Step 3 Click **OK** to complete the setting.

4.9.2 Port

Set the maximum clients that the standalone can be connected to and port numbers.

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

Figure 4-22 Port



Step 2 Configure port numbers. See the following table.

Except max connection, you need to reboot the standalone to make the configuration effective after modifying values.

Table 4-4 Port description

Parameter	Description
Max Connection	You can set the maximum clients that the standalone can be connected to. Platform clients like SmartPSS are not counted.
TCP Port	The value is 37777 by default.
HTTP Port	The value is 80 by default. If other value is used as port number, you need to add this value behind the address when logging in through browsers.
HTTPS Port	The value is 443 by default.

Step 3 Click **OK** to complete the setting.

4.9.3 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 so that more than one standalone can be managed on the mobile app. You do not need to apply dynamic domain name, do port mapping or do not need transit server.

If you are to use P2P, you must connect the standalone to external network; otherwise the standalone cannot be used.

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

Figure 4-23 P2P

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

Step 3 Click **OK** to complete the setting.

Scan the QR code on your web interface to get the serial number of the standalone.

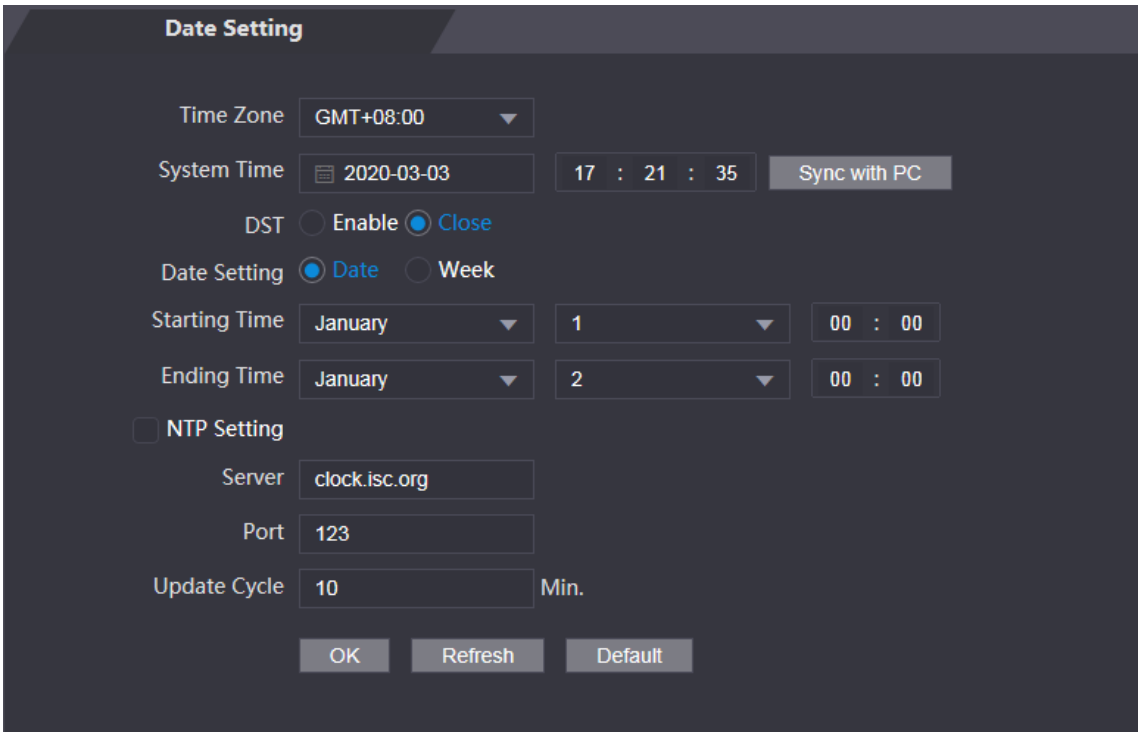
4.10 Data Setting

You can set time zone, system time, date, DST, and NTP.

When you select Network Time Protocol (NTP), you need to configure the following parameters. You need to enable the NTP Check function first.

- Server: Enter the IP address of the time server, and time of the standalone will be synchronized with the time server.
- Port: Enter the port number of the time server.
- Update Cycle (min): NPT check interval. Tap the save icon to save.

Figure 4-24 Date setting

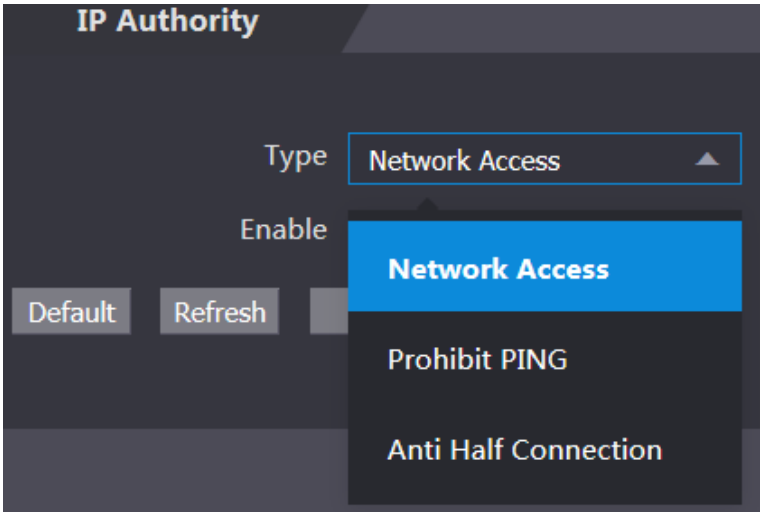


4.11 Safety Management

4.11.1 IP Authority

Select a cyber security mode as needed.

Figure 4-25 IP authority



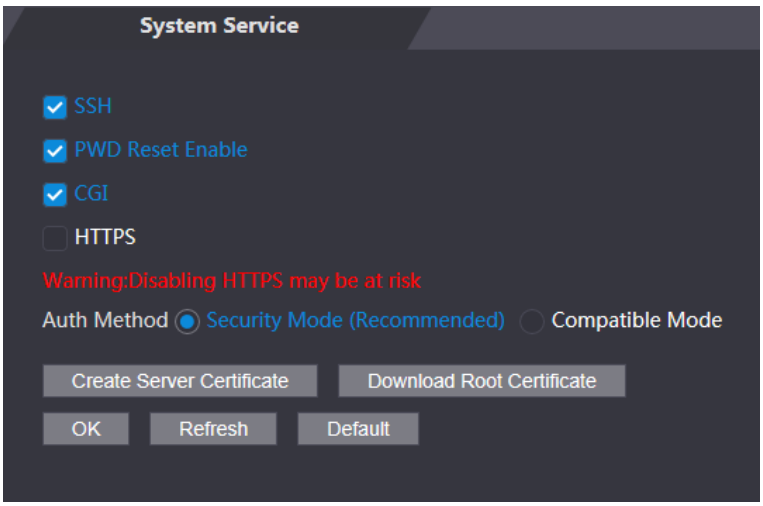
4.11.2 System

4.11.2.1 System Service

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

The system service configuration done on the web page and the configuration on the **Privacy Setting** interface of the standalone will be synchronized.

Figure 4-26 System service



4.11.3 User Management

You can add and delete users, modify users' passwords, and enter an email address for resetting the password when you forget your password.

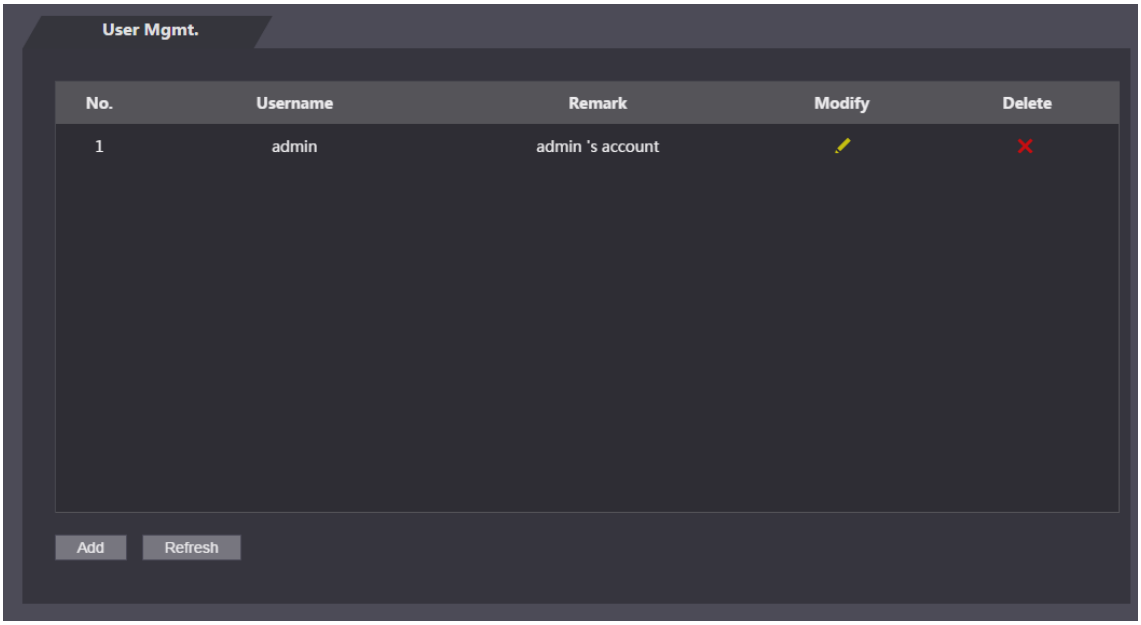
4.11.3.1 Add Users

Click **Add** on the **User Mgmt.** interface to add users, and then enter username, password, confirmed password, and remark. Click **OK** to complete the user adding.

4.11.3.2 Modify User Information

You can modify user information by clicking on the **User Mgmt.** interface.

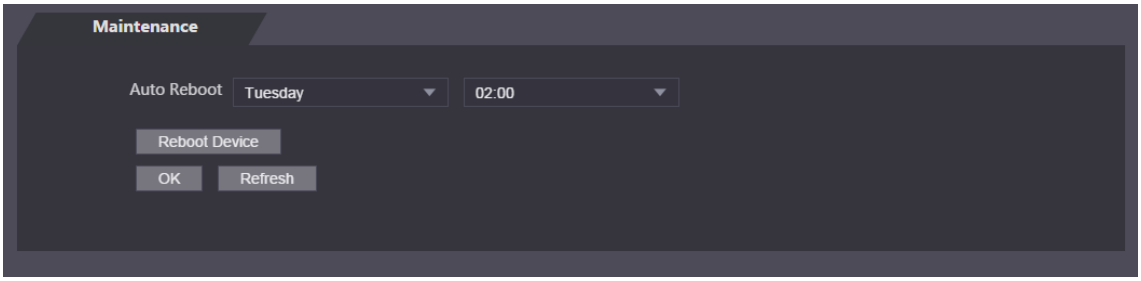
Figure 4-27 User management



4.11.4 Maintenance

You can make the standalone restart automatically in idle time to improve the running speed of the standalone.

Figure 4-28 Maintenance

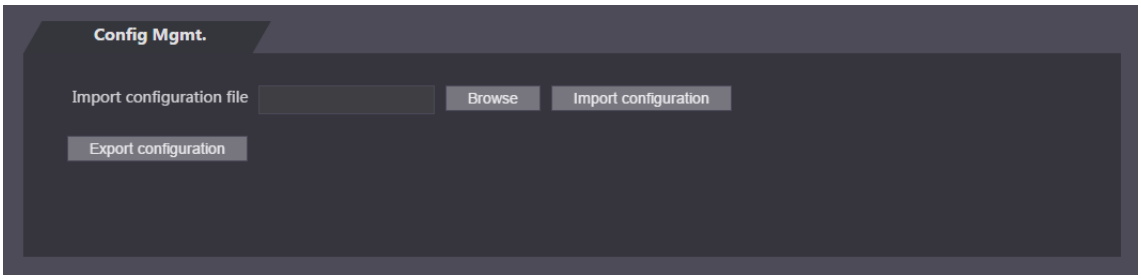


Select the auto reboot date and time. The default reboot time is at 2 o’clock in the morning on Tuesday. Click **Reboot Device**, the standalone will reboot immediately. Click **OK**, the standalone will reboot at 2 o’clock in the morning every Tuesday.

4.11.5 Configuration Management

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

Figure 4-29 Configuration management



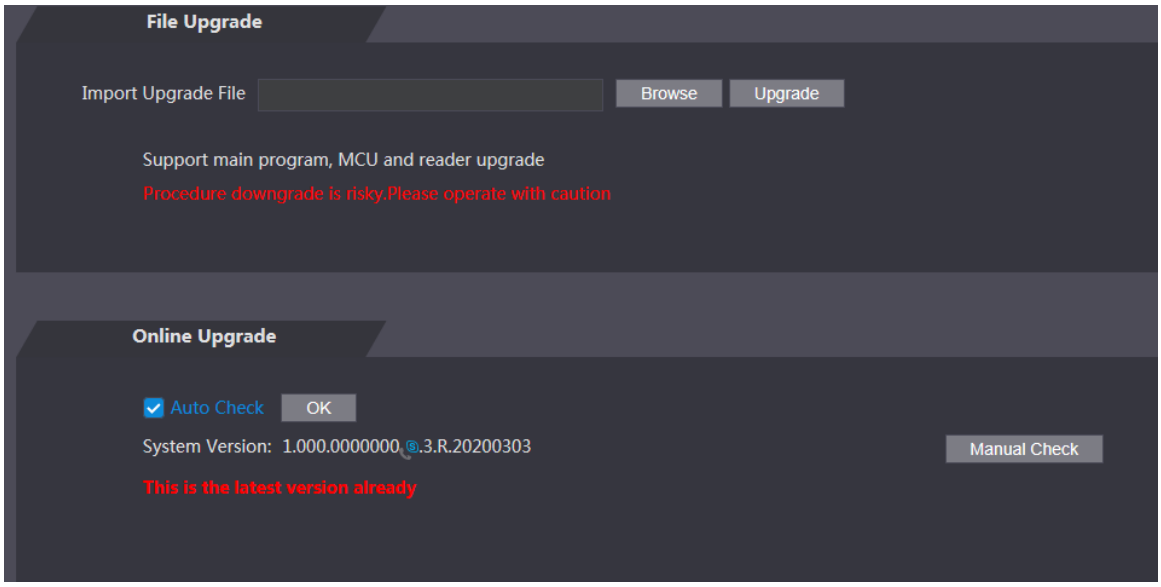
4.11.6 Upgrade

Upgrading to the latest system can perfect standalone functions and improve stability.

If wrong upgrade file has been used, the system will prompt that the upgrading fails and restart the device automatically.

Step 1 Click **Upgrade** on the navigation bar.

Figure 4-30 Upgrade



Step 2 Select upgrading method according to the actual needs.

- File Upgrade

1) Click **Browse**, and then upload upgrade file.
   The upgrade file should be a .bin file.
2) Click **Upgrade**.
   The upgrade starts.

- Online Upgrade

1) Select the **Auto Check** check box, and click **OK**.

The system checks for upgrade once a day automatically, and there will be system notice if any upgrade is available.

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

2) If there is any upgrade available, click **Upgrade**, and then the system starts upgrading.

Click **Manual Check** to check for upgrade manually.

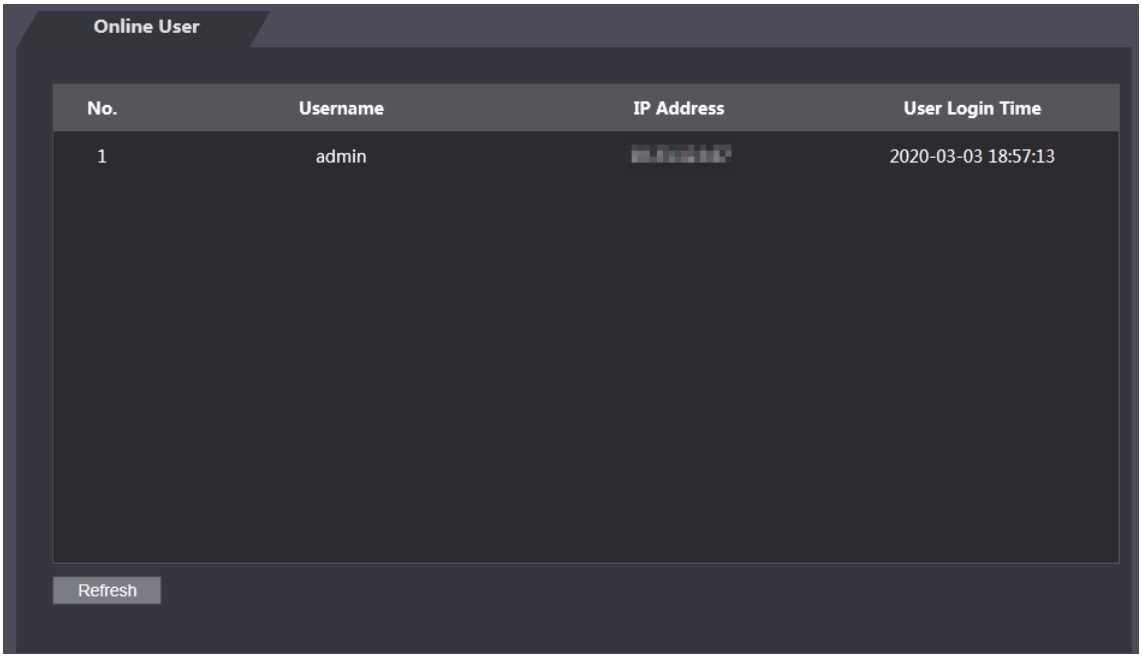
4.11.7 Version Information

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

4.11.8 Online User

You can view username, IP address, and user login time on the **Online User** interface.

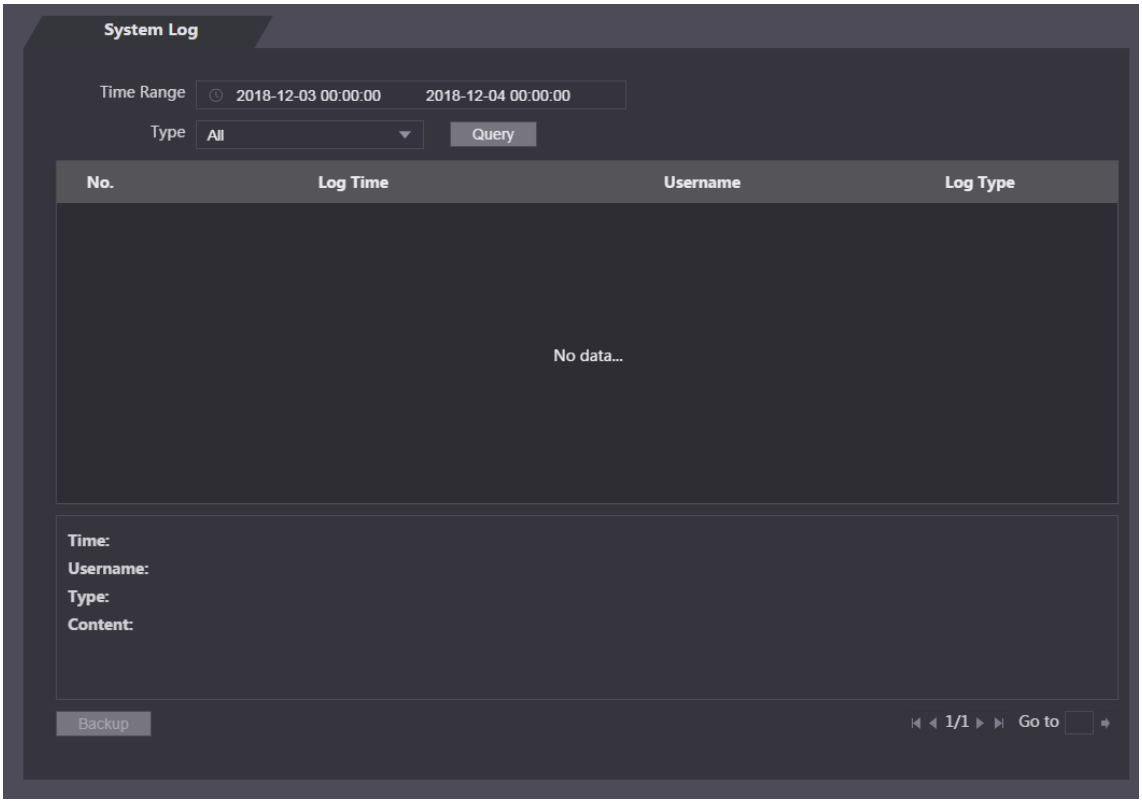
Figure 4-31 Online user



4.12 System Log

You can view and backup the system log on the **System Log** interface.

Figure 4-32 System log



4.12.1 Query Logs

Select a time range, type, click **Query**, and logs meet the conditions will be displayed.

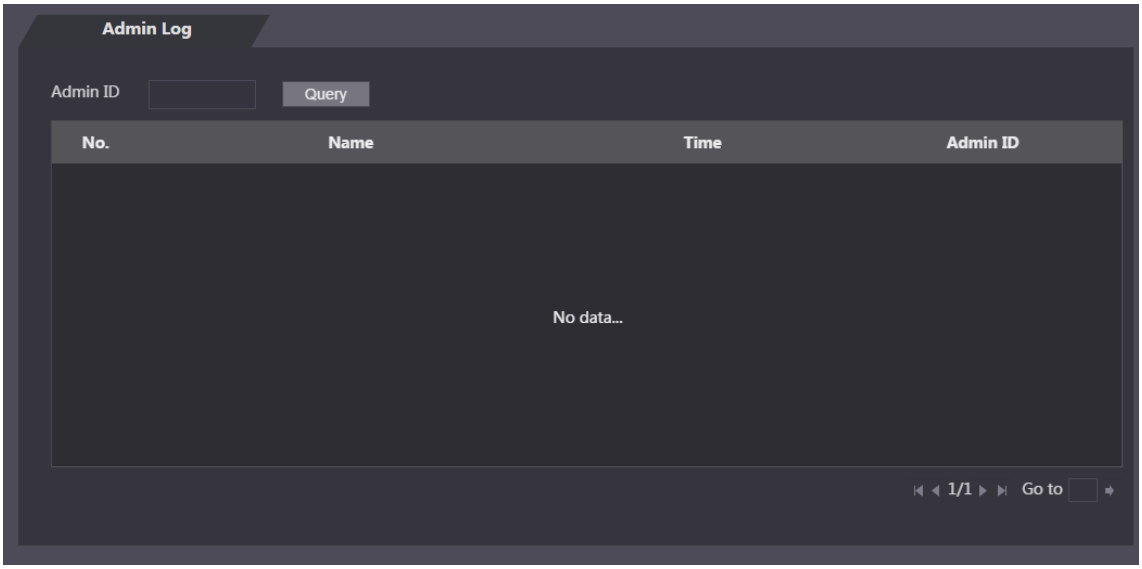
4.12.2 Backup Logs

Click **Backup** to back up the logs displayed.

4.13 Admin Log

Enter Admin ID on the **Admin Log** interface, click **Query**, and then you will see the administrator's operation records.

Figure 4-33 Admin log



4.14 Exit

Click , click **OK**, and then you will log out the web interface.

Hover over , and then you can see detailed information of the current user.

5 Mobile Phone Operation

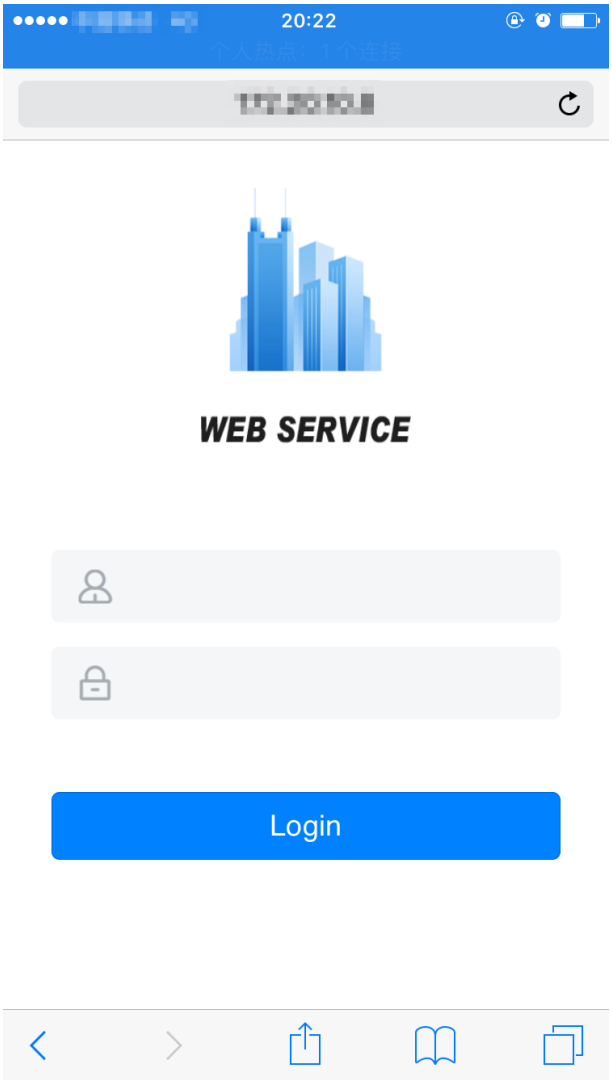
The standalone can be configured and operated on the mobile phone. Through the mobile phone you can set parameters including network parameters, video parameters, and standalone parameters; and you can also maintain and update the system.

Login

Step 1 Connect the device and mobile phone to the same network.

Step 2 Open the browser on the mobile phone, enter the device IP address (it is displayed on the Wi-Fi interface, and 192.168.1.108 by default) of the standalone in the address bar, and then press Enter.

Figure 5-1 Login



Step 3 Enter the username and password.

The default username of administrator is admin, and the password is the login password after initializing the standalone. Modify the administrator password regularly and keep it properly for security.

Step 4 Click **Login**.

The homepage of the web is displayed.

6 Configuration on DSS Pro

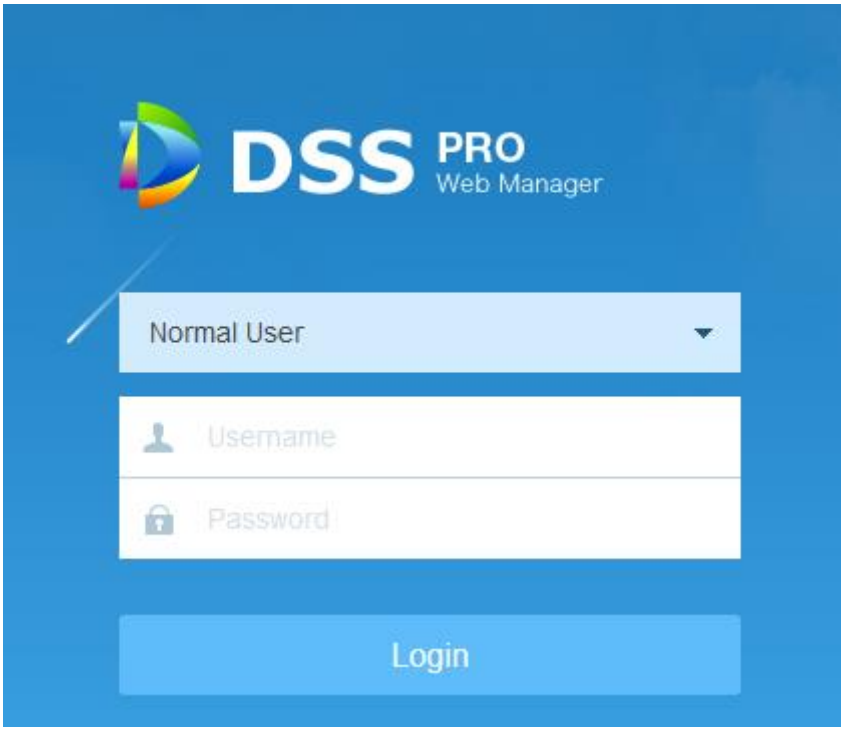
Before doing access control configurations, you need to add roles, users, and access control devices to DSS Pro; and you can set lock/unlock period and mode for certain users, devices, and door groups; and then you can give access permission to certain users or users in different door groups on DSS Pro Client. For detailed operation, see *DSS Pro User's Manual*.

6.1 Adding Devices

You need to add devise to the DSS Pro first so that you can do unlock management, period management, access permission configuration, and more on DSS Pro.

Step 1 Enter DSS Pro IP into the browser address bar, and press Enter.

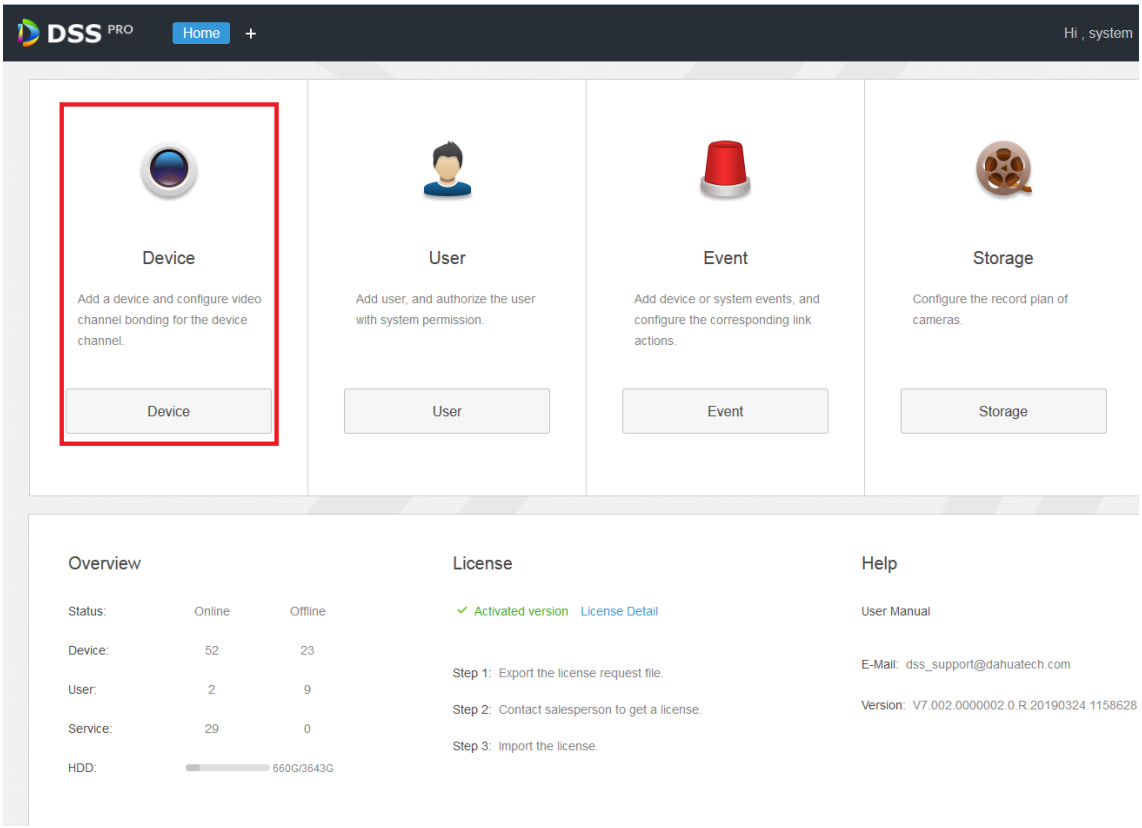
Figure 6-1 Login



Step 2 Enter the username and password

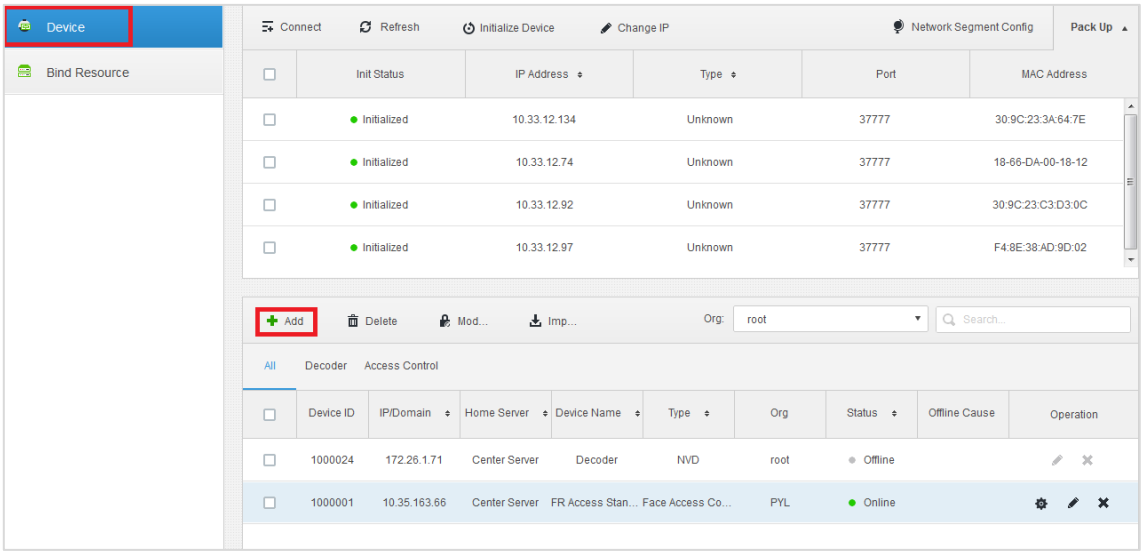
Step 3 Click **Login**.

Figure 6-2 Homepage



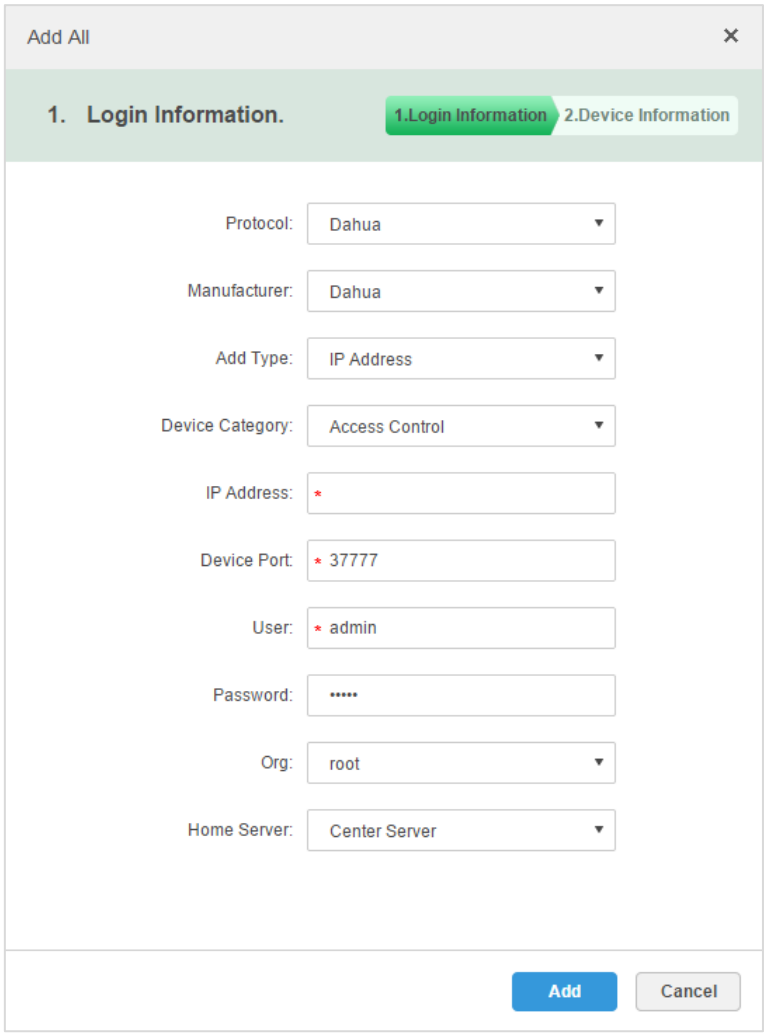
Step 4 On the homepage, click **Device**.

Figure 6-3 Device



Step 5 Click **Add**.

Figure 6-4 Add all

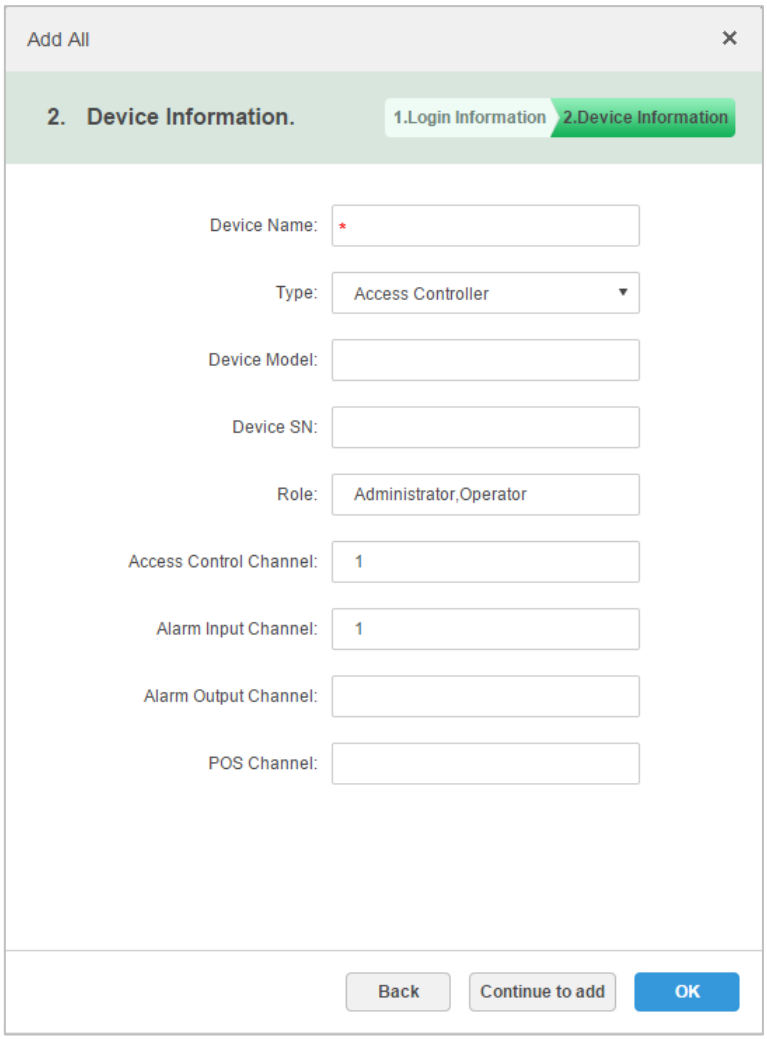


Step 6 Select Protocol, Manufacturer, Add Type, and Device Category; and enter IP Address, Device Port, User, Password, and more.

- Select **Access Control** as **Device Category**.
- Different protocols mean you will set different parameters; the actual interface shall prevail.
- When **IP Address** is selected, you need to enter IP address of the device you are to add.
- When Auto Register is selected, you need to enter Registration ID of the device you are to add. Auto Register is only for adding encoder, and the Registration ID should be the same as the Registration ID configured on the encoder.
- When Domain Name is selected. You need to enter domain name of the device you are to add.

Step 7 Click **Add**.

Figure 6-5 Device information



Step 8 Enter Device Name, Type, Device SN, Role, Access Control Channel, Alarm Input Channel, Alarm Output Channel, and POS Channel.

The type is obtained automatically after Step 7.

You can see the device you added on the **Device** interface.

If you want to add more devices, click **Continue to add**.

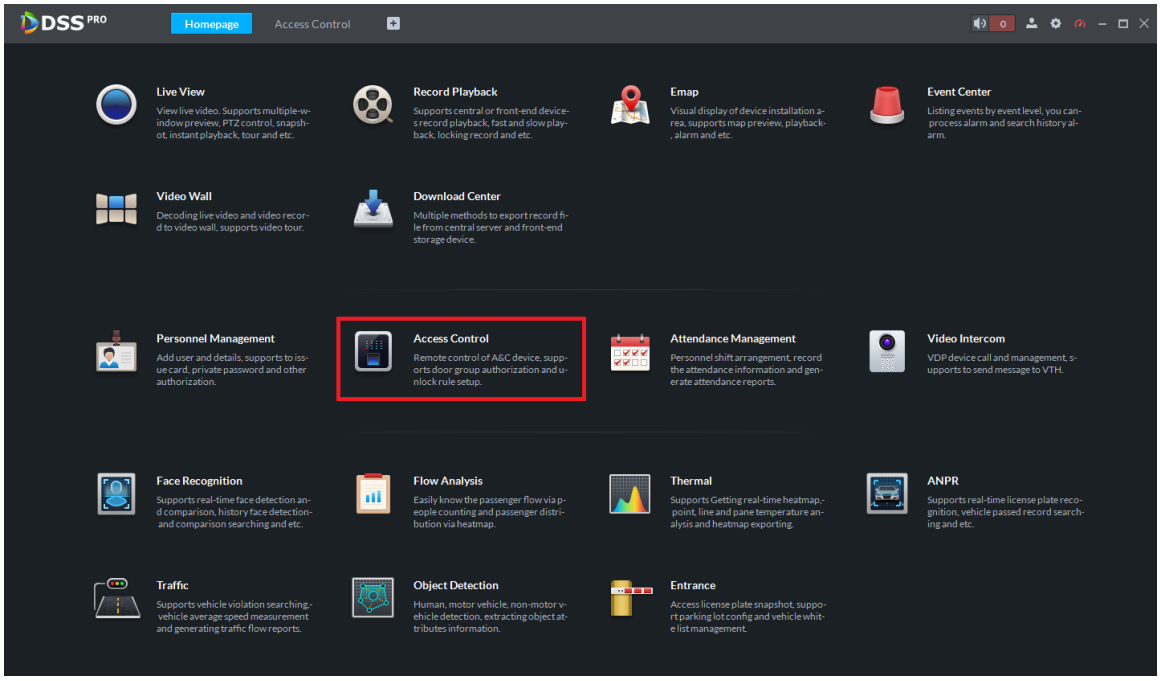
6.2 Access Control Management

You can do door configuration (door status, NO Period, NC Period, Alarm Enable, Unlock Length, Unlock Method) on DSS Pro Client depending on your needs.

6.2.1 Door Configuration

Step 1 Log in to DSS Pro Client.

Figure 6-6 Homepage



Step 2 Click **Access Control**.

Step 3 On the left side of the interface, right-click an access control channel in the device tree, and select **Door Configuration**.

Figure 6-7 Access control

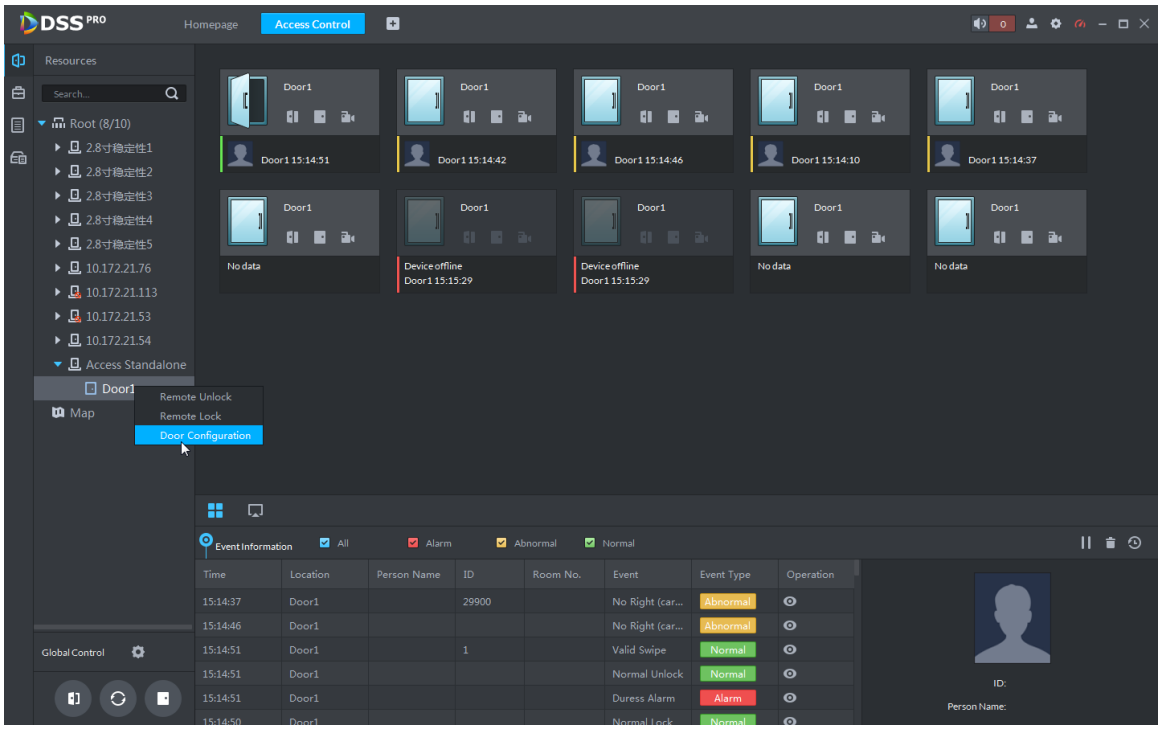


Figure 6-8 Door configuration

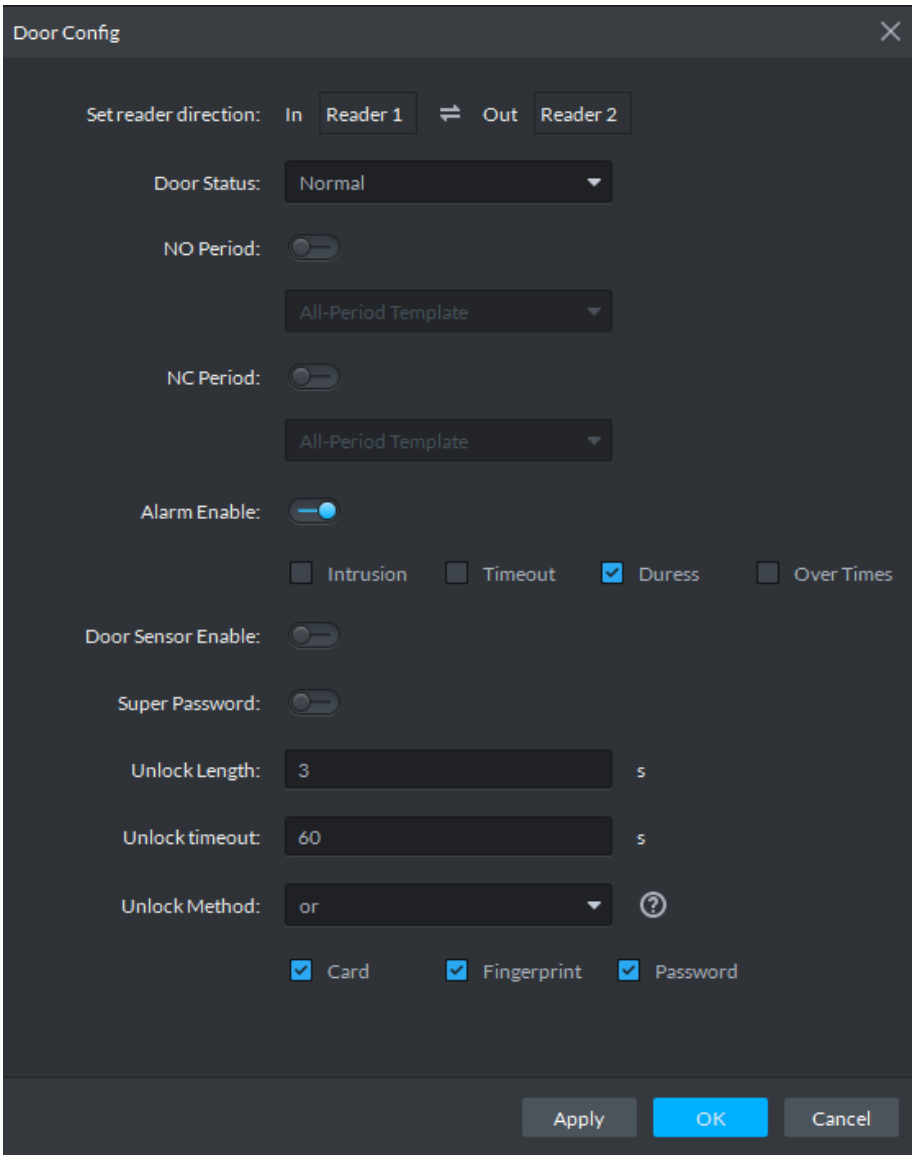


Table 6-1 Door configuration description

Parameter	Description
Set reader direction	Indicates the in/out reader based on the wiring of ACS.
Door Status	Sets the access control status to **Normal**, **Always Open**, or **Always Close**.
NO Period	If enabled, you can set a period during which the door is always open.
NC Period	If enabled, you can set a period during which the door is always closed.
Alarm Enable	● If the door is opened not as intended, the door sensor is enabled and triggers an intrusion alarm. ● Entry with the Duress Card, Duress Password, or Duress Fingerprint triggers a duress alarm. ● Unlock duration exceeding the unlock timeout triggers a timeout alarm. ● Swiping an illegal card for more than five times triggers a malicious alarm.

Parameter	Description
Door Sensor Enable	Enables the door sensor. The intrusion alarm and timeout alarm take effect only when door sensor is enabled.
Super Password	Enter the administrator password.
Unlock Length	Sets the duration of door unlocking. The door is automatically locked when the duration is over.
Unlock timeout	Unlock duration exceeding the unlock timeout triggers a timeout alarm.
Unlock Method	You can use any one of the methods, card, fingerprint, and password, or any of their combinations to unlock the door.

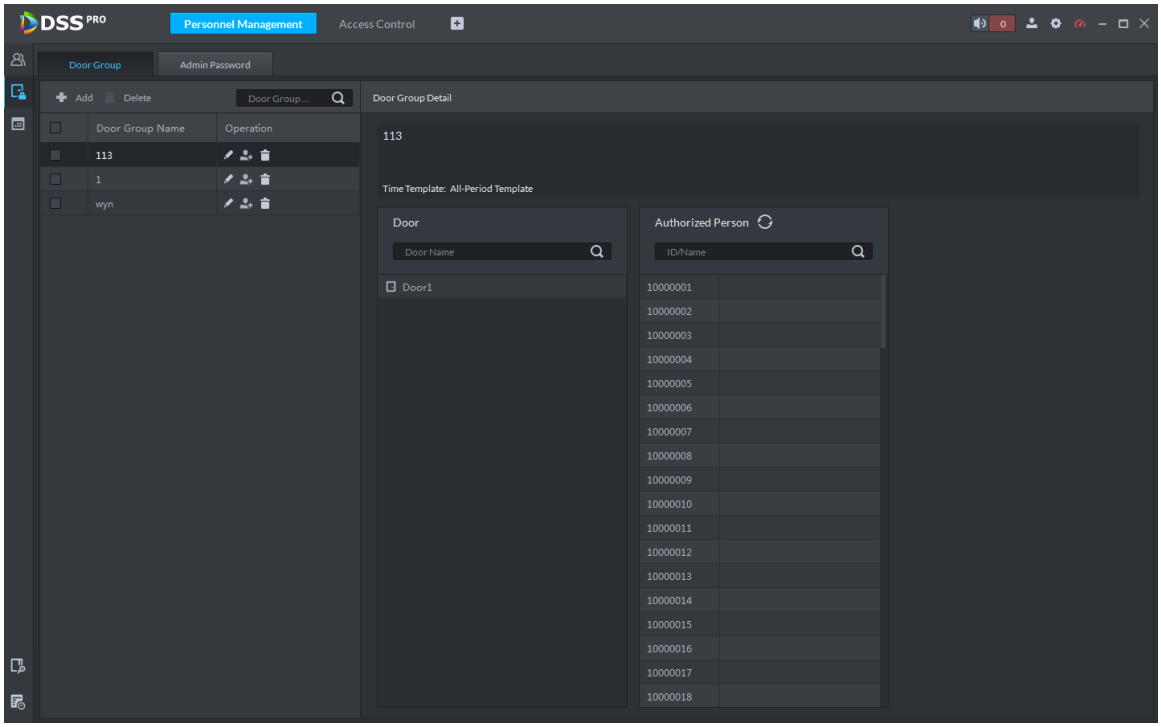
Step 4 Click **OK**.

6.2.2 Creating Door Groups

You can group doors, and then you do not have to give access permission of certain doors to certain users one by one (when creating door rules in the following, you need to select which people have access permission of which door groups).

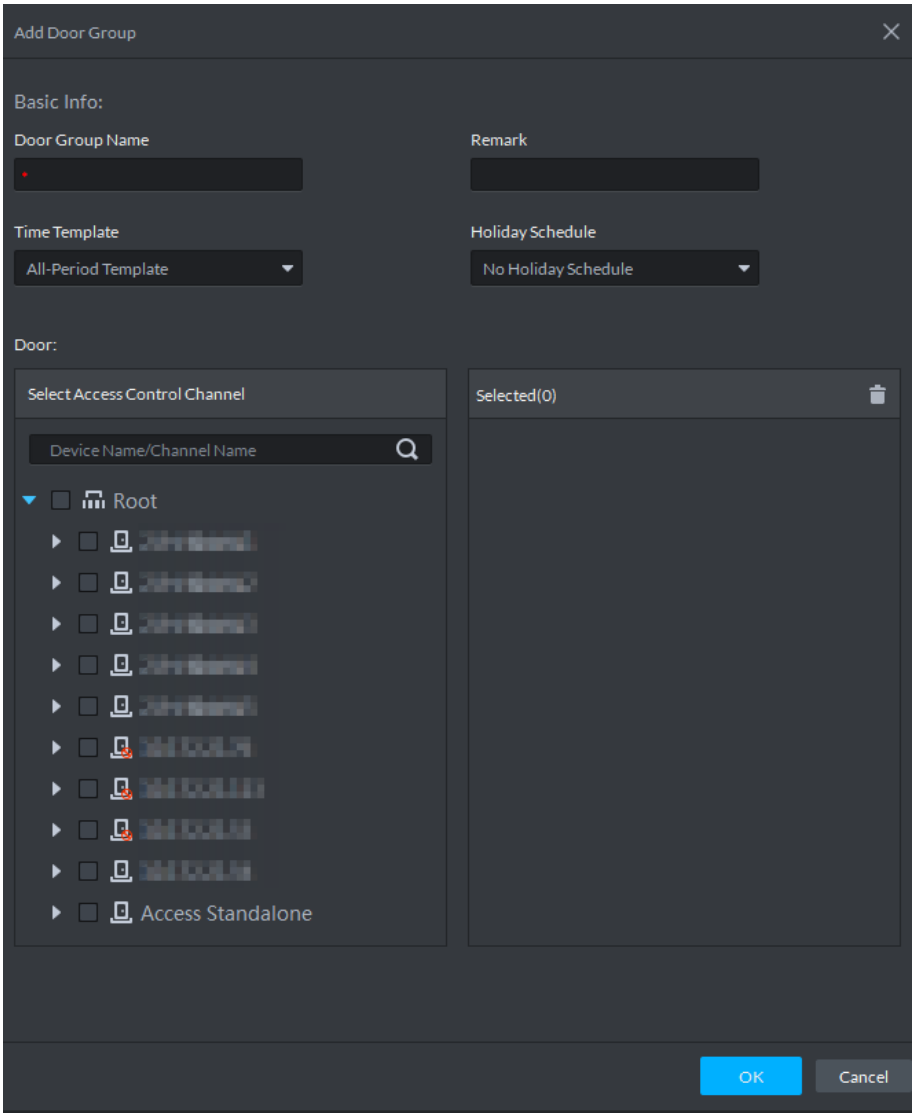
Step 1 Click on the **Personnel Management** interface.

Figure 6-9 Door group



Step 2 Click **Add** on the **Door Group** interface.

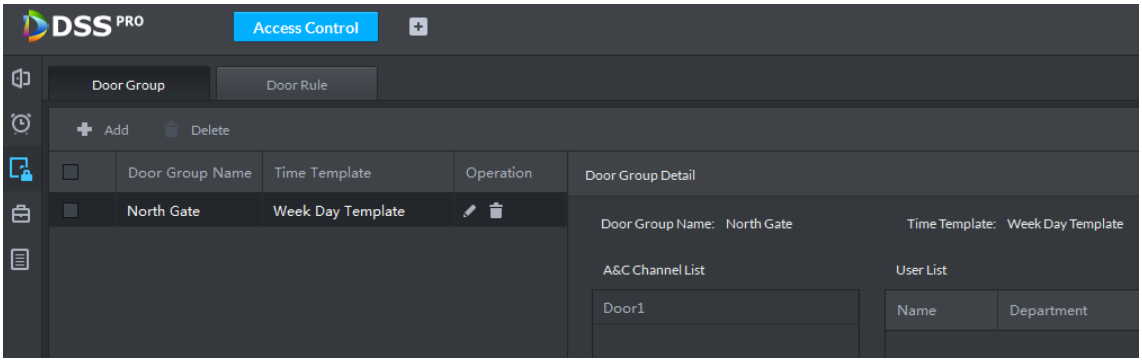
Figure 6-10 Add door group



Step 3 Enter door group name, select a time template, and set the holiday schedule.

Step 4 Select a channel, and Click **OK**.

Figure 6-11 Door group

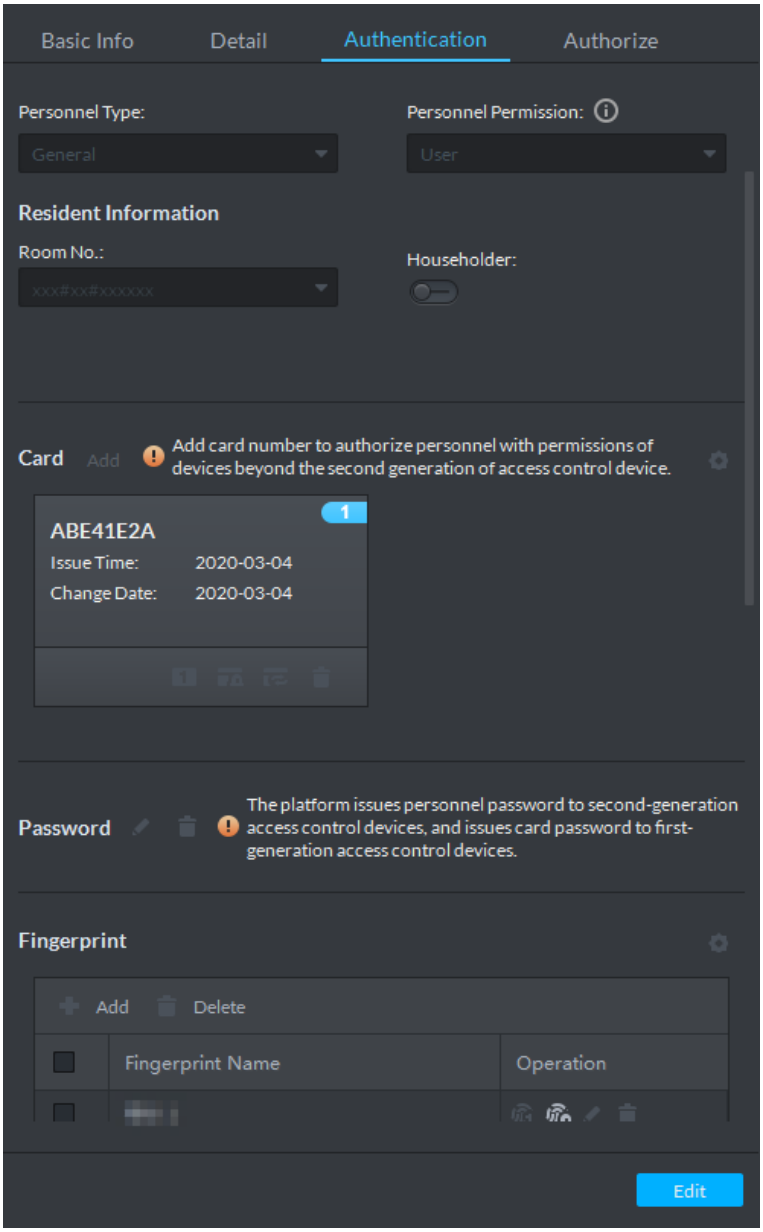


6.2.3 Issuing Access Cards

You can issue access cards to people one by one or in batches.

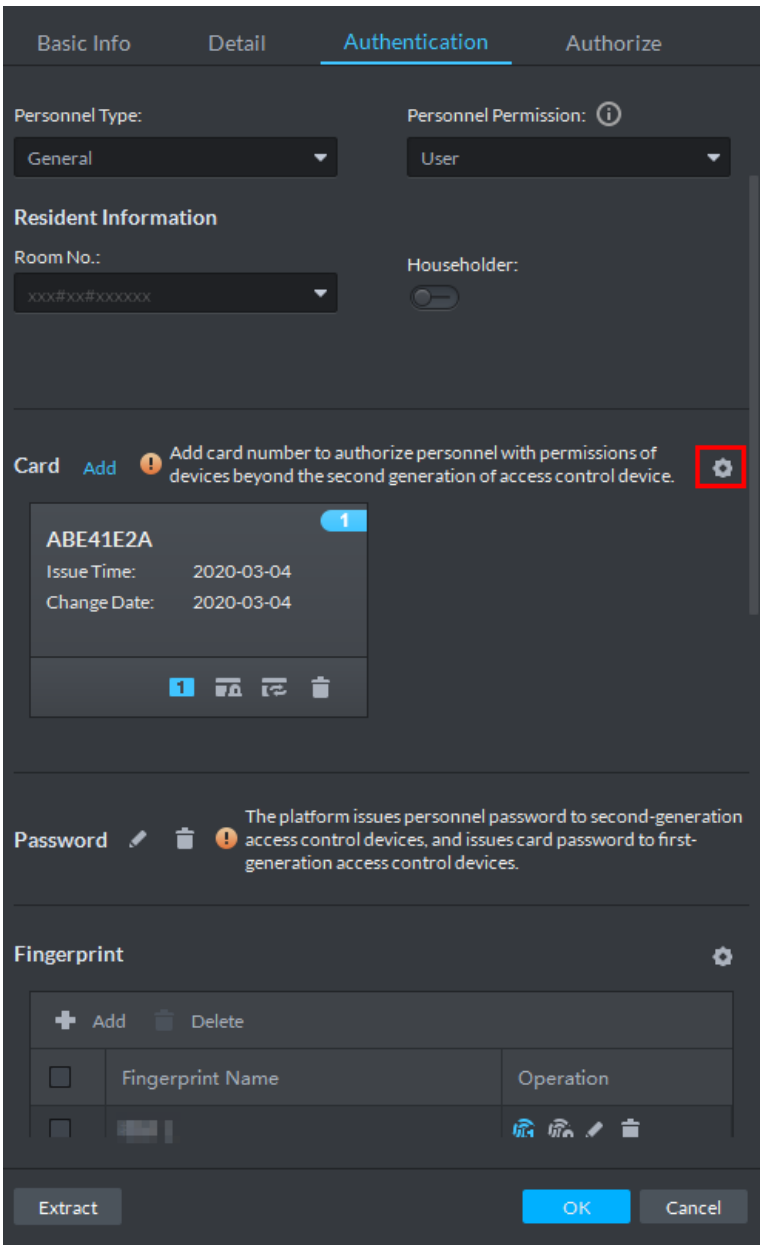
Step 1 On the **Personnel Management** interface, double-click any people you need to issue access card to, and then click **Authentication** tab.

Figure 6-12 Authentication



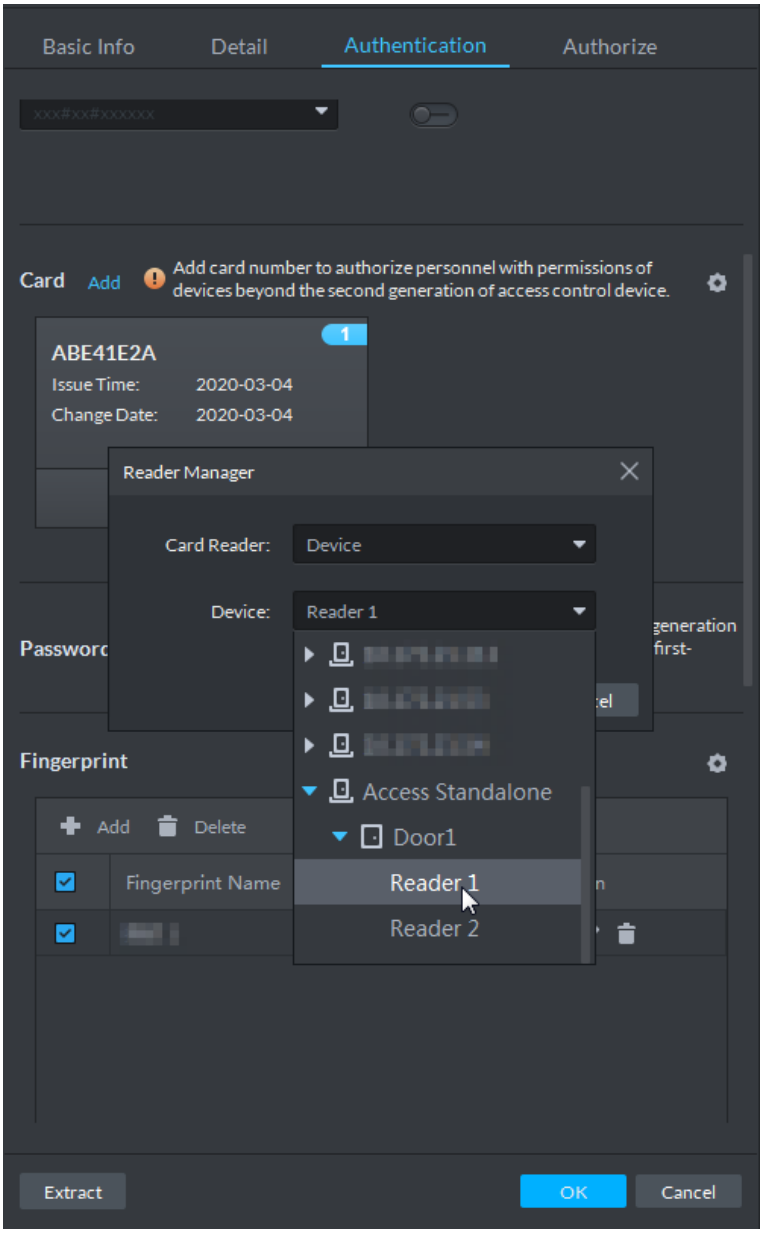
Step 2 Click **Edit**, and then click in **Card** section.

Figure 6-13 Editing



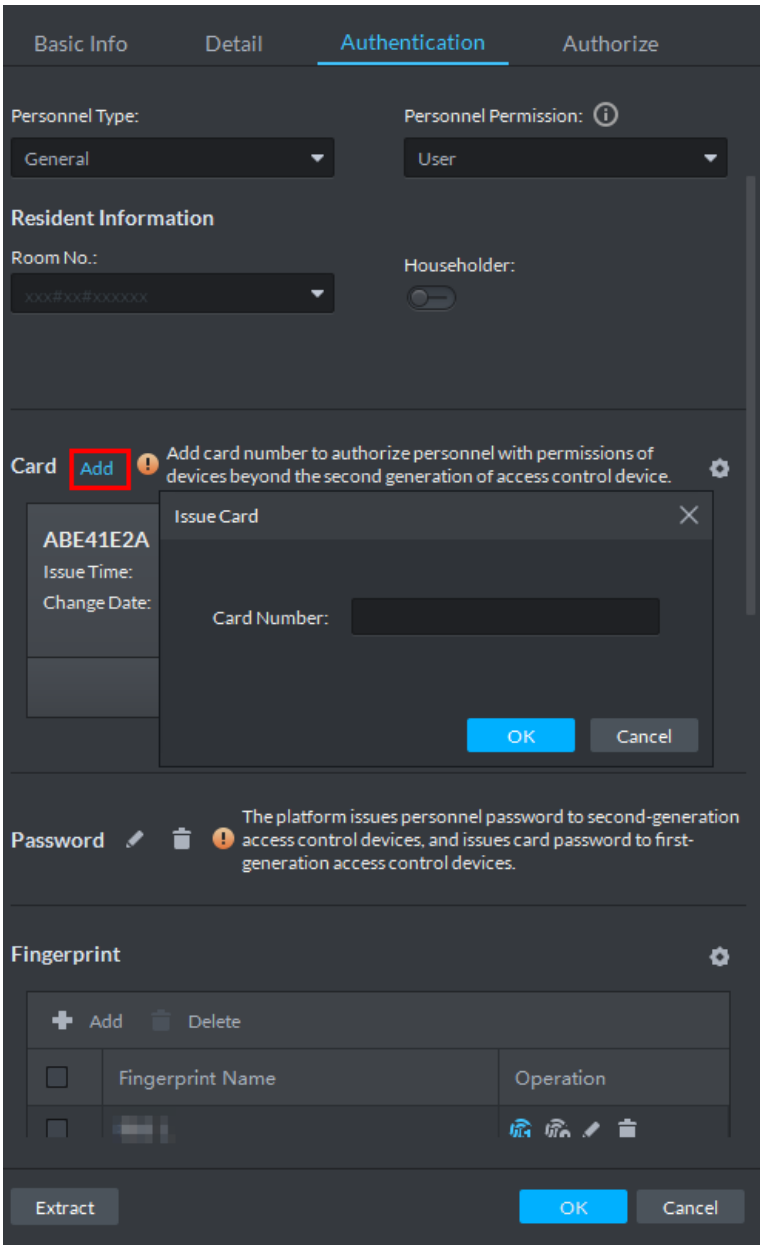
Step 3 Select the card reader of the access standalone as needed.

Figure 6-14 Reader manager



Step 4 Click **Add** next to **Card**, and then put the card to the card reader to issue card. The card number is displayed.

Figure 6-15 Card number



Step 5 Click **OK**.

The card is issued to the people you selected.

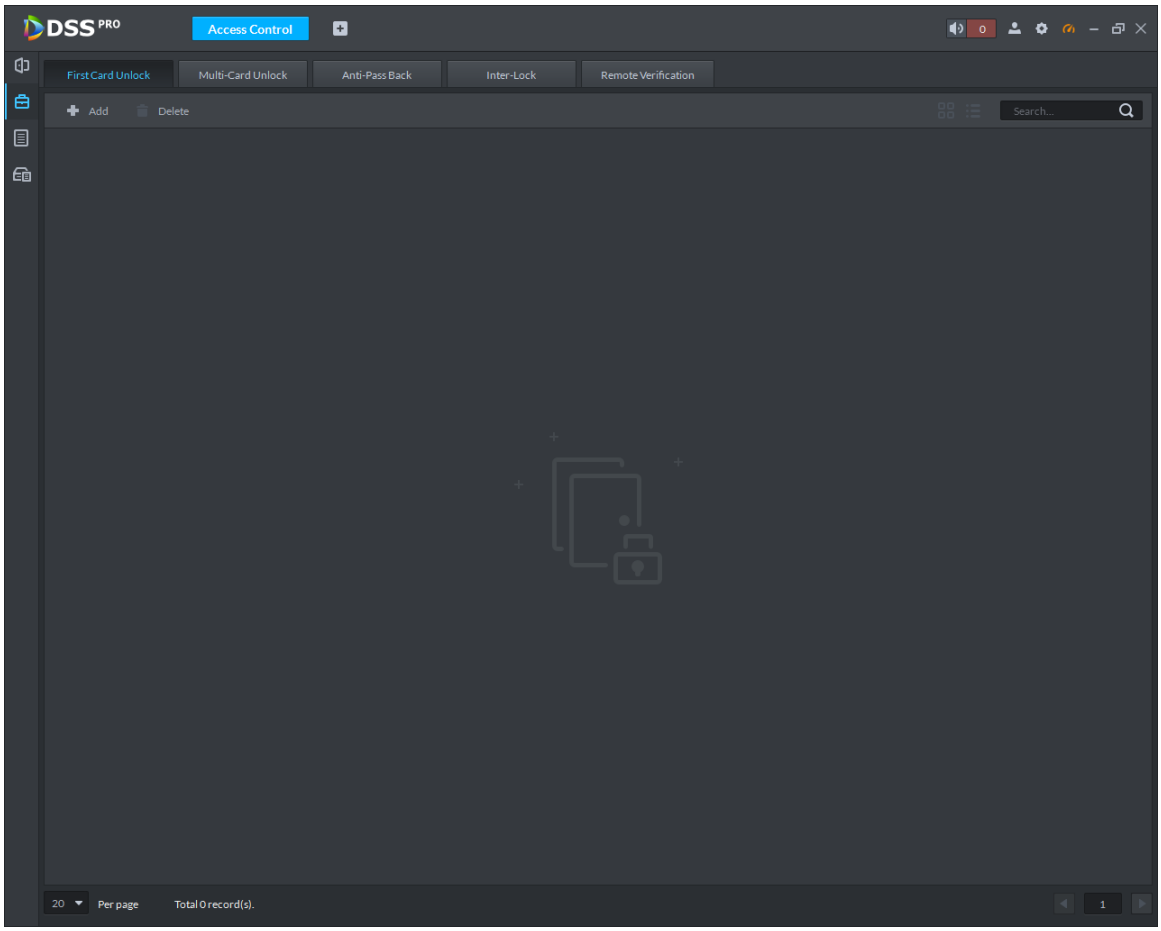
- You can also issue cards in batches by clicking **Batch Issue Card**.
- You can refer to steps of issuing cards to record fingerprints.

6.2.4 First Card Unlock

Only after the specified first-card user swipes the card every day can other users unlock the door with their cards. You can set up multiple first cards. Only after any one of the users swipes the first card can other users without first cards unlock the door with their cards.

Step 1 On the **Access Control** interface, click .

Figure 6-16 Advanced function

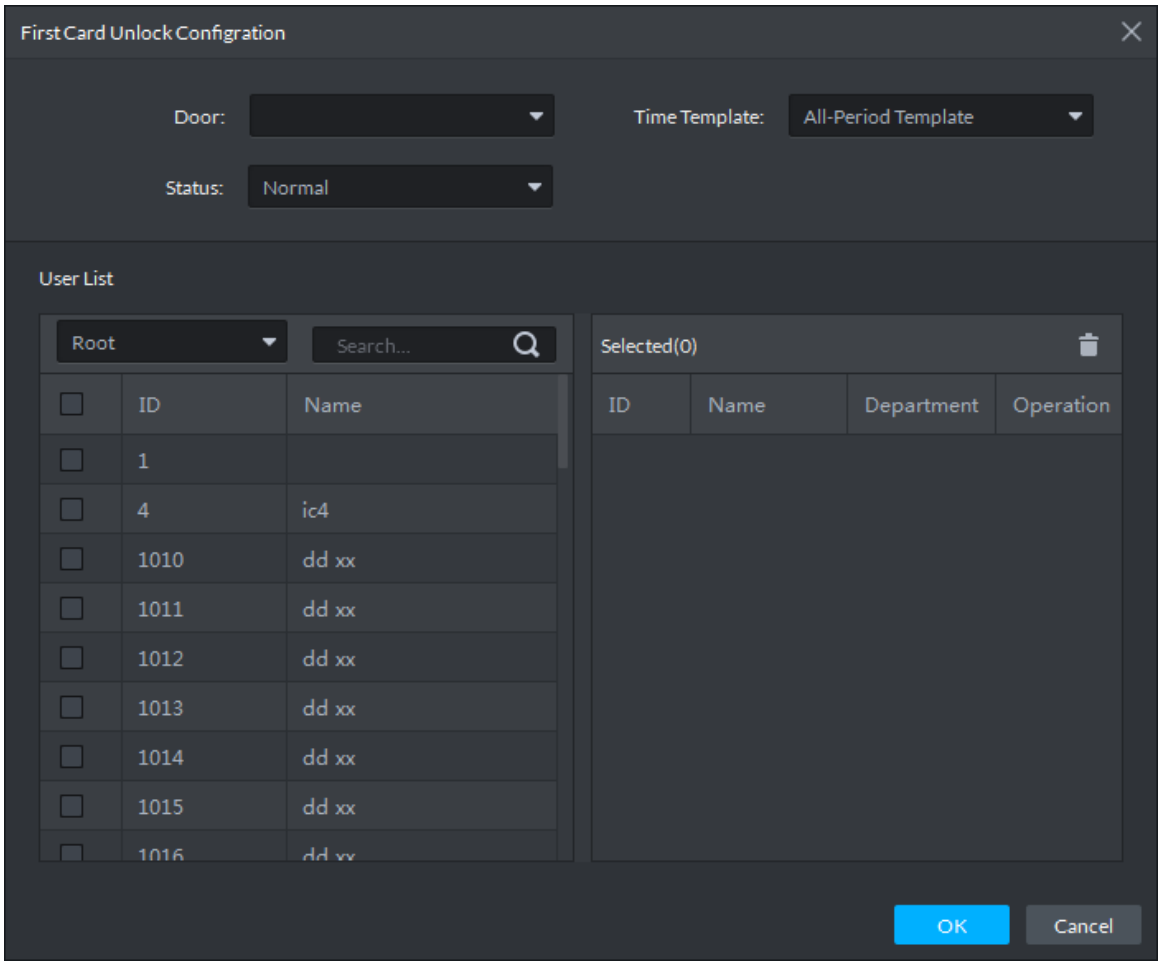


Step 2 Click the **First Card Unlock** tab.

The **First Card Unlock** interface is displayed.

Step 3 Click **Add**.

Figure 6-17 First card unlock configuration

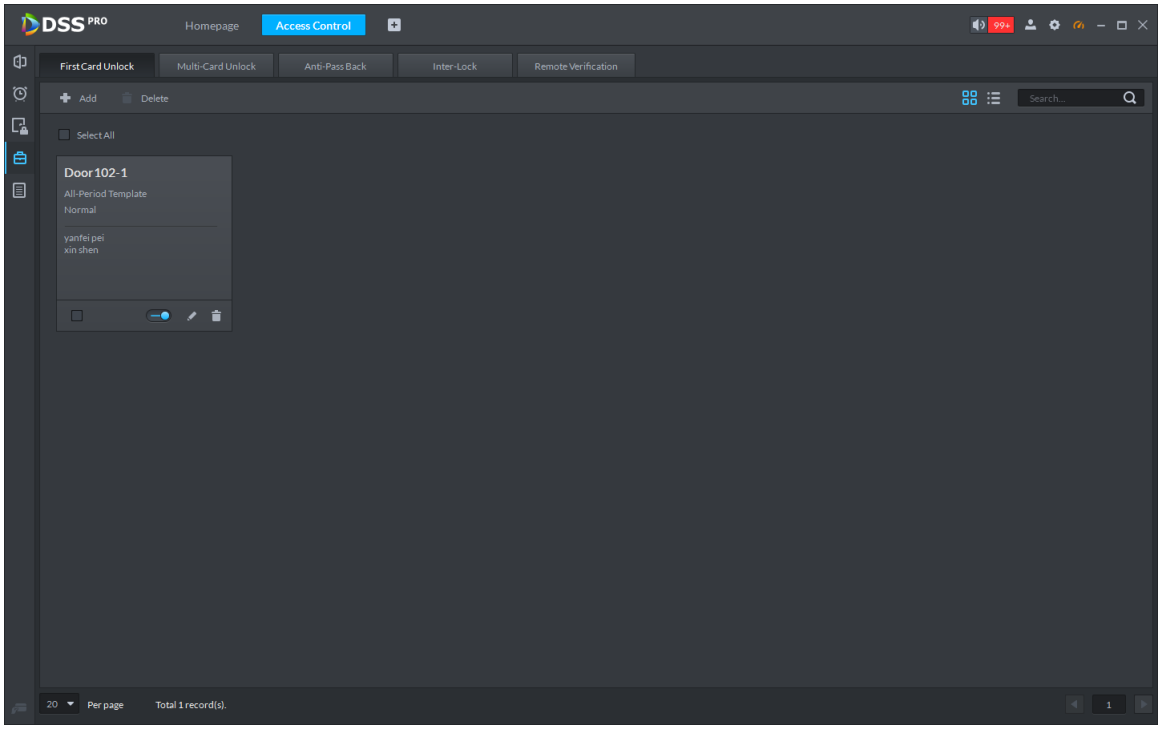


Step 4 Configure the **First Card Unlock** parameters and click **OK**. For details, see Table 6-2. The system displays the **First Card Unlock** information. See Figure 6-18. **First Card Unlock** is enabled by default.

Table 6-2 First card unlock parameters

Parameter	Description
Door	You can select the target access control channel to configure the first card unlock.
Time Template	First Card Unlock is valid in the time period of the selected time template.
Status	After First Card Unlock is enabled, the door is in either the Normal mode or Always Open mode.
User	You can select the user to hold the first card. Supports selecting a number of users to hold first cards. Any one of them swiping the first card means first card unlock is done.

Figure 6-18 First card unlock information



Step 5 Click .

The icon changing into indicates First Card Unlock is enabled.

6.2.5 Multi-Card Unlock

In this mode, multiple groups of users have to swipe cards for an access control channel in an established sequence to unlock the door.

- One group can have up to 50 users.
- With Multi-Card Unlock enabled for an access control channel, it supports up to four groups of users being on site at the same time for verification. The total number of users can be 64 at most, with up to five valid users.

Step 1 On the **Access Control** interface, click .

The **Advanced Function** interface is displayed.

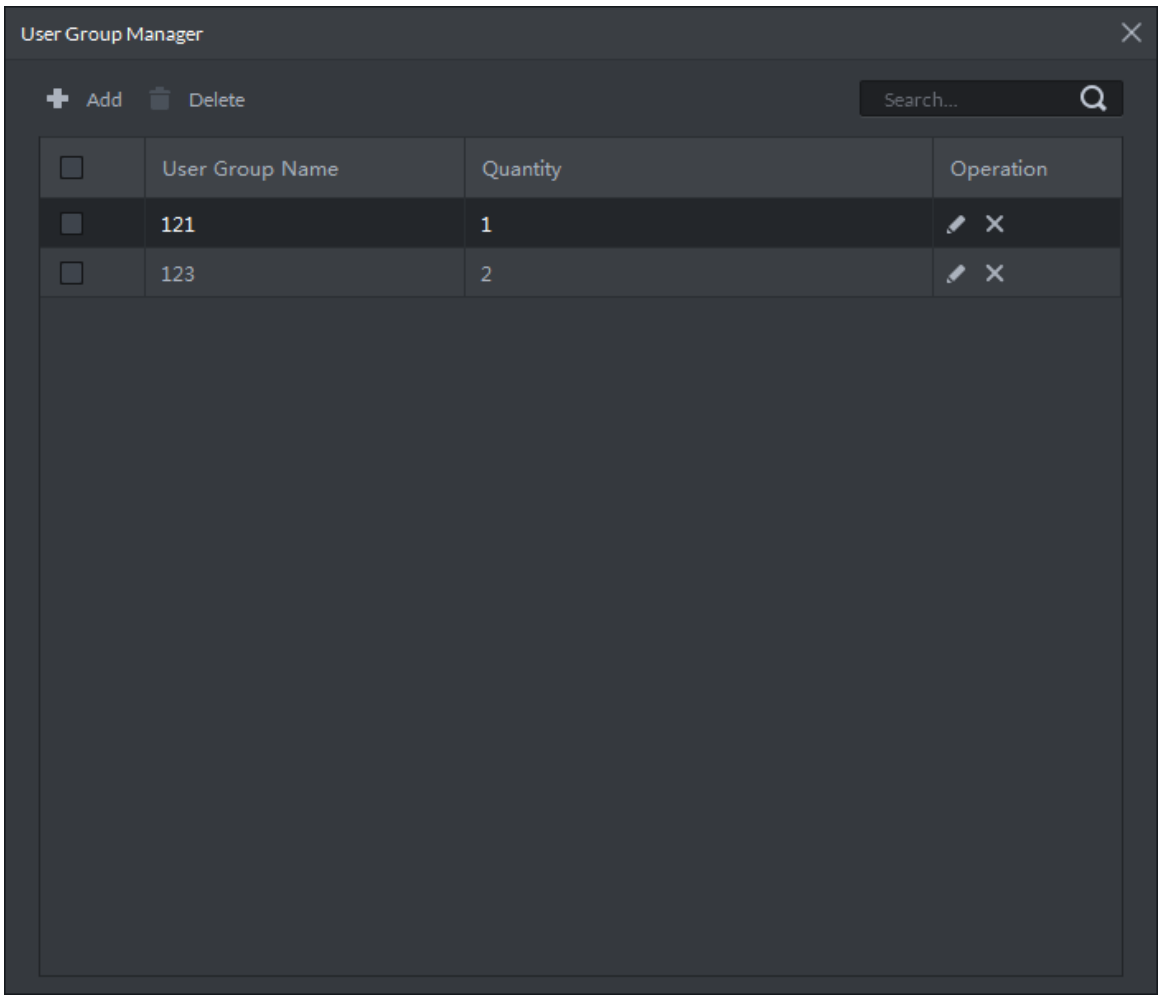
Step 2 Click the **Multi-Card Unlock** tab.

The **Multi-Card Unlock** interface is displayed.

Step 3 Add user group.

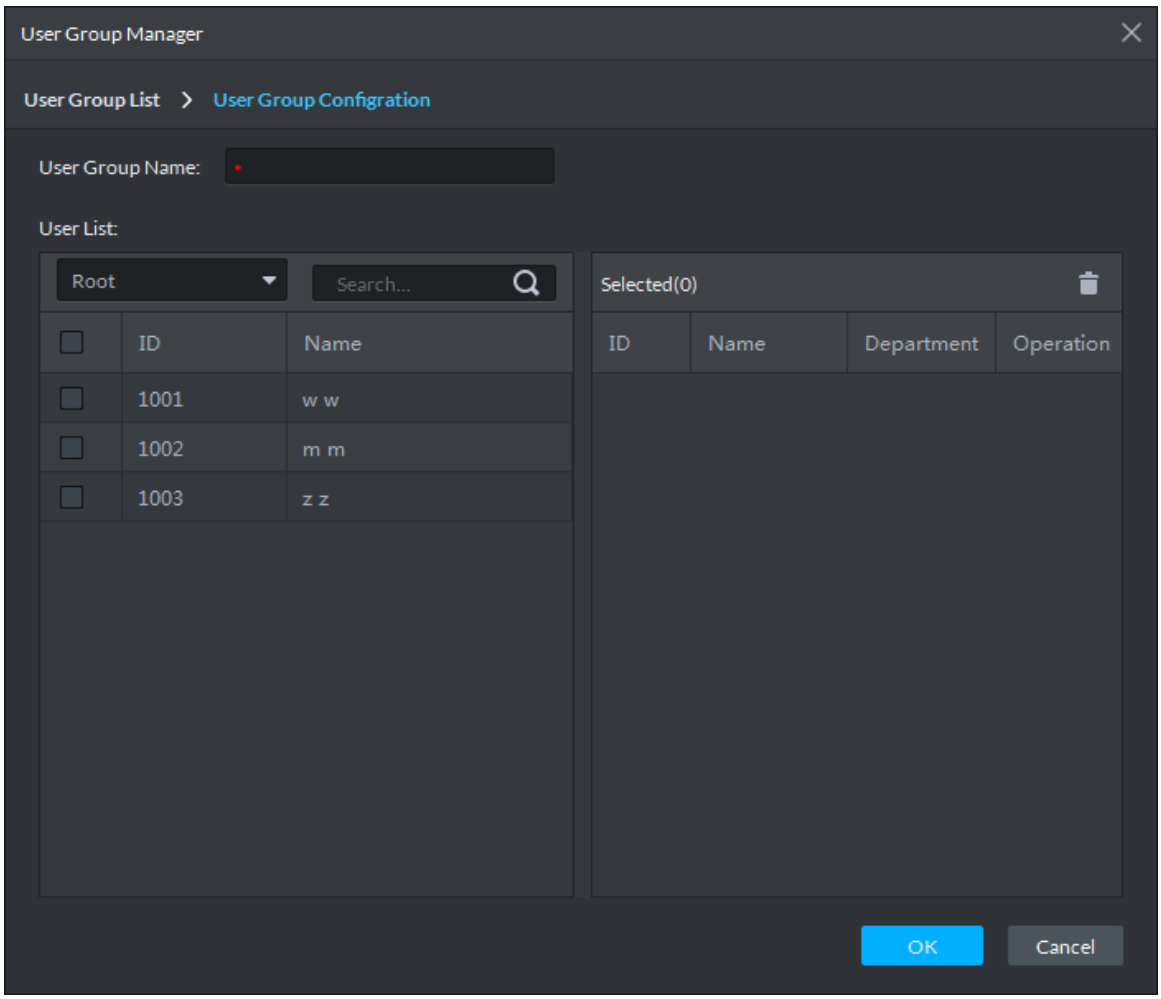
1) Click **Person Group**.

Figure 6-19 User group manager



2) Click **Add**.

Figure 6-20 User group configuration

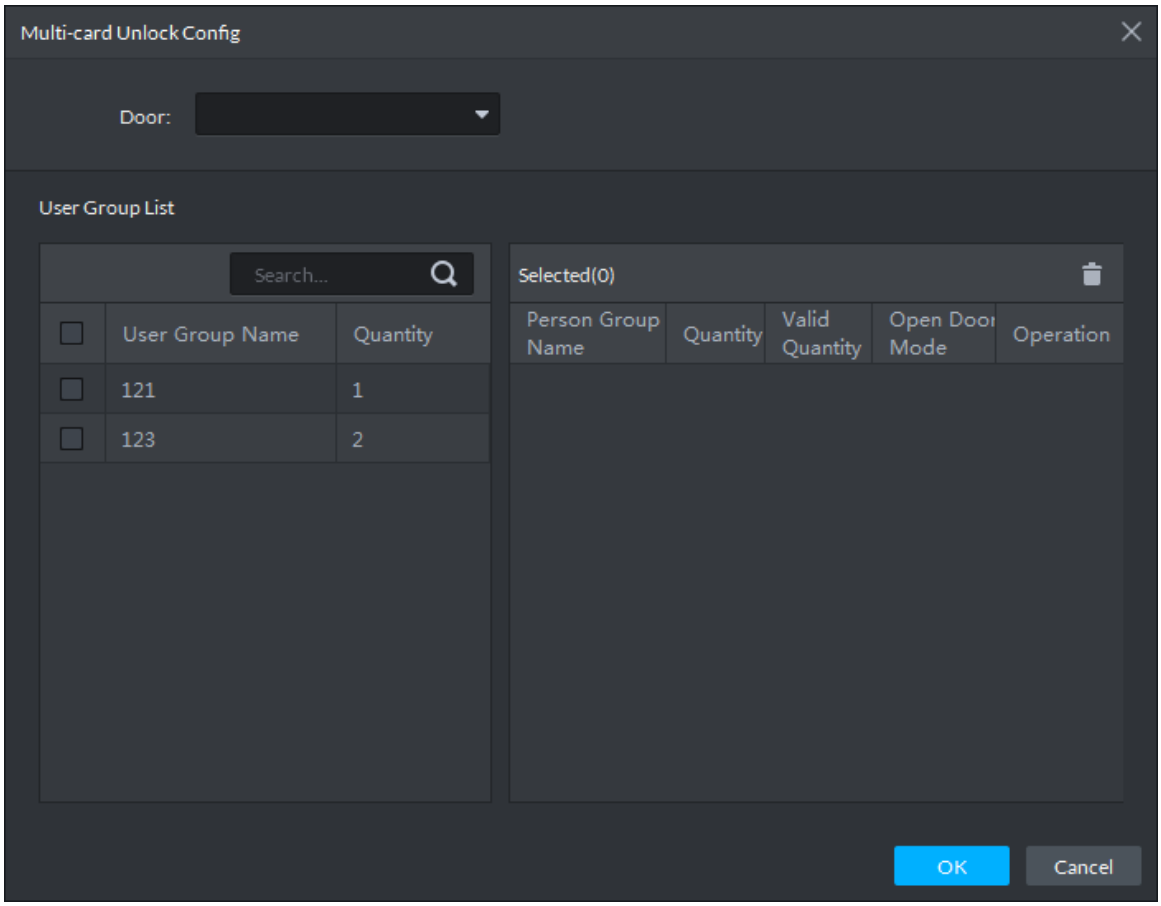


3) Set up **User Group Name**. Select users from **User List** and click **OK**. You can select up to 64 users.
   The system displays the user group information.
4) Click ☒ in the upper right corner of the **User Group Manager** interface.

Step 4 Configure Multi-Card Unlock.

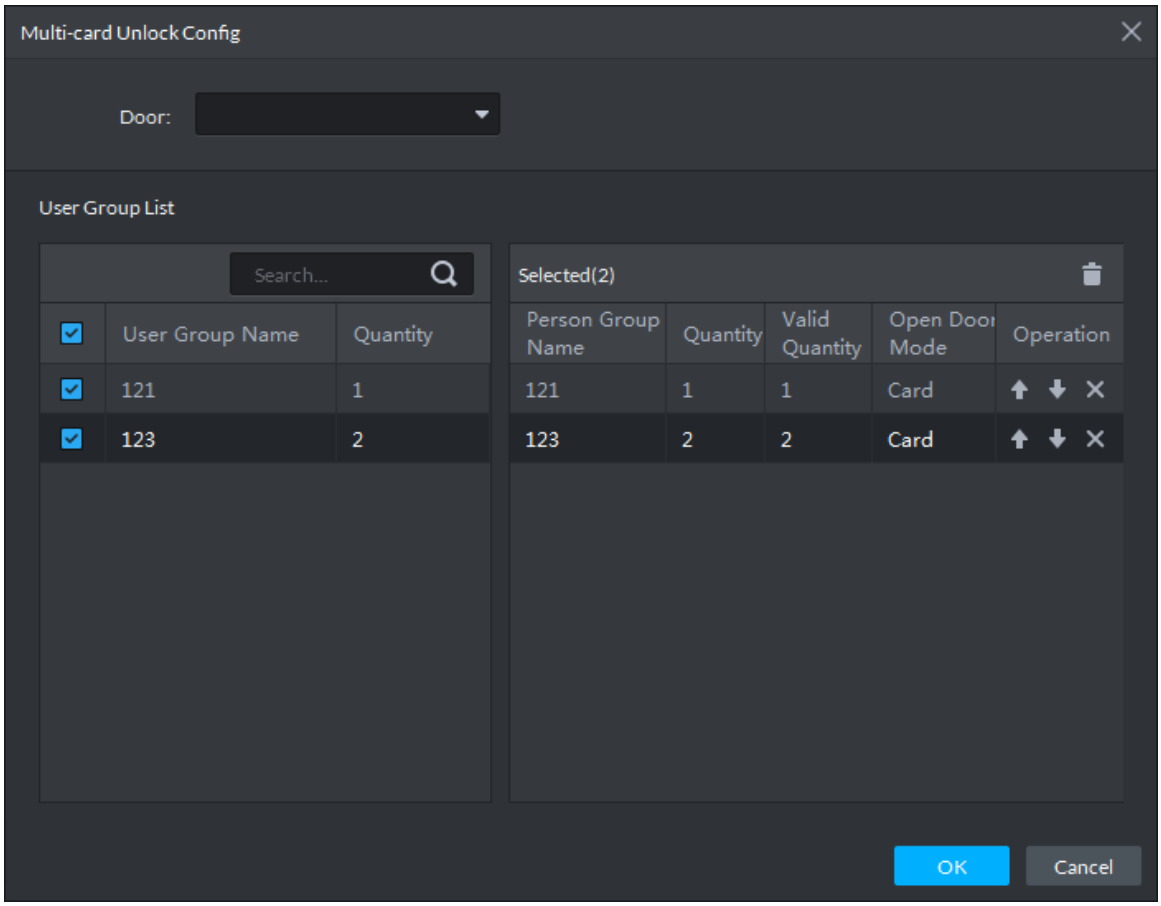
1) Click **Add**.

Figure 6-21 Multi-card unlock configuration



2) Select the door to configure Multi-Card Unlock.
3) Select the user group. You can select up to four groups.
   The system displays the user group information.

Figure 6-22 User group information



4) Enter the **Valid Quantity** for each group to be on site and the **Open Door Mode**.

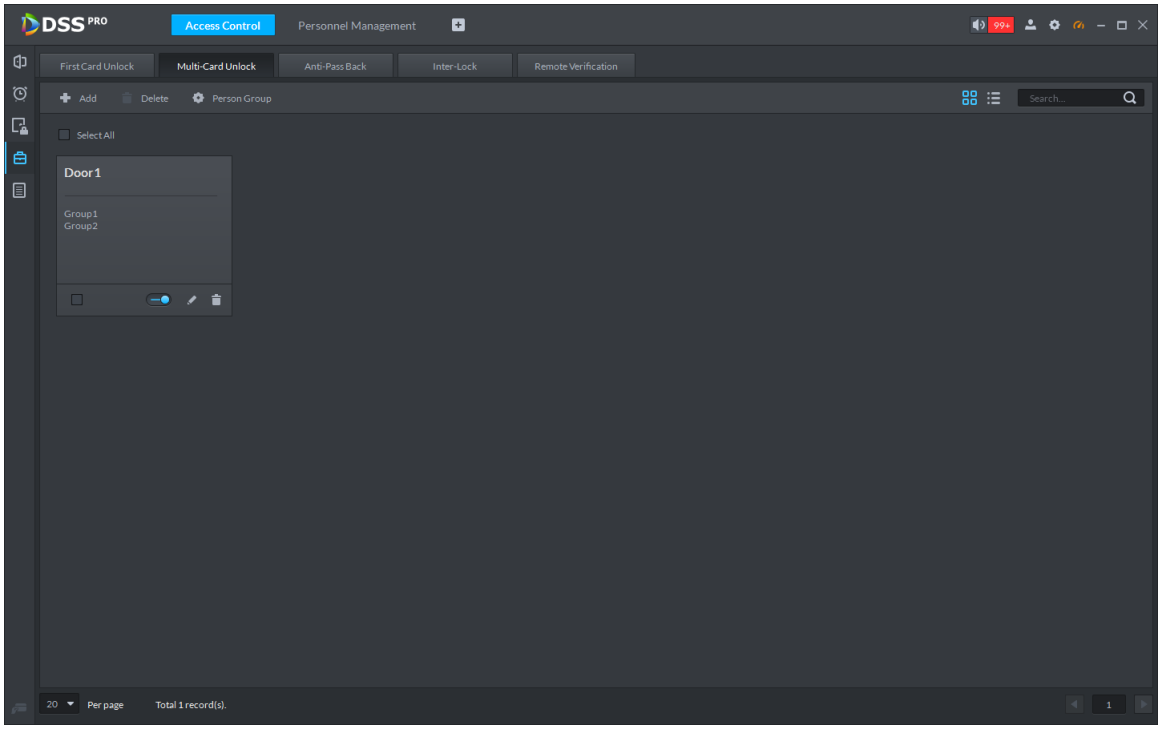
   Click or to adjust the user sequence for each group to unlock the door.

   The valid quantity refers to the number of users in each group that must be on site to swipe their cards.

5) Click **OK**.

   The system displays the **Multi-Card Unlock** information.

Figure 6-23 Multi-card unlock details



Step 5 Click .

The icon changing into indicates Multi-Card Unlock is enabled.

6.2.6 Anti-passback

The Anti-passback feature requires a person to exit from the door that he or she came in from. For the same person, an entry record must pair with an exit record. If someone has entered by tailing someone else, which means there is no entry record, this person cannot unlock the door for exit.

Step 1 On the **Access Control** interface, click .

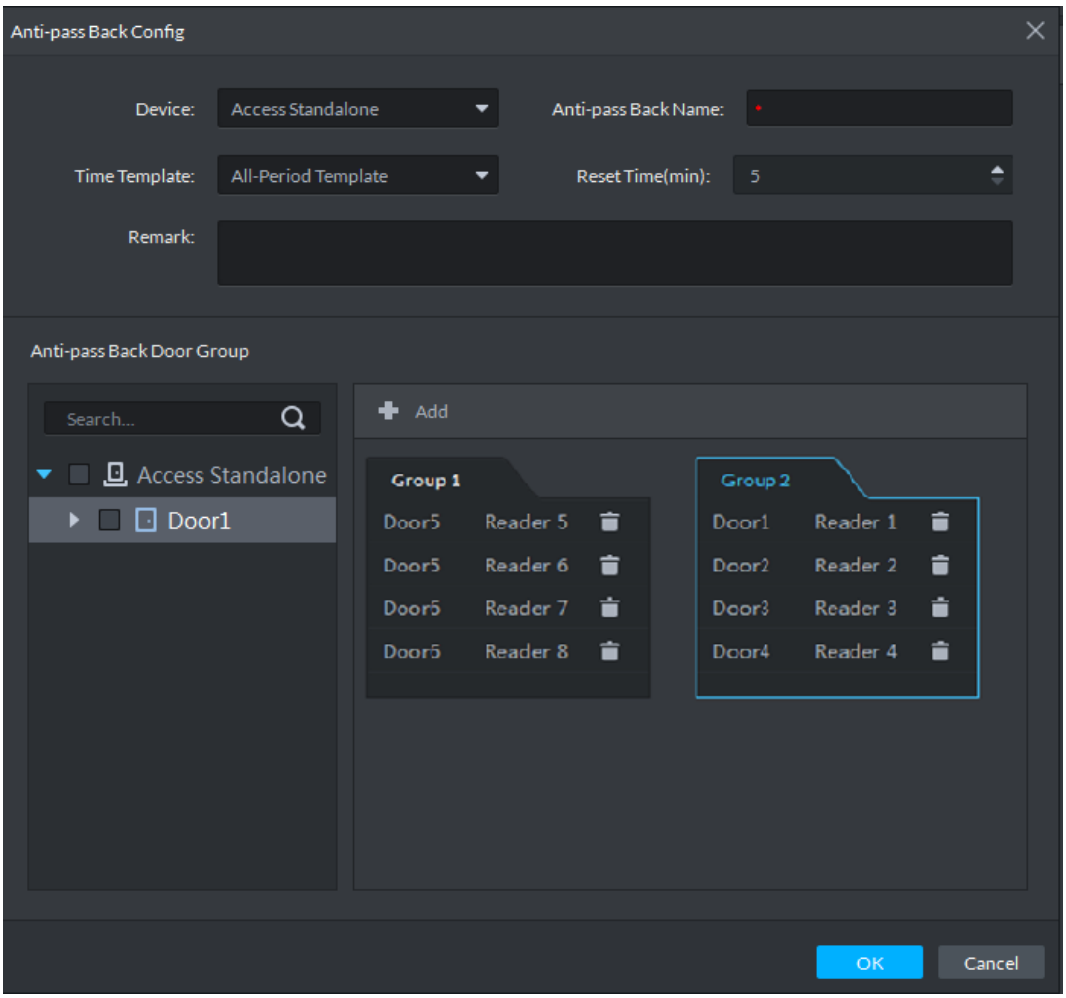
The **Advanced Function** interface is displayed.

Step 2 Click the **Anti-passback** tab.

The **Anti-passback** interface is displayed.

Step 3 Click **Add**.

Figure 6-24 Anti-passback configuration

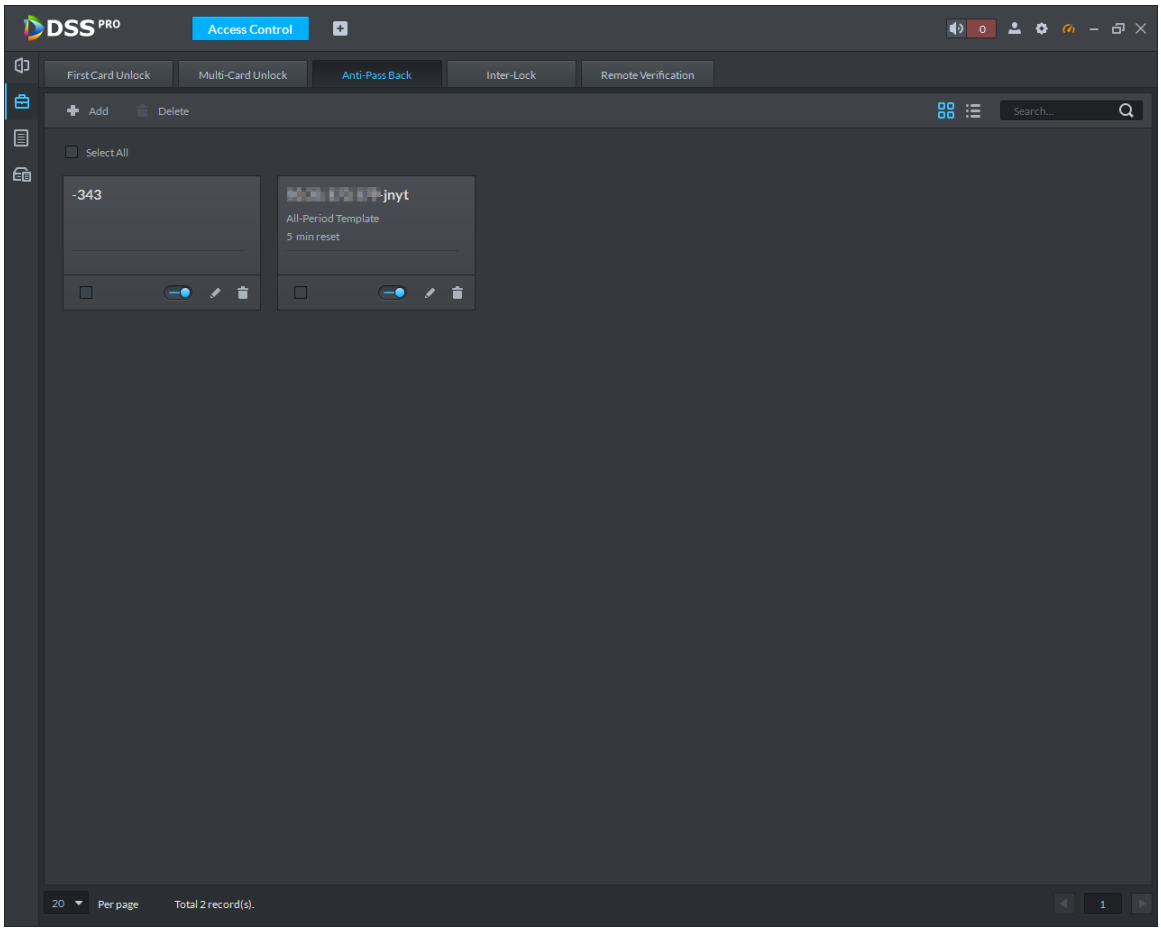


Step 4 Configure the anti-passback parameters and click **OK**. For details, see Table 6-3.
The system displays the user selection information. See Figure 6-25.

Table 6-3 User selection information description

Parameter	Description	
Device	You can select the device to configure the anti-passback rules.	
Anti-passback name	You can customize the name of an anti-passback rule.	
Reset Time(min)	The access card becomes invalid if an anti-passback rule is violated. The reset time is the invalidity duration.	When the selected device is a multi-door controller, you must set up these parameters.
Time Template	You can select the time periods to implement the anti-passback rules.	
Remark	Description information.	
Group X	The group sequence here is the sequence for swiping cards. You can add up to 16 readers for each group. Each group can swipe cards on any of the readers. X is a number.	

Figure 6-25 Anti-passback information



Step 5 Click .

The icon changing into indicates Anti-passback is enabled.

6.2.7 Remote Verification

For devices with remote verification, when users unlock the doors with card, fingerprint, or password in the specified time period, it must be confirmed on the platform client before the access controller can be opened.

Step 1 On the **Access Control** interface, click .

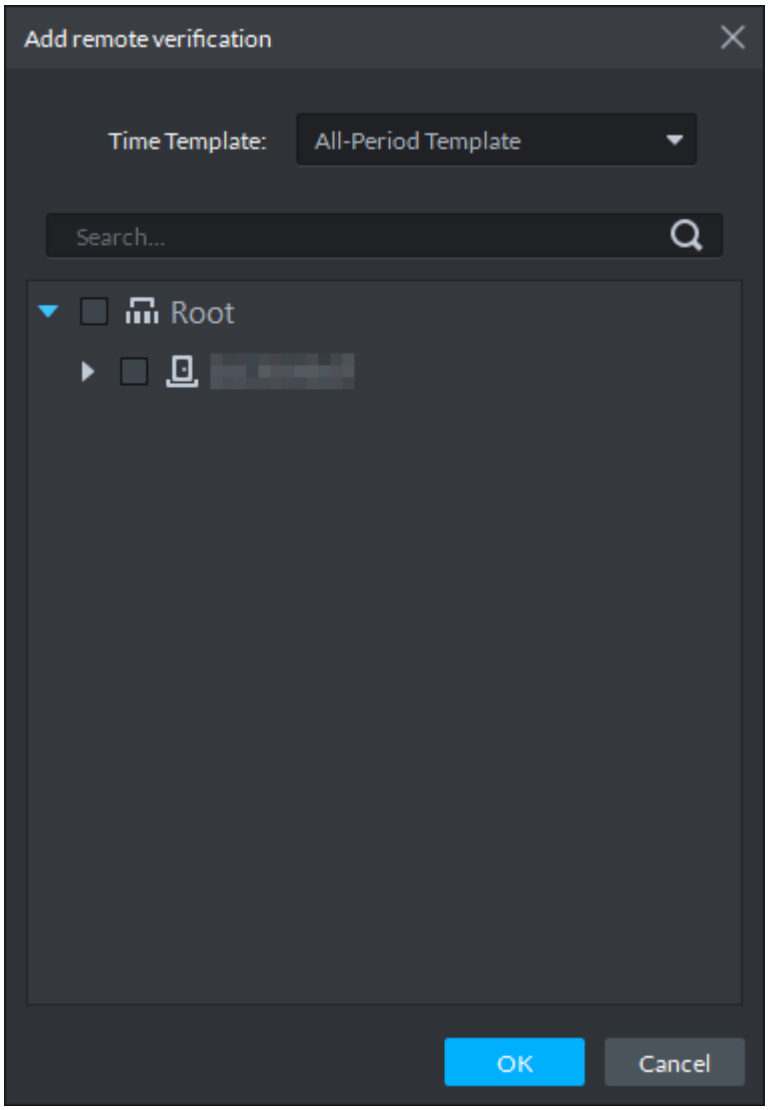
The **Advanced Function** interface is displayed.

Step 2 Click the **Remote Verification** tab.

The **Remote Verification** interface is displayed.

Step 3 Click **Add**.

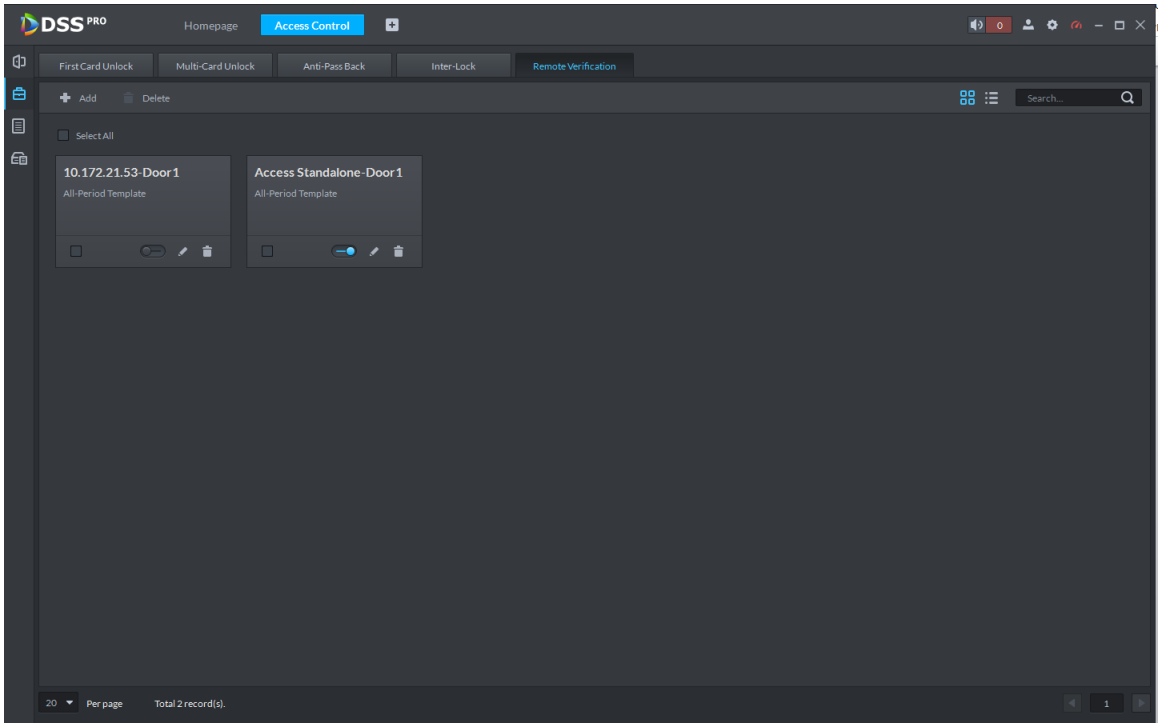
Figure 6-26 Add remote verification



Step 4 Select **Time Template** and access control channel, and click **OK**.

The system displays the remote verification information.

Figure 6-27 Remote verification information



Step 5 Click .

The icon changing into indicates **Remote Verification** is enabled.

6.2.8 Viewing Access Control Records

You can view access control records. There are two types of records:

- Online records

  The access control records stored on the platform.

- Offline records

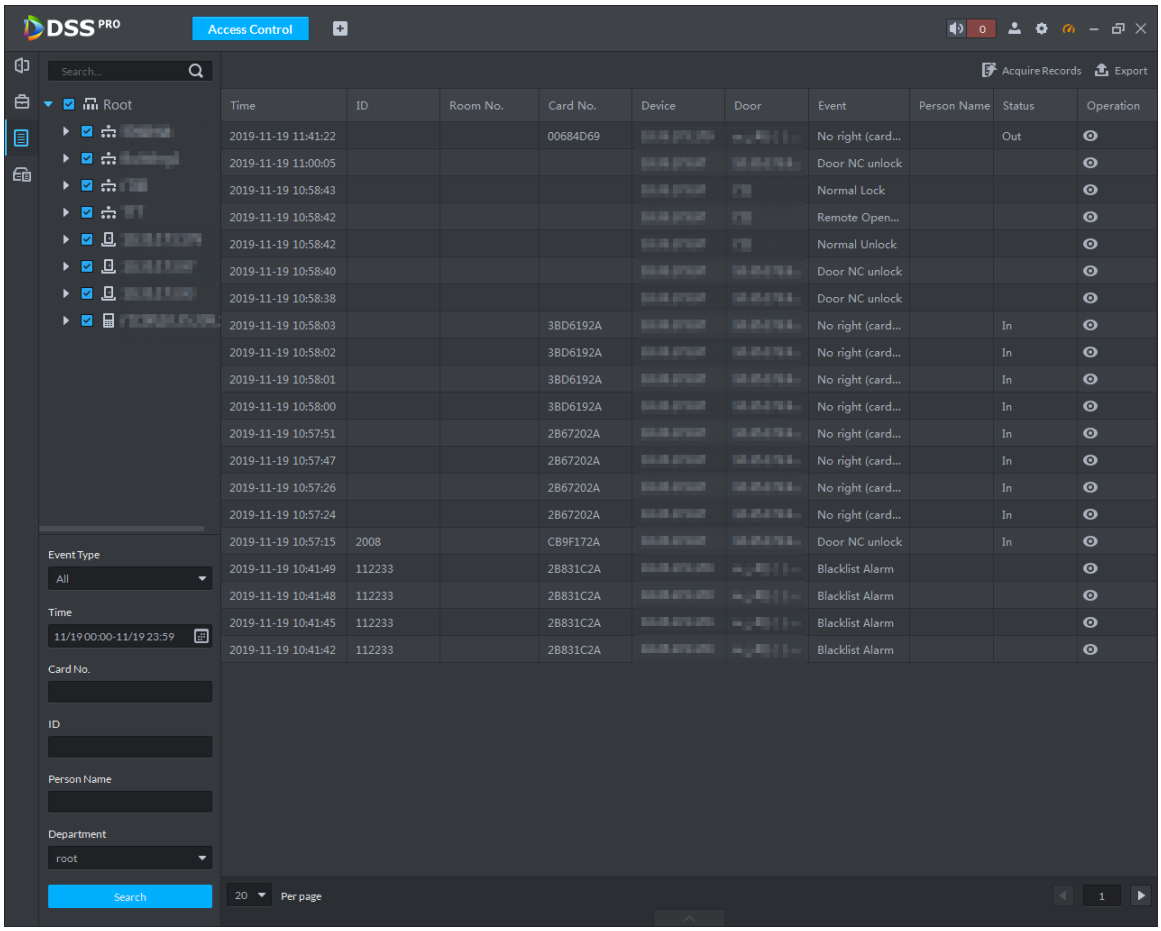
  The access control records stored in the device when it had not been added to the platform or were disconnected from the platform. After the device is added to the platform or reconnects to the platform, the platform will read the records generated when the device was offline.

Configure the alarm in Event manually so that the external alarm can be uploaded to the platform.

6.2.8.1 Online Records

Go to the **Access Control** module from the **Homepage** on the platform client, and click to go to the access control records search interface. See Figure 6-28. Click **Export** in the upper-right corner of the interface and save the exported log to a local disk.

Figure 6-28 Log search



6.2.8.2 Offline Records

You can extract unlock records and alarm records separately.

Step 1 On **Access Control** interface, click .

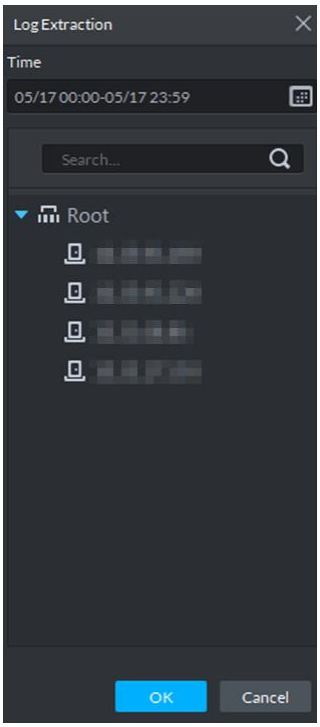
The **Access Control Records** interface is displayed.

Step 2 Click Acquire Records at the upper-right corner.

The **Password Verification** interface is displayed.

Step 3 Enter the login password on the **Password Verification** interface. The **Log Extract interface** is displayed.

Figure 6-29 Extract logs during device offline



Step 4 Click and set period.

Step 5 Click to display devices, and then select a channel.

Step 6 Click **OK**.

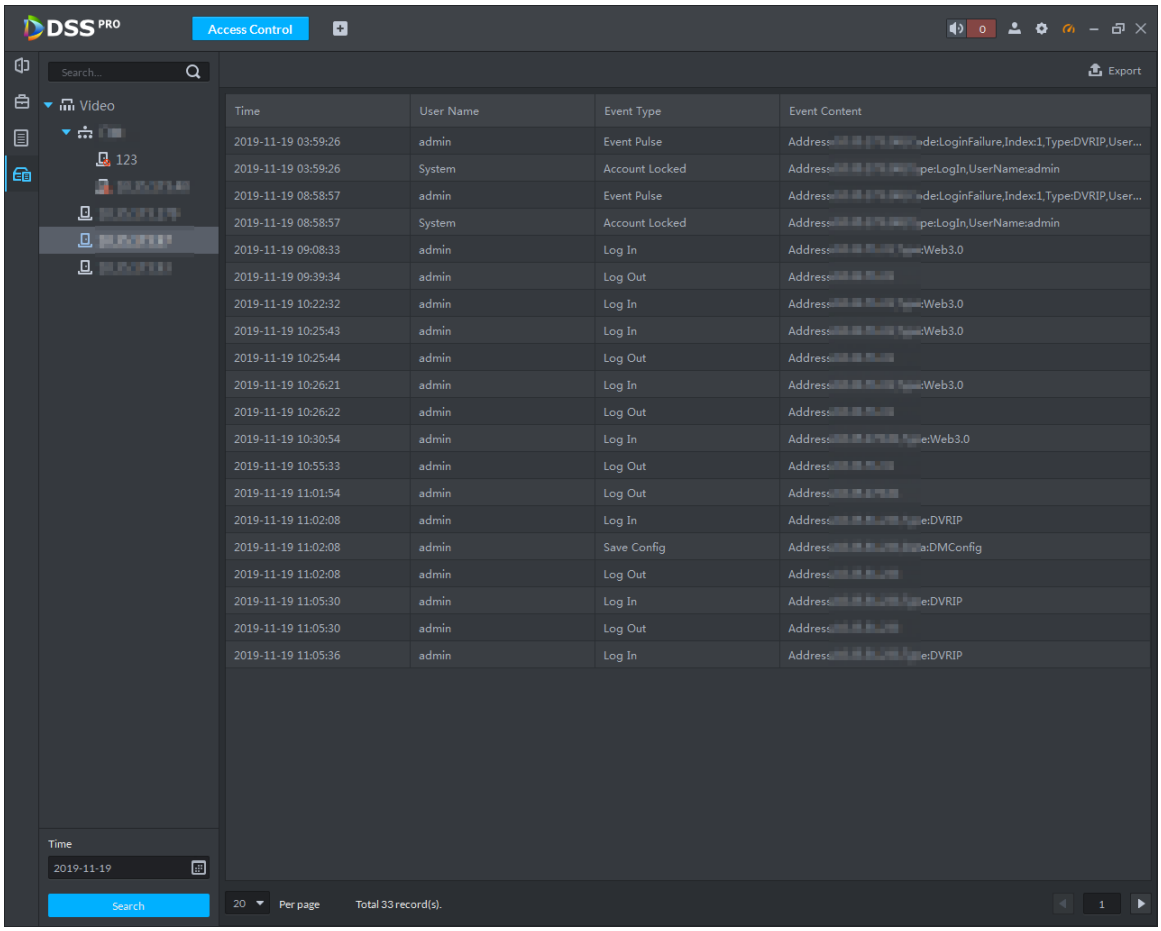
The records are displayed.

6.2.9 Viewing Device Logs

View logs of access control devices, such as login and logout logs.

Step 1 On the **Access Control** interface, click .

Figure 6-30 Device log



Step 2 Select a device and time, and then click **Search**.

The search results are displayed.

Appendix 1 Cybersecurity Recommendations

Cybersecurity is more than just a buzzword: it's something that pertains to every device that is connected to the internet. IP video surveillance is not immune to cyber risks, but taking basic steps toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations on how to create a more secured security system.

Mandatory actions to be taken for basic equipment network security:

1. **Use Strong Passwords**

   Please refer to the following suggestions to set passwords:

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

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

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

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

1. **Physical Protection**

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

2. **Change Passwords Regularly**

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

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

   The equipment 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. **Enable Whitelist**
   We suggest you to enable whitelist function to prevent everyone, except those with specified IP addresses, from accessing the system. Therefore, please be sure to add your computer's IP address and the accompanying equipment's IP address to the whitelist.
8. **MAC Address Binding**
   We recommend you to bind the IP and MAC address of the gateway to the equipment, thus reducing the risk of ARP spoofing.
9. **Assign Accounts and Privileges Reasonably**
   According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.
10. **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.
11. **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.
12. **Secure Auditing**
    - Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
    - Check equipment log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.
13. **Network Log**
    Due to the limited storage capacity of the equipment, the stored log is limited. If you need to save the log for a long time, it is recommended that you enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.
14. **Construct a Safe Network Environment**
    In order to better ensure the safety of equipment and reduce potential cyber risks, we recommend:
    - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
    - The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is

suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.

- Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
- It is recommended that you enable your device's firewall or blacklist and whitelist feature to reduce the risk that your device might be attacked.