Access Standalone

User's Manual

V1.0.2

Foreword

General

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

Safety Instructions

The following signal words might appear in the manual.

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

Revision History

Version	Revision Content	Release Time
V1.0.3	Updated the manual.	January 2023
V1.0.2	Updated the manual.	May 2022
V1.0.1	Updated the card reader configurations.	October 2021
V1.0.0	First release	September 2021

Privacy Protection Notice

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

About the Manual

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

Important Safeguards and Warnings

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

Transportation Requirements

Transport the Device under allowed humidity and temperature conditions.

Storage Requirements

Store the Device under allowed humidity and temperature conditions.

Installation Requirements

WARNING

- Connect the Device 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 Device.
- Do not connect the Device to more than one power supply. Otherwise, the Device might become damaged.

- Observe all safety procedures and wear required protective equipment provided for your use while working at heights.
- Keep the Device on a stable place to prevent it from falling.
- Do not expose the Device to direct sunlight or heat sources.
- Do not install the Device in humid, dusty or smoky places.
- Install the device in a well-ventilated place, and do not block the ventilator of the Device.
- Use the power adapter or case power supply provided by the Device 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 Device label.
- Connect class I electrical appliances to a power socket with protective earthing.

Operating Requirements

- Make sure that the power supply of the Device works properly before use.
- Do not pull out the power cable of the Device while it is powered on.
- Only use the Device within the rated power range.
- Use the Device under allowed humidity and temperature conditions.
- Prevent liquids from splashing or dripping on the Device. Make sure that there are no objects filled with liquid on top of the Device to avoid liquids flowing into it.
- Do not disassemble the Device.

Table of Contents

Foreword ..... **I**
Important Safeguards and Warnings ..... **III**
1 Product Overview **1**
1.1 Introduction 1
1.2 Features 1
1.3 Dimensions 2
1.4 Application 3
2 Local Configuration **4**
2.1 Configuration Process 4
2.2 Keypad Function 4
2.3 Initialization 4
2.4 Standby Screen 5
2.5 Logging in to the Main Menu 6
2.6 Unlocking Methods 7
2.6.1 Card 7
2.6.2 Fingerprint 7
2.6.3 User Password 7
2.6.4 Administrator Password 8
2.7 User Management 8
2.7.1 Adding New User 8
2.7.2 User/Admin List 10
2.7.3 Setting Administrator Password 11
2.8 Access Control Management 11
2.8.1 Configuring Unlocking Mode 12
2.8.2 Configuring Lock Holding Time 12
2.9 Communication 12
2.9.1 Configuring IP 12
2.9.2 Configuring Wi-Fi 13
2.9.3 Configuring Wiegand 14
2.9.4 Configuring Serial Port 14
2.9.5 Configuring Mode 15
2.10 System 16
2.10.1 Time 16
2.10.2 Volume 17
2.10.3 Restoring to Default Settings 17
2.10.4 Restarting the Device 18
2.11 USB Management 18
2.11.1 Exporting to USB 18
2.11.2 Importing From USB 18
2.11.3 Updating System 19
2.11.4 Exporting Unlocking Records 19
2.11.5 Exporting/Importing User Information 20
2.12 System Information 20

3 Web Configuration 21
3.1 Web on Computer 21
3.1.1 Initialization 21
3.1.2 Logging In 22
3.1.3 Resetting the Password 23
3.1.4 Configuring Door Parameter 25
3.1.5 Alarm Linkage 27
3.1.6 Time Section 29
3.1.7 Data Capacity 32
3.1.8 Setting Volume 32
3.1.9 Configuring Network 33
3.1.10 Setting Date 36
3.1.11 Safety Management 37
3.1.12 User Management 44
3.1.13 Maintenance 47
3.1.14 Configuration Management 48
3.1.15 Updating System 50
3.1.16 Version Information 51
3.1.17 Viewing Online User 51
3.1.18 Viewing System Logs 52
3.1.19 Logging Out 53
3.2 Web on Phone 54
4 SmartPSS AC Configuration 55
4.1 Logging in 55
4.2 Adding Devices 55
4.2.1 Adding Individually 55
4.2.2 Adding in Batch 56
4.3 User Management 57
4.3.1 Setting Card Type 57
4.3.2 Adding User 58
4.4 Assigning Permissions 61
Appendix 1 Fingerprint Registration Instructions 63
Appendix 2 Cybersecurity Recommendations 64

1 Product Overview

1.1 Introduction

Integrated with a powerful processor and a deep-learning algorithm, the Device can identify fingerprints instantly and accurately. The Device also supports unlocking the door by cards, passwords, fingerprints, or their combinations. To meet different needs, it also works with a management software to perform more functions.

The fingerprint function is available on select models.

1.2 Features

- LCD display.
- PC + ABS/acrylic panel that is suitable for outdoor use.
- Supports card reader and controller modes to adapt to different situations.
- Supports unlocking the door remotely on SmartPSS AC, or by cards, passwords, fingerprints, or their combinations.
- Supports multiple alarm types, such as duress, intrusion and tamper.
- Supports various types of users, including guest, patrol, blocklist, VIP, normal users, and other user types.
- You can log in to the web browser with a PC or a phone.
- Supports door bell.
- Works with SmartPSS AC and DSS Pro.

1.3 Dimensions

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

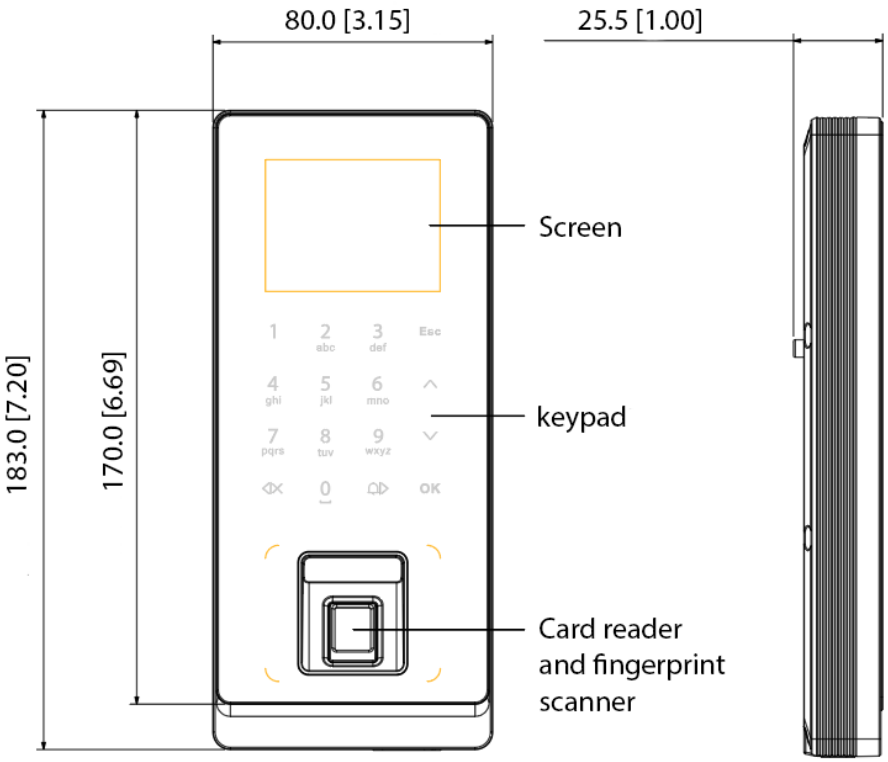
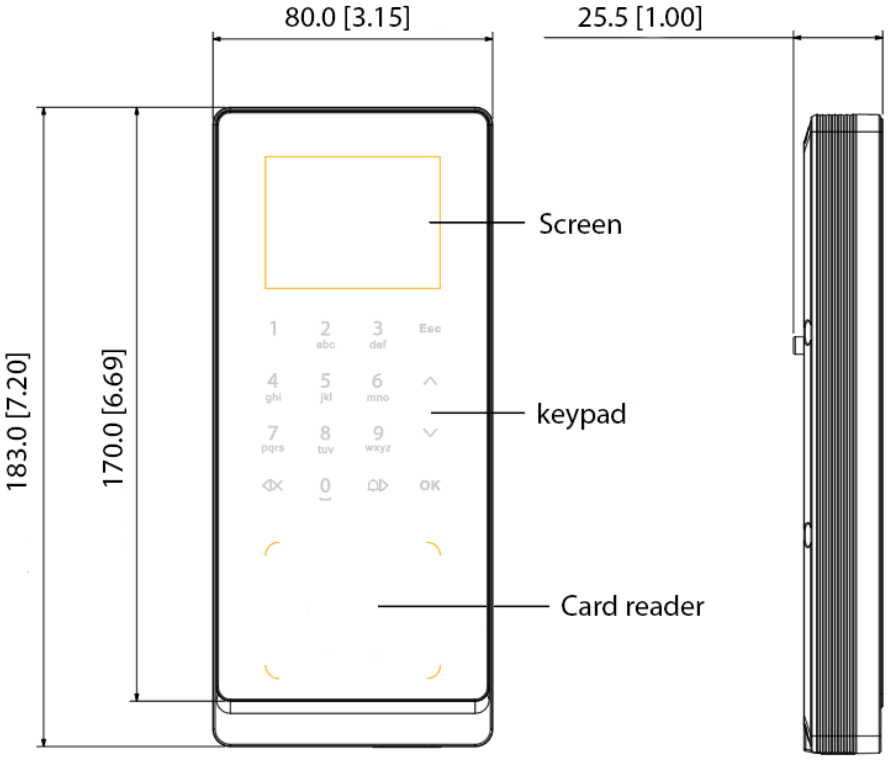


Figure 1-2 Dimensions (2) (mm[inch])

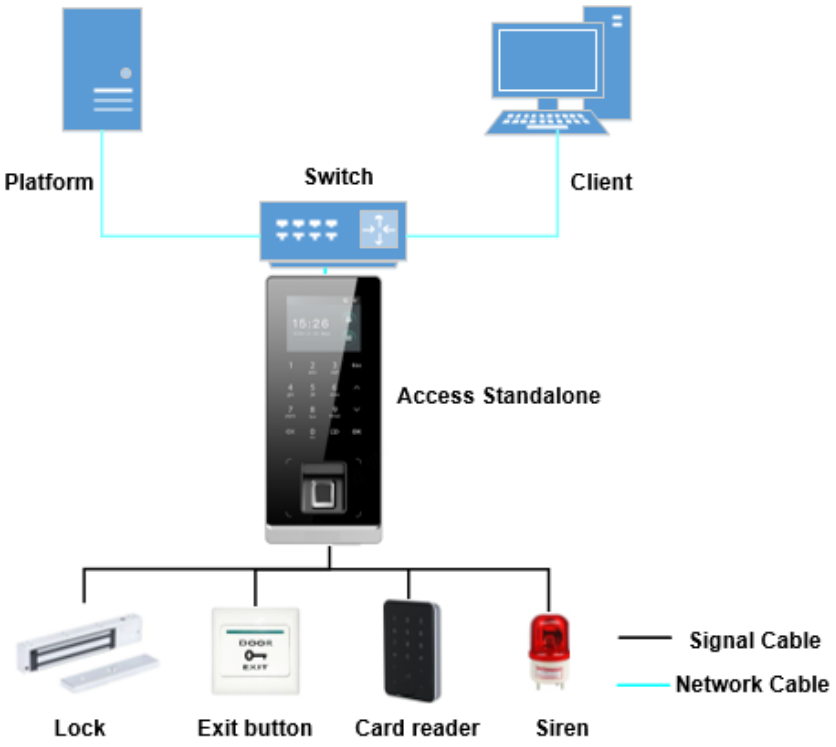


1.4 Application

The Device is applicable to a variety of scenarios, such as office buildings, schools, industrial parks, apartment complexes, factories, public stadiums, and business centers. This user manual mainly describes the Device with the fingerprint function in the controller mode.

The user manual is for reference only, and might differ from the actual product.

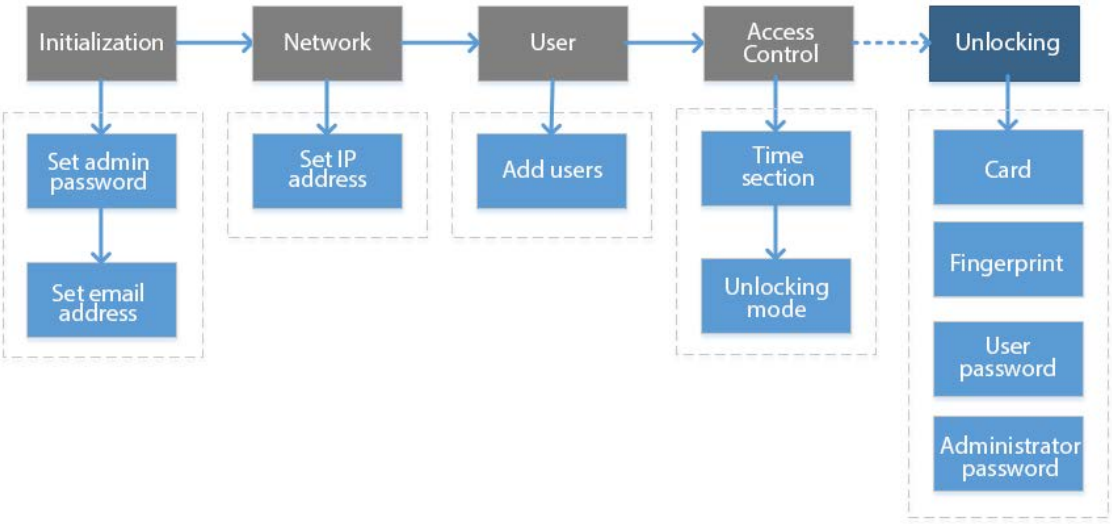
Figure 1-3 Network diagram



2 Local Configuration

2.1 Configuration Process

Figure 2-1 Configuration workflow



2.2 Keypad Function

Table 2-1 Description of keypad

Item	Description
Number or letter	Used to enter information or password.
^	Navigate the page.
v	
Esc	Cancel an operation or go back to the previous page.
OK	Go to the selected page or confirm your change.
	Go to the administrator login page.
	Backspace.
	Ring the bell (only on the standby page), navigate the page, or change the input method.

2.3 Initialization

For first-time use or after restoring factory defaults, you need to set a password and associate your email address for the admin account. You also need to set the time zone of the Device. You can use the admin account to log in to the main menu of the Device, configure the Device, and log in to the web browser and SmartPSS AC.

Figure 2-2 Initialization

- If you forget the administrator password, send a reset request to your associated e-mail address.
- 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.

2.4 Standby Screen

You can unlock the door on the standby page with your card, password, or fingerprint.

- The Device goes back to the standby page if there is no operation in 30 seconds.
- The Device turns off the screen if it stays on the standby page for 30 seconds.
- The screen in the user manual is for reference only.

Figure 2-3 Standby screen

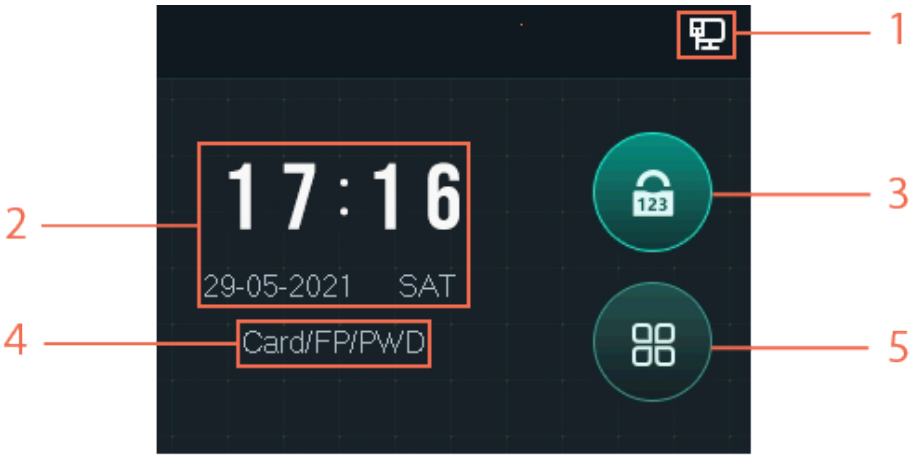


Table 2-2 Description of standby page

No.	Item	Description
1	Status	Displays the status of Wi-Fi, wired network (if any), and USB drive.
2	Date & Time	Time and date.

No.	Item	Description
3	Unlock the door with password	Enter the user ID and password, or the administrator password (for details, see "2.6.4 Administrator Password") to unlock the door.
4	Unlocking methods	Displays the unlocking methods you configured.
5	Main menu	Tap to enter the main menu. Only Admin and users with administrator permission can log in to the main menu. See "2.5 Logging in to the Main Menu".

2.5 Logging in to the Main Menu

Log in to the main menu to configure parameters of the Device. For example, you can add users of different permissions and change the unlocking mode.

Only the administrator and admin users can log in to the main menu.

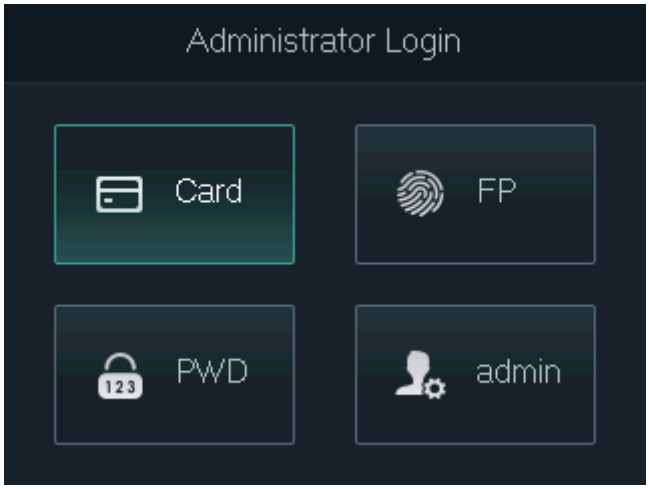
Step 1 On the standby screen, tap .

Verification methods varies with the Device type.

Step 2 Log in to the main menu.

- Log in as a user with the administrator permission by using a card, fingerprint, or password.
- Log in as **admin**: Tap **admin**, and then enter the password you set during initialization.

Figure 2-4 Log in as an administrator



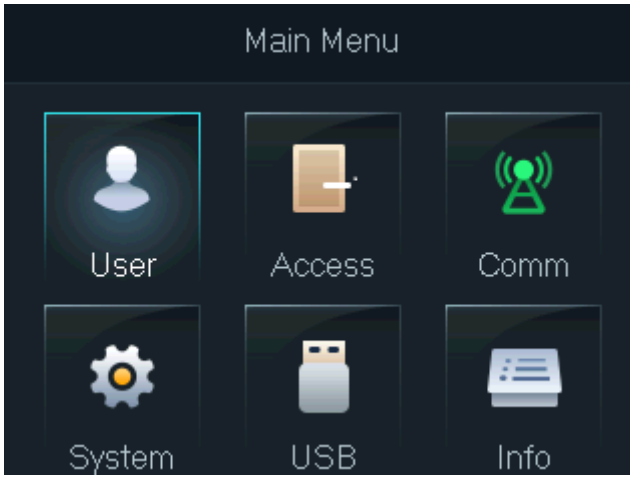
Step 3 On the main menu, tap ∧/∨ to navigate the page, and then tap **OK** to configure parameters of the Device.

Use the shortcuts to configure parameters by simply tapping 1–6.

- To configure user management, tap 1.
- To configure access control, tap 2.
- To configure communication, tap 3.

- To configure system, tap 4.
- To configure USB, tap 5.
- To view system information, tap 6.

Figure 2-5 Main menu



2.6 Unlocking Methods

2.6.1 Card

Swipe your card to unlock the door.

For the Access Standalone with ID function, if it is connected with an external ID card reader, the distance between the Access Standalone and the card reader must be larger than 10 cm. Otherwise, the card reader might malfunction because it is too close to the Access Standalone.

2.6.2 Fingerprint

Press your enrolled fingerprint on the fingerprint scanner to unlock the door.

2.6.3 User Password

Enter the user ID and password to unlock the door.

Step 1 Tap on the standby page.

Step 2 Select **PWD**, and then tap **OK**.

Step 3 Enter the user ID and password.

- To enter the user ID, you need to select the input box of user ID and tap **OK**.
- You can directly enter the password on the keypad.
- Tap to change the input method.

Step 4 Select **OK**, and then tap **OK**.

The system will prompt that the door is unlocked.

2.6.4 Administrator Password

After you set your administrator password and enable it, you can unlock the door by simply entering the administrator password. Using administrator password to unlock the door without being subject to user levels, unlock modes, periods, holiday plans, and anti-passback except for normally closed door.

The Device only allows for one administrator password.

To use the administrator password for door access, you need to enable the function. See "2.7.3 Setting Administrator Password".

Step 1 Select on the standby screen.

Step 2 Select **Admin PWD**, and then tap **OK**.

Step 3 Enter the administrator password.

Step 4 Select **OK**, and then tap **OK**.

The door is unlocked.

2.7 User Management

You can add new users, view the user list or admin list on the **User** screen.

2.7.1 Adding New User

Step 1 Select on the standby screen, and then tap **OK**.

Step 2 Log in with the administrator account, and then select **User > New User**.

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

Figure 2-6 Add a new user

Step 3 Configure the parameters.

Table 2-3 Description of user parameters

Parameter	Description
ID	Each user ID is unique. It can be 18 characters of numbers, letters, or their combination.
Name	Enter the name (a maximum of 32 characters, including numbers, symbols, and letters).
Fingerprint	Each user can add up to 3 fingerprints. Follow the on-screen prompts and voice prompts to add fingerprints. You can enable the duress fingerprint function under each fingerprint. After the duress alarm function is enabled, an alarm will be triggered if the door is unlocked by the duress fingerprint. ● We do not recommend setting the first fingerprint as the duress fingerprint. ● Only certain models support the fingerprint function.
Card	You can register five cards for each user. On the card registration page, swipe your card on the card reader, and then the card information will be read by the Device. You can enable the duress card function on the card registration page. After the duress alarm function is enabled, an alarm will be triggered if the door is unlocked by the duress card.
PWD	Enter password to unlock the door. The maximum length of the ID digits is 8.
Permission	You can select a user permission for the new user. ● Normal users only have door unlock permission. ● Administrators can configure the Device and unlock the door.
Period	A user can only have door access within the defined period. The default value is 255, which means no period is configured.
Holiday Plan	A user can only have door access within the scheduled holidays. The default value is 255, which means no holiday plan is configured.
Valid Date	Define a period during which the user has door access control.
User Type	● **General**: General users can unlock the door normally. ● **Blocklist**: When users in the blocklist unlock the door, service personnel receive a notification. ● **Guest**: Guests can unlock the door within a defined period or for a certain number of times. After the defined period expires or the unlocking times runs out, they cannot unlock the door. ● **Patrol**: Paroling users can have their attendance tracked, but they have no unlocking permissions. ● **VIP**: When VIP unlock the door, service personnel will receive a notification. The VIP user is not restricted by unlock modes, such as **Multi-card** and **Time Section**. ● **Others**: When they unlock the door, the door will stay unlocked for 5 more seconds. ● **Custom User 1/2**: Same as **General**.

Step 4 After you have configured all the parameters, tap **Esc**.

Step 5 Tap **OK** to save changes.

2.7.2 User/Admin List

You can view and search all the general users and admin users, and edit user information.

On the main menu, select **User > User List/Admin List**.

Figure 2-7 User list

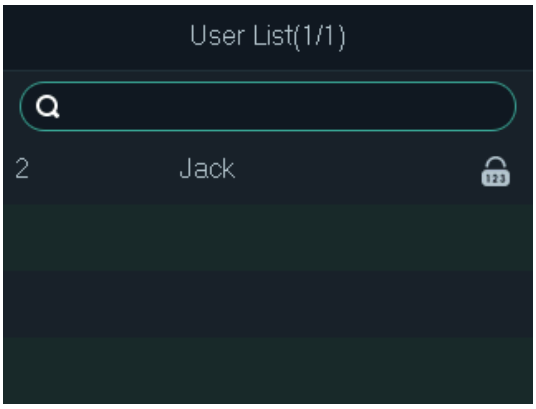
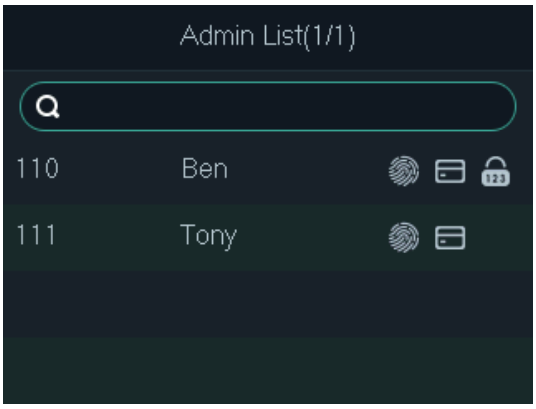


Figure 2-8 Admin list



- Unlocking method
  - ◇ : Fingerprint.
  - ◇ : Card.
  - ◇ : Password.

Editing User Information

Step 1 Select the user and tap **OK**.
Step 2 Edit the user information.
Step 3 Tap **Esc**.
Step 4 Tap **OK** to save changes.

Searching Users

Step 1 Select and tap **OK**.

Step 2 Enter the user ID, swipe a card, or press a fingerprint to search the user.

Deleting Users

Select the user, tap **OK**, and then select to delete the user.

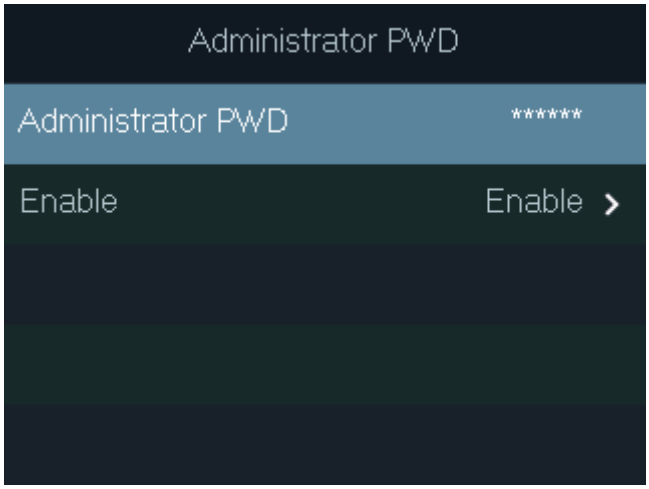
2.7.3 Setting Administrator Password

The Device allows for only one administrator password. You can use it to unlock the door without entering user ID.

Step 1 On the main menu, select **User > Administrator PWD**.

Step 2 Enter the administrator password, and then tap **OK**.

Figure 2-9 Administrator password

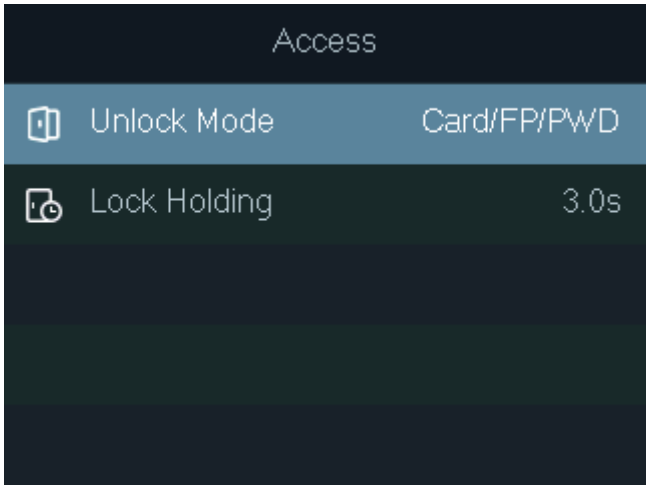


Step 3 Select **Enable**, and then tap **OK** to enable the function.

2.8 Access Control Management

Configure the unlocking mode and the unlocking duration.

Figure 2-10 Access control management



2.8.1 Configuring Unlocking Mode

Configure the unlocking combinations. The unlocking methods vary with different device types.

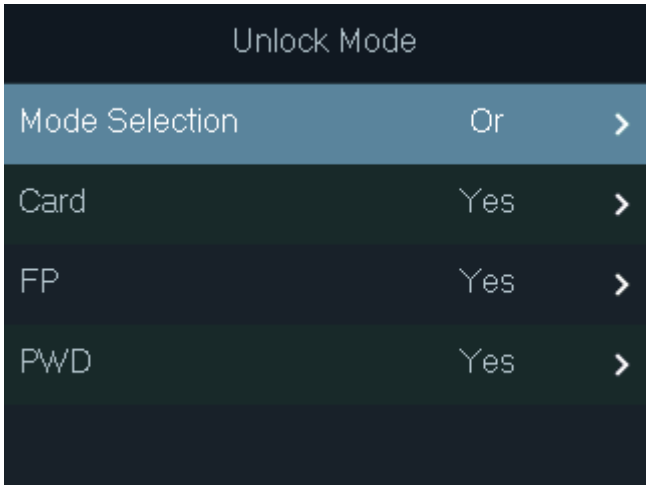
Use card, fingerprint, password, or any of their combinations to unlock the door.

Step 1 On the main menu, select **Access > Unlock Mode**, and then tap **OK**.

Step 2 Tap **OK** to configure the unlocking combinations.

- **And**: You have to verify all the selected unlocking methods to open the door.
- **Or**: You can verify one of the selected unlocking methods to open the door.

Figure 2-11 Element (Multiple Choice)



Step 3 Tap **Esc**.

Step 4 Tap **OK** to save changes.

2.8.2 Configuring Lock Holding Time

The door will remain unlocked during the defined period.

Step 1 On the main menu, select **Access > Lock Holding**.

Step 2 Tap **OK**, and then enter the time.

Tap to change the input method.

2.9 Communication

Configure the network, serial port and Wiegand port parameters to connect the Device to the network or other devices.

2.9.1 Configuring IP

Set IP address for the Device to connect it to the network. After that, you can log in to the web portal to configure the Device, and add it to SmartPSS AC.

Step 1 On the main menu, select **Comm > IP Address**, and then tap **OK**.

Step 2 Select **IP Address** and tap **OK** to configure parameters.

Figure 2-12 Configure IP

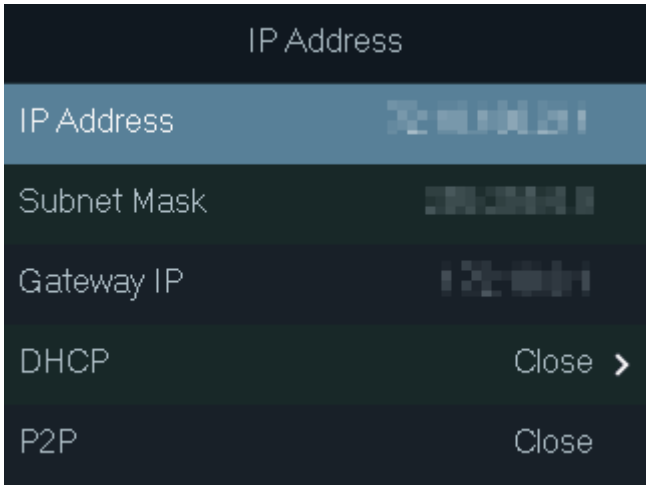


Table 2-4 Description of network parameters

Parameter	Description
IP address, subnet mask and gateway	The IP address, subnet mask, and gateway IP address should be on the same network segment. Tap **Esc** to save the configurations.
DHCP	It stands for Dynamic Host Configuration Protocol. When it is enabled, the Device will automatically obtain an IP address.
P2P	When it is enabled, you can directly manage the Device without a dynamic domain, relay server, or port mapping.

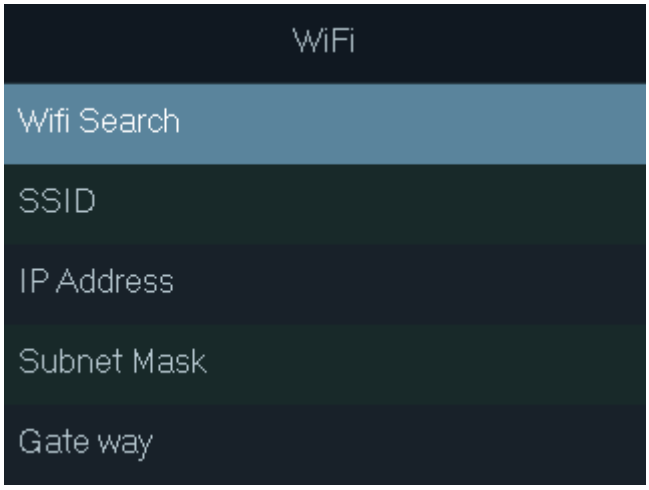
2.9.2 Configuring Wi-Fi

Connect the Device to a wireless network.

Only certain models support Wi-Fi.

Step 1 On the main menu, select **Comm > Wi-Fi**, and then tap **OK**.

Figure 2-13 Wi-Fi



Step 2 Select **Wifi Search**, and then tap **OK**.

Step 3 Select **WiFi**, and then tap **OK** to enable the Wi-Fi function.

The Device will search for and display available wireless networks.

Tap or to go to the previous or next page.

Step 4 Select a wireless network, tap **OK**, and then enter the password.

2.9.3 Configuring Wiegand

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

On the main menu, select **Comm > Wiegand**, and then tap **OK**.

- Select **Wiegand Input** when you need to connect a card reader to the Device.
- Select **Wiegand Output** when the Device functions as a card reader, and you need to connect it to another access controller.

Figure 2-14 Wiegand

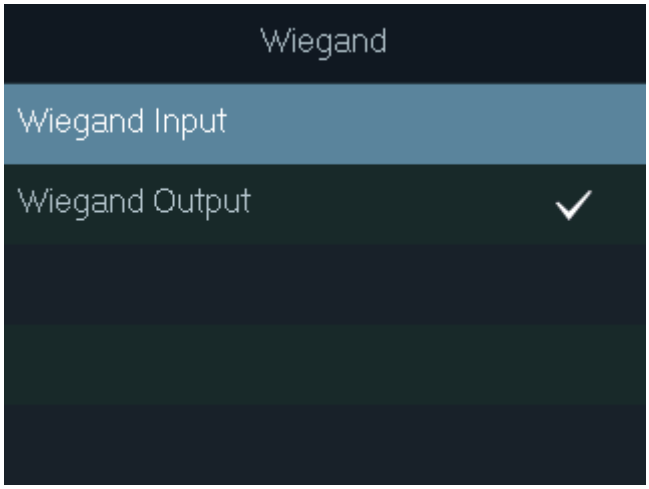


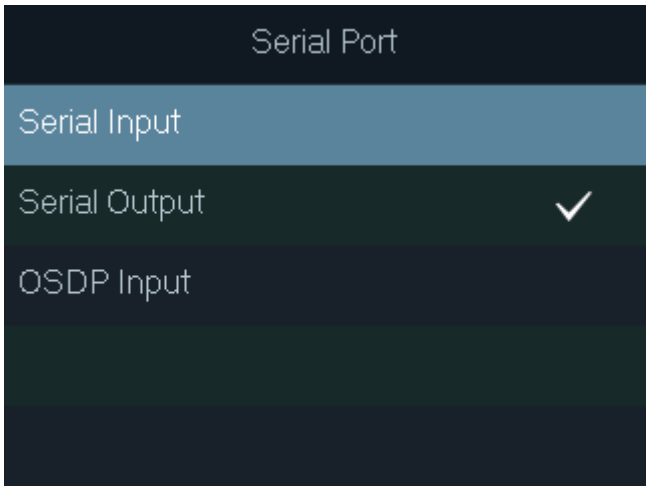
Table 2-5 Description of Wiegand parameters

Parameter	Description
Output Type	Select a Wiegand format to read card numbers or ID numbers. ● **Wiegand26**: Reads 3 bytes or 6 digits. ● **Wiegand34**: Reads 4 bytes or 8 digits. ● **Wiegand66**: Reads 8 bytes or 16 digits.
Pulse Width	Enter the value.
Pulse Interval	
Output Data Type	● **UserID**: Outputs the ID of the user who swipes a card. ● **Card No.**: Outputs the card number that is used.

2.9.4 Configuring Serial Port

On the main menu, select **Comm > Serial Port**, and then tap **OK**.

Figure 2-15 Serial port settings



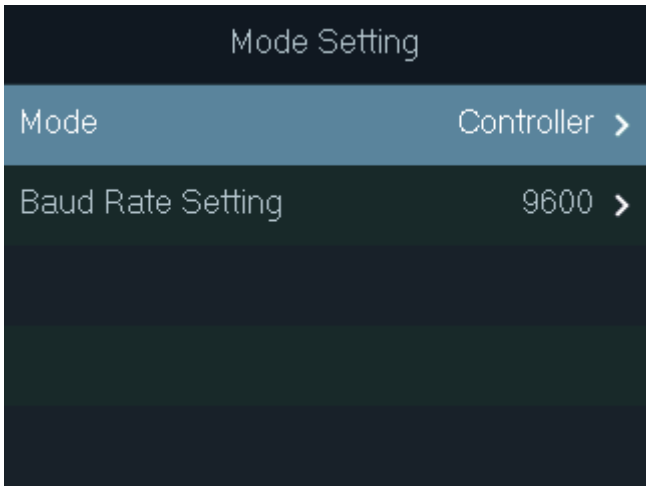
- Select **Serial Input** when the Device connects to a card reader. The card reader will send the card number to the Device or SmartPSS AC.
- Select **Serial Output** when the Device functions as a card reader. The Device will send the card number to the controller, and the controller controls the door access.
  - ◇ **UserID**: Outputs the ID of the user who swipes a card.
  - ◇ **Card No.**: Outputs the card number that is used.
- Select **OSDP Input** when the Device connects a card reader through OSDP protocol. The card reader will send the card information to the Device or SmartPSS AC.

2.9.5 Configuring Mode

The Device can function as a controller or a card reader.

On the main menu, select **Comm > Mode Setting**.

Figure 2-16 Serial port settings



- Mode
  - ◇ **Controller**: The Device works as an access controller. You can connect it to a card reader, and the card reader sends the card information to the Device or SmartPSS AC.
  - ◇ **Card Reader**: The Device functions as a card reader, and it can be connected to a controller or another access standalone.

    - The serial port input cannot be configured in the card reader mode.

- For the card reader mode, refer to the wiring method of a card reader. You can connect the Device to an external controller or another access standalone via RS485 protocol. It does not support Wiegand.
- For card reader mode, the two wires A/B (RS-485) are connected to the A/B wires of the controller. To realize the tamper alarm function, DOOR1_COM and DOOR1_NC should be connected to the CASE and GND wires of the external controller.

- Baud Rate Setting
  - ◇ **9600**: By default.
  - ◇ **115200**: Applicable to the controller and card reader with this baud rate.

  - For the card reader mode, the baud rate will automatically adjust according to the external controller. We recommend you not to modify other configurations on the web portal and on the device.
  - For the controller mode, you need to manually set the same baud rate as the external device.

2.10 System

2.10.1 Time

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

Step 1 On the main menu, select **System > Time**, and then tap **OK**.

Step 2 Select a parameter, and then tap **OK**.

Figure 2-17 Time settings

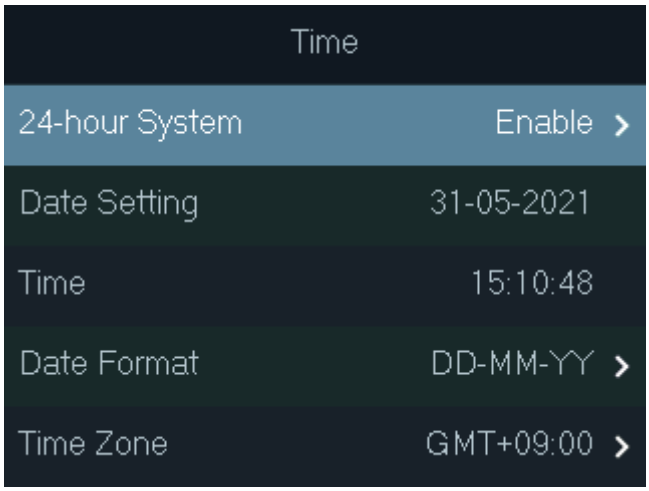


Table 2-6 Description of time parameters

Parameter	Description
24-hour System	Enable 24-hour format.
Date Setting	Set up the date.
Time	Set up the time.
Date Format	Select a date format.
Time Zone	Select a time zone.

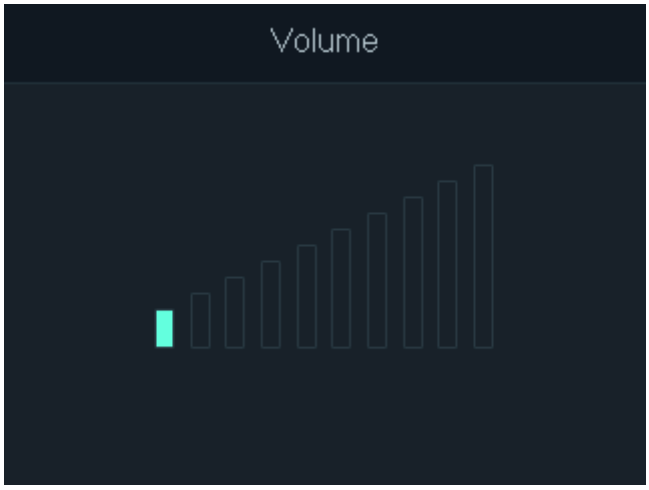
2.10.2 Volume

Adjust the volume of the voice prompt.

Step 1 On the main menu, select **System > Volume**, and then tap **OK**.

Step 2 Tap the up arrow or down arrow to adjust the volume.

Figure 2-18 Adjust the volume



2.10.3 Restoring to Default Settings

⚠

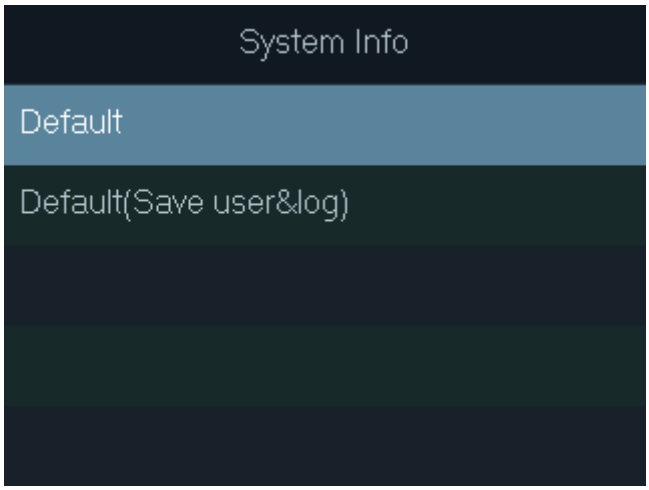
Data will be lost if you restore the Device to factory defaults. Please be advised.

Step 1 On the main menu, select **System > Restore Factory**, and then tap **OK**.

Step 2 Select an option, and then tap **OK**.

- **Default**: Restores factory defaults and deletes all data, including users, device information, and logs.
- **Default (Save user&log)**: Restores factory defaults and deletes all data except user information and logs.

Figure 2-19 Restore to default settings



2.10.4 Restarting the Device

On the main menu, select **System > Reboot**, and then tap **OK** to restart the Device.

2.11 USB Management

⚠

- Make sure that a USB flash drive is inserted to the Device before exporting user information or upgrading system. To avoid failure, do not pull out the USB flash 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 flash drive first.

You can use a USB flash drive to update the Device, and export or import user information.

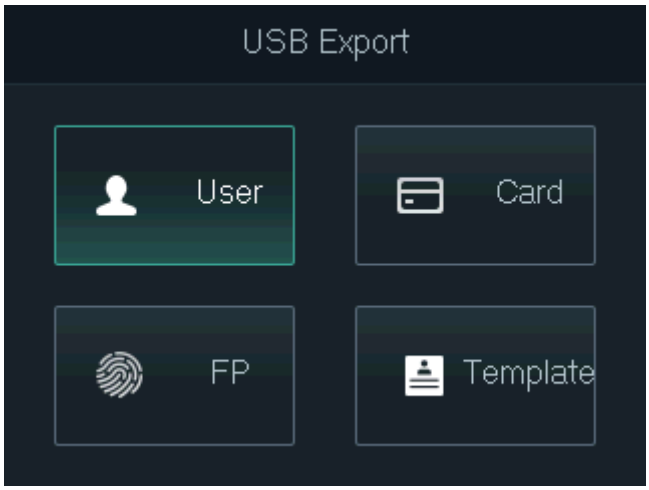
2.11.1 Exporting to USB

Export data from the Device to a USB flash drive. The exported data is encrypted and cannot be edited.

Step 1 On the main menu, select **USB > USB Export**, and then tap **OK**.

Step 2 Select the type of data you want to export, and then tap **OK**.

Figure 2-20 Export data to the USB drive



Step 3 Tap **OK**.

The selected data is exported to the USB flash drive.

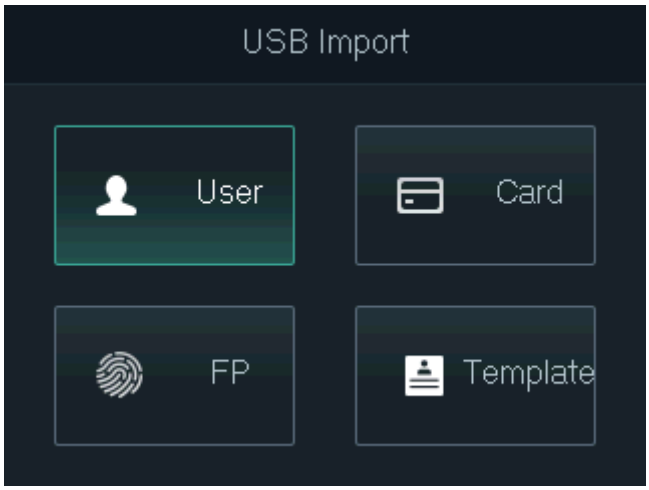
2.11.2 Importing From USB

You can import data from USB to the Device.

Step 1 On the main menu, select **USB > USB Import**, and then tap **OK**.

Step 2 Select the type of data you want to import, and then tap **OK**.

Figure 2-21 Import data from the USB flash drive



Step 3 Tap **OK**.

The selected data is imported to the Device.

2.11.3 Updating System

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

Step 1 Rename the update file to "update.bin", put it in the root directory of the USB flash drive, and then insert the USB flash drive to the Device.

Step 2 On the main menu, select **USB > USB Update**.

Step 3 Tap **OK**.

The Device will restart when update is complete.

2.11.4 Exporting Unlocking Records

Export unlocking records to a USB flash drive.

Step 1 On the main menu, select **USB > Export Records**, and then tap **OK**.

Step 2 Select the time.

Figure 2-22 Export unlocking records

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

The unlocking records are exported to the USB flash drive.

2.11.5 Exporting/Importing User Information

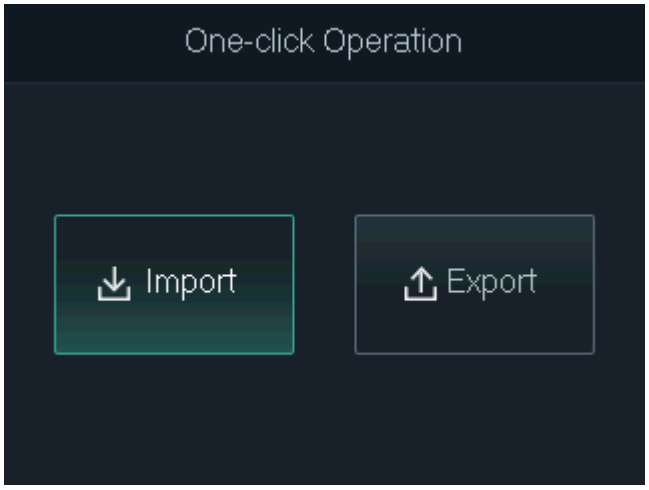
You can use one-click function to import or export user information, including cards and fingerprints.

Step 1 On the main menu, select **USB > One-click Operation**, and then tap **OK**.

- **Import**: Import user information, including cards and fingerprints.
- **Export**: Export user information, including cards and fingerprints.

Step 2 Select **Import** or **Export**, and then tap **OK**.

Figure 2-23 One-click operation



2.12 System Information

On the main menu, select **Info**, and then tap **OK**. You can view data capacity and system information of the Device.

- **Data Capacity**: Displays the number of general users, admin users, cards, fingerprints, unlocking records, and alarm records that have been stored, and the storage capacity.
- **Device Version**: Displays software and hardware information of the Device.

3 Web Configuration

Open the web browser on your computer or phone. Log in to the web page to configure and update the Device.

3.1 Web on Computer

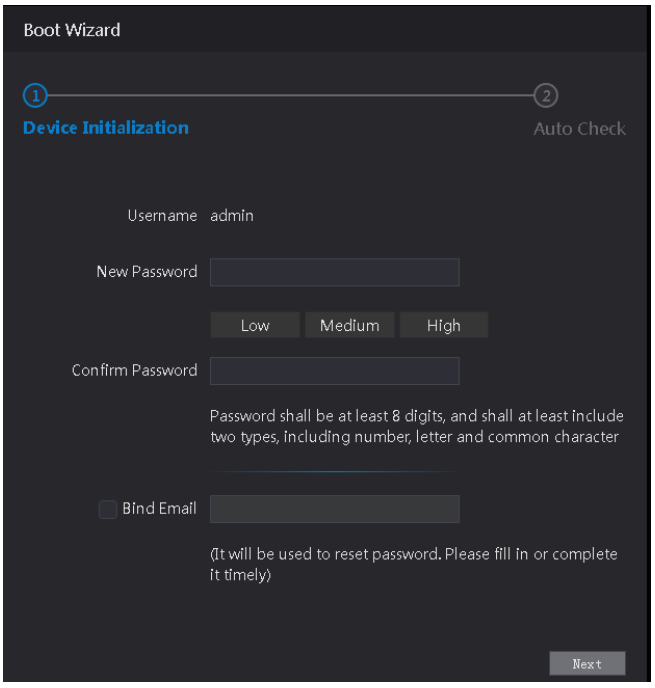
3.1.1 Initialization

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

Step 1 Go to the IP address (192.168.1.108 by default) of the Device in the browser.

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

Figure 3-1 Initialization

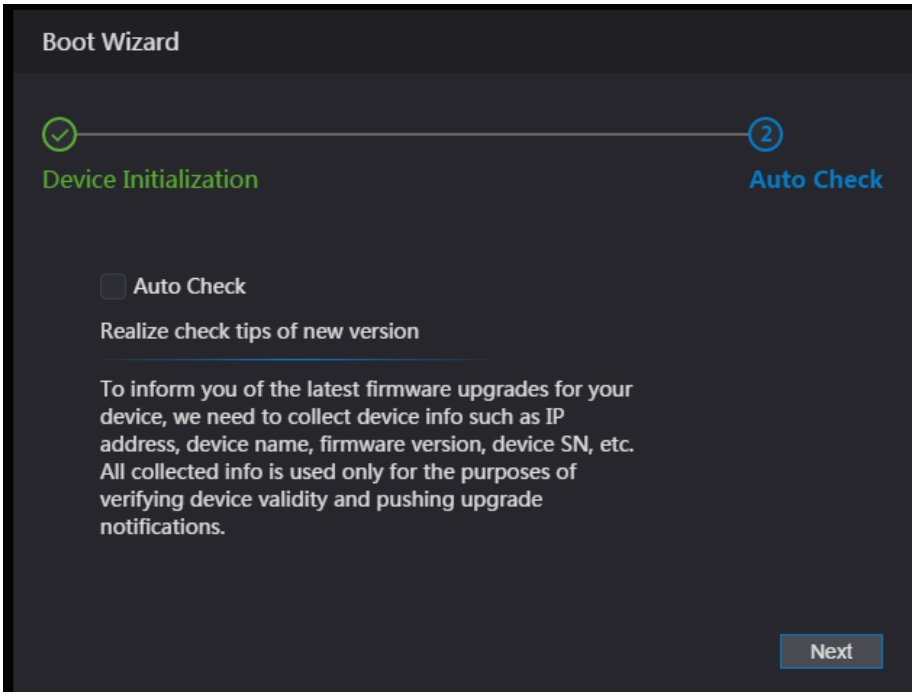


Step 2 Enter the new password, confirm password, enable **Bind Email**, enter an email address, and then click **Next**.

- 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.
- Keep the password properly after initialization and change the password regularly to improve security.
- When you need to reset the administrator password by scanning the QR code, you need the associated email address to receive the security code.

Step 3 Click **Next**.

Figure 3-2 Auto check

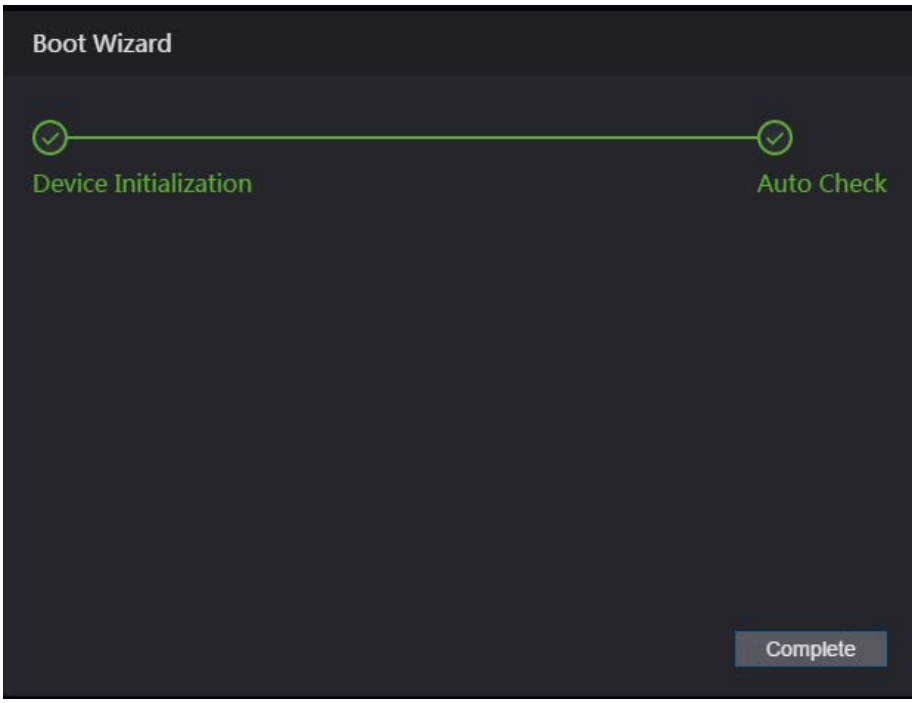


Step 4 (Optional) Select **Auto Check**.

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

Step 5 Click **Next**.

Figure 3-3 Finish initialization



Step 6 Click **Complete**.

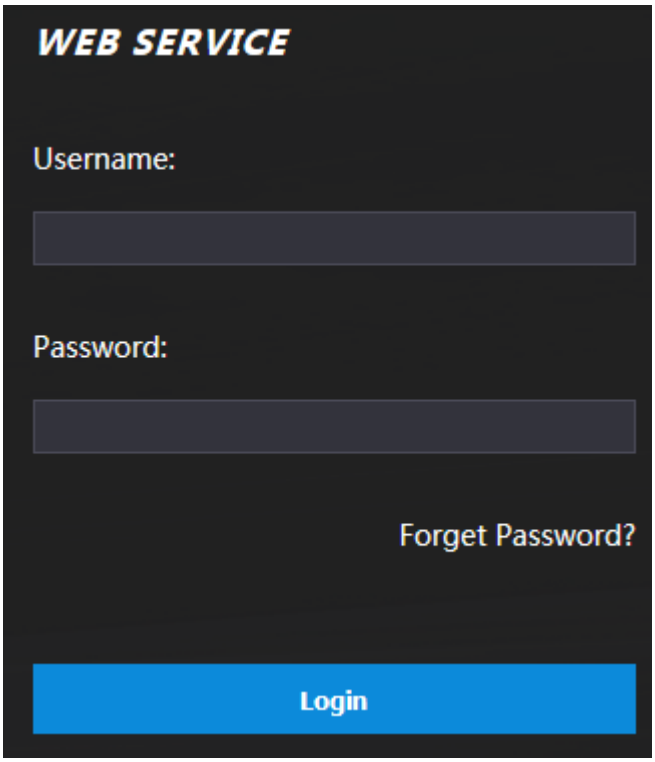
3.1.2 Logging In

Step 1 Go to the IP address (192.168.1.108 by default) of the Device in the browser, and press the

Enter key.

- Make sure that the computer is on the same LAN as the Device.
- The default IP address is 192.168.1.108.

Figure 3-4 Login



Step 2 Enter the user name and password.

- The default administrator name is admin, and the password is the one you set during initialization. We recommend you to change the administrator password regularly to increase security.
- If you forgot the administrator password, click **Forget Password?** to reset it. See "3.3 Resetting the Password".

Step 3 Click **Login**.

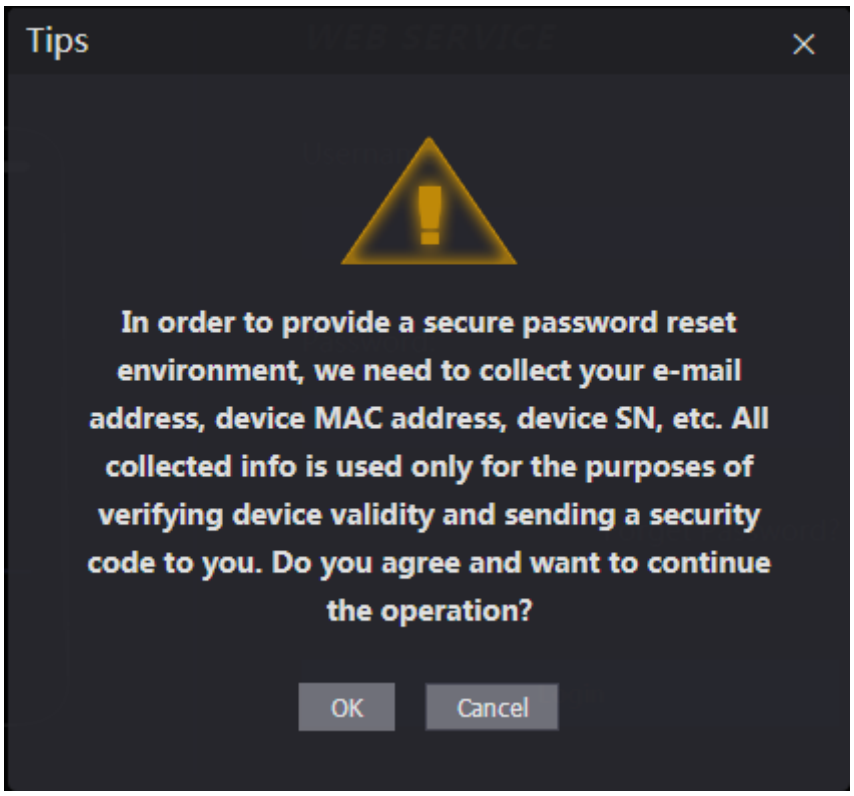
3.1.3 Resetting the Password

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

Step 1 On the login page, click **Forgot Password**.

Step 2 Read the prompt carefully and click **OK**.

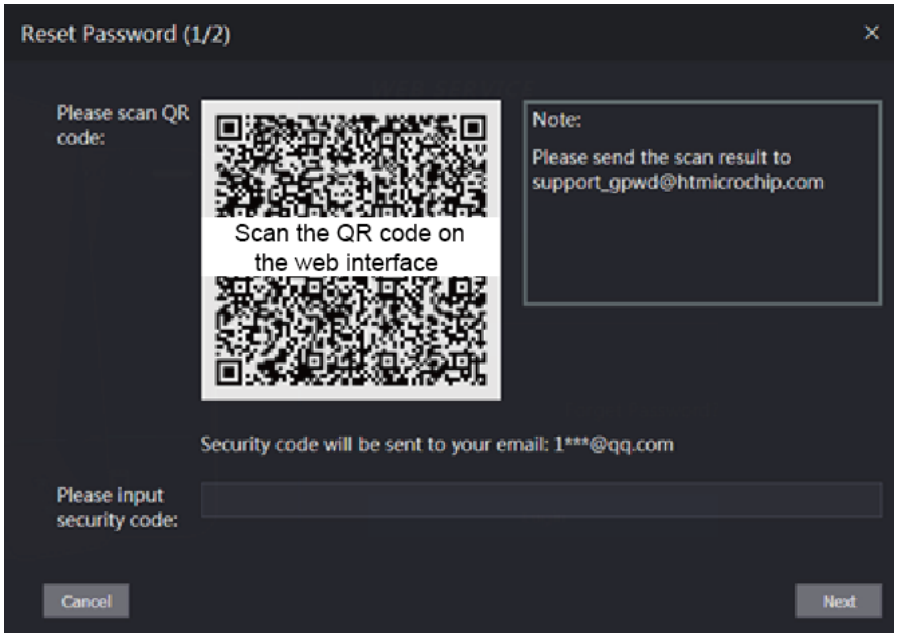
Figure 3-5 Reset prompt



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

Figure 3-6 Reset Password



Step 4 Enter the security code you have received.

Step 5 Click **Next**.

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** to complete resetting.

3.1.4 Configuring Door Parameter

Configure the access control parameters.

Step 1 Log in to the web page.

Step 2 Select **Door Parameter**.

Figure 3-7 Figure 3-9 Door parameter

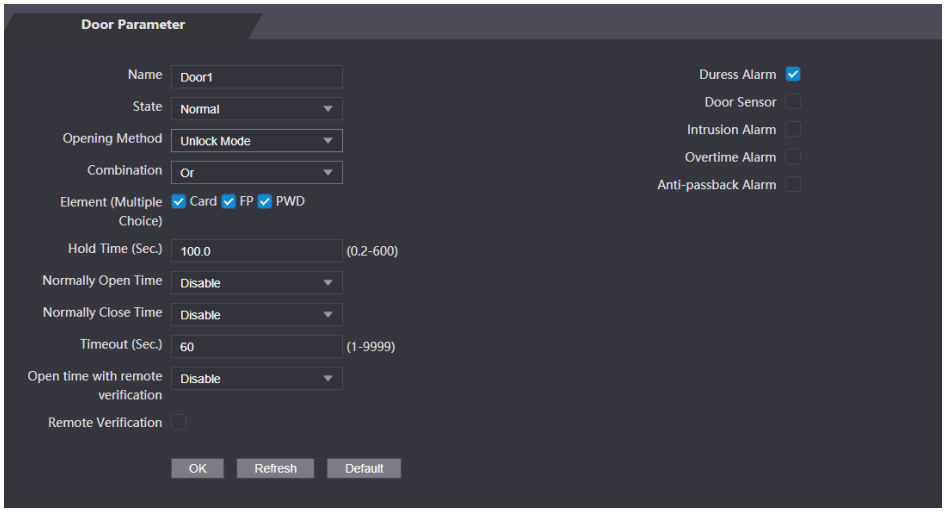


Table 3-1 Description of door parameters

Parameter	Description
Name	Enter a name for the door that the Device controls.
State	Select **NC** for normally closed, or **NO** for normally open. If either is selected, the defined opening method will not be effective.
Opening Method	• **Time Section:** Set different unlock method for defined periods. • **Multi-card**: The user can unlock the door when multiple users and multiple user groups grant access. • **Unlock mode**: set unlock combinations.
Hold Time (Sec.)	Unlock duration. The door will be locked again after the duration. It ranges from 0.2 to 600 seconds.
Normally Open Time	The door remains open or closed during the defined period.
Normally Close Time	

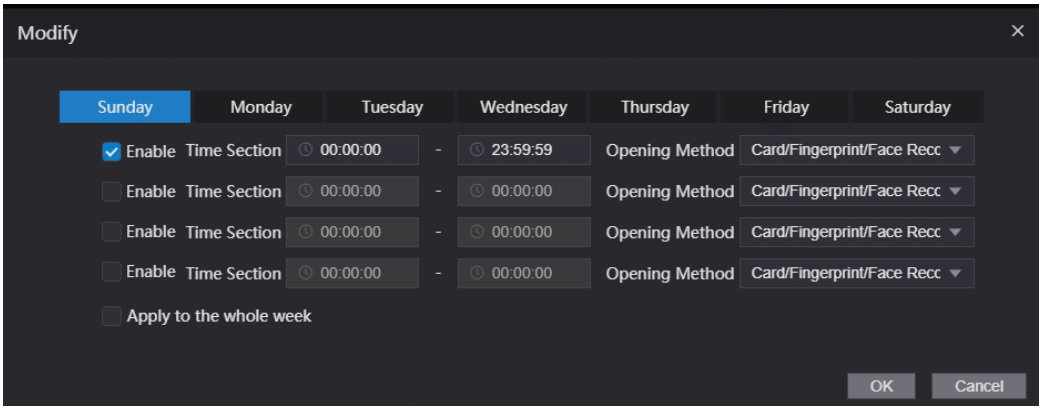
Parameter	Description
Timeout (Sec.)	A timeout alarm will be triggered if the door remains unlocked for longer time than this value.
Remote Verification	Set the remote verification door opening period. For details, see "3.6.1 Configuring Time Section". When opening a door is authorized on the device, it needs to be confirmed on the platform before it can be opened.
Duress Alarm	An alarm will be triggered when a duress card or duress password is used to unlock the door.
Door Sensor	Intrusion and overtime alarms can be triggered only after **Door Sensor** is enabled.
Intrusion Alarm	When **Door Sensor** is enabled, an intrusion alarm will be triggered if the door is opened abnormally.
Overtime Alarm	A timeout alarm will be triggered if the door remains unlocked for longer time than the **Timeout(Sec)**, which ranges from 1 to 9999 seconds.
Anti-passback Alarm	If enabled, users need to verify identities both for entry and exit; otherwise an alarm will be triggered. ● If a person enters with verification and exits without verification, an alarm will be triggered when they attempt to unlock again, and access is denied at the same time. ● If a person enters without verification and exits with verification, an alarm will be triggered when the they attempt to unlock again, and access is denied at the same time.

Step 3 Configure unlock method.

- Time section

1) In the **Opening Method** list, select **Time Section**, and then click .

Figure 3-8 Time section parameter

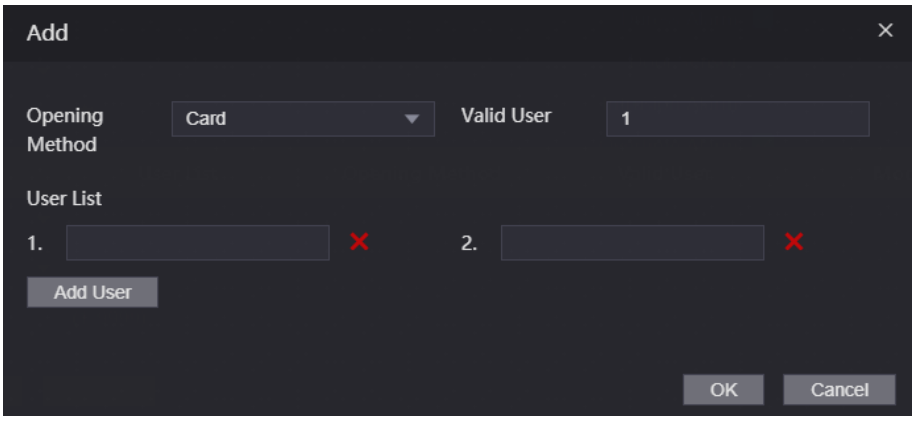


2) Configure the time and opening method for a time section. You can configure up to four time sections for a single day.
3) (Optional) Select **Apply to the whole week** to copy the configuration to the rest of days.
4) Click **OK**.

- Multi-card

1) In the **Opening Method** list, select **Multi-card**, and then click .
2) Click **Add**.
3) Select an unlocking method in the **Opening Method** list., and enter a number for the valid user.

Figure 3-9 Multi-card parameter



4) In the **User List** area, enter user ID. For details, see "2.7.1 Adding New User".

- VIP, patrol, and blocklist users cannot be added.
- All the users in different groups must all verify their identities in the group order to unlock the door.

- Unlock mode

1) In the **Opening Method** list, select **Unlock Mode**.
2) In the **Combination** list, select **Or** or **And**.
   - **And** means you must use all the selected methods to open the door.
   - **Or** means you can open the door with any of the selected methods.
3) In the **Element** list, select the unlock method.

Step 4 Configure other parameters.

Step 5 Click **OK**.

3.1.5 Alarm Linkage

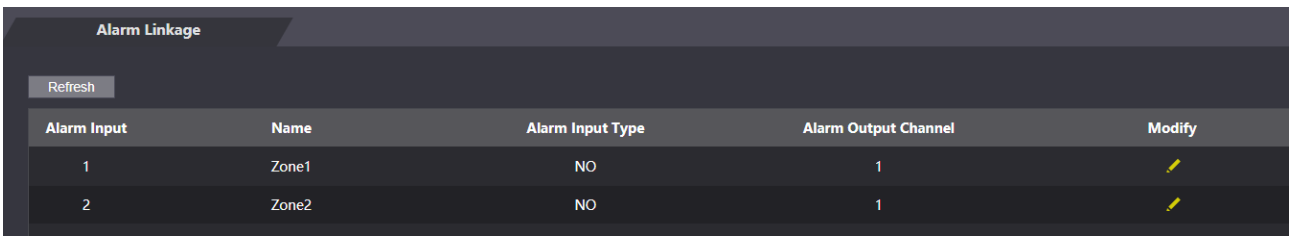
3.1.5.1 Setting Alarm Linkage

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

Step 1 Log in to the web page.

Step 2 Select **Alarm Linkage** > **Alarm Linkage**.

Figure 3-10 Alarm linkage



Step 3 Click to configure alarm linkage.

Figure 3-11 Modify linkage parameters

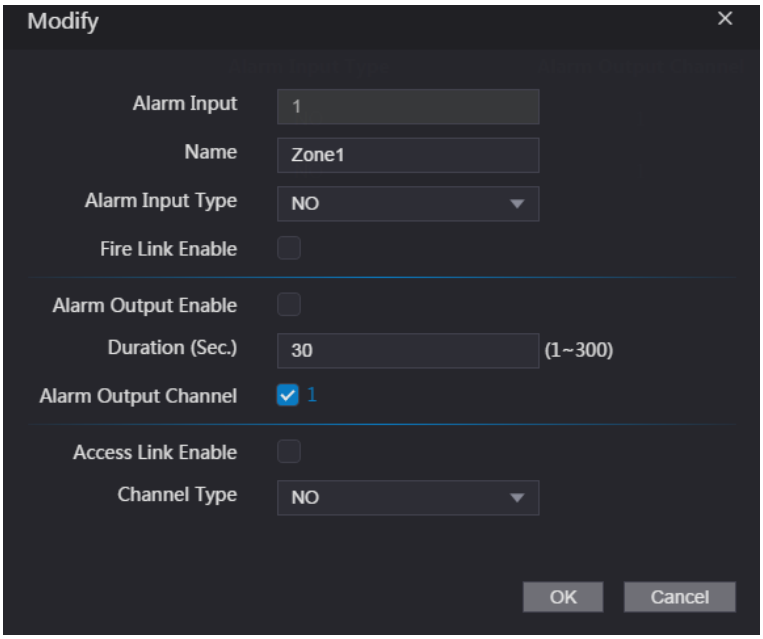


Table 3-2 Description of alarm linkage parameters

Parameter	Description
Alarm Input	You cannot modify the value. Keep it default.
Name	Enter a zone name.
Alarm Input Type	Select the type according to the alarm device. ● **NO**: The circuit of the alarm device is normally open, and it closes when an alarm is triggered. ● **NC**: The circuit of the alarm device is normally closed, and it opens when an alarm is triggered.
Fire Link Enable	If fire linkage is enabled, the device will generate fire alarms when being triggered. The alarm messages are displayed in the alarm log. If fire link is enabled, alarm output and access linkage are NO by default.
Alarm Output Enable	If alarm output is enabled, the relay can generate alarm messages.
Duration (Sec.)	Alarm duration. It ranges from 1 s through 300 s.
Alarm Output Channel	The Device has only one output channel. Select the output channel according to your alarm device.
Access Link Enable	If access linkage is enabled, the Device will be normally on or normally closed when there are input alarm signals.
Channel Type	There are two options: NO and NC.

Step 4 Click **OK** to save changes.

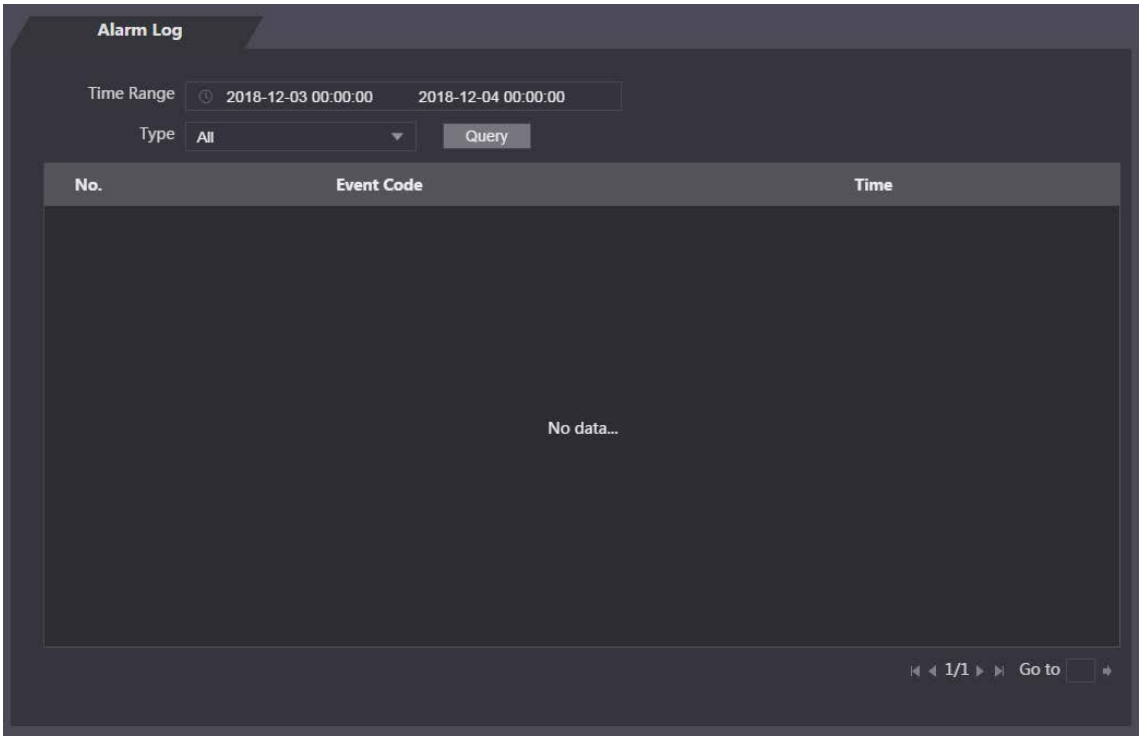
The configurations on the web will be synchronized with the software client if the Device is added to the client.

3.1.5.2 Alarm Log

Step 1 Log in to the web page.

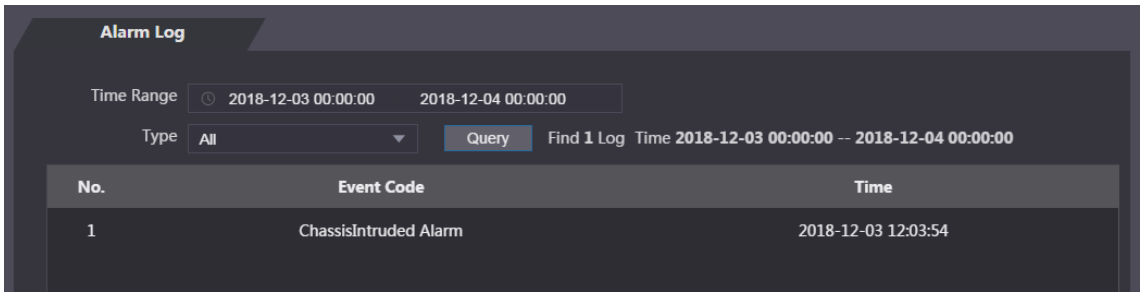
Step 2 Select **Alarm Linkage** > **Alarm Log**.

Figure 3-12 Alarm log



Step 3 Select a time range and alarm type, and then click **Query**.

Figure 3-13 Query results



3.1.6 Time Section

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

3.1.6.1 Configuring Time Section

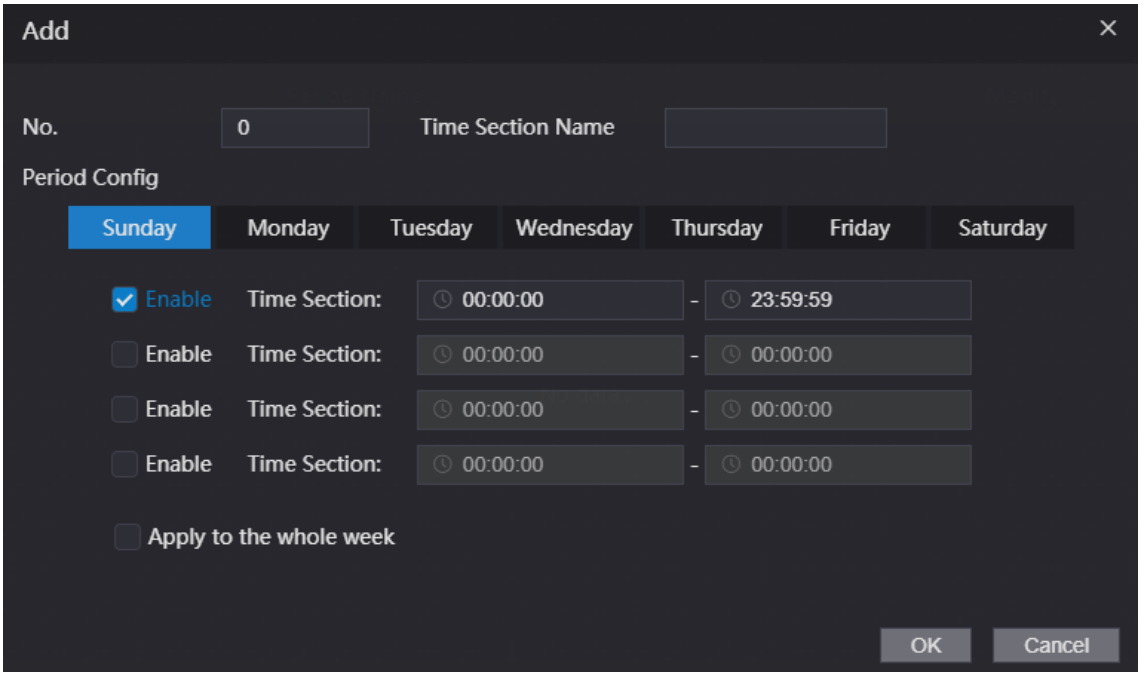
You can configure up to 128 groups (from No.0 through No.127) of time section. In each group, you need to configure door access schedules for a whole week. A user can only unlock the door during the scheduled time.

Step 1 Log in to the web page.

Step 2 Select **Time Section** > **Time Section**.

Step 3 Click **Add**.

Figure 3-14 Time section parameters



Step 4 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 5 Configure time sections for each day.

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

Step 6 (Optional) Click **Apply to the whole week** to copy the configuration to the rest of days.

Step 7 Click **OK** to save the changes.

3.1.6.2 Configuring Holiday Group

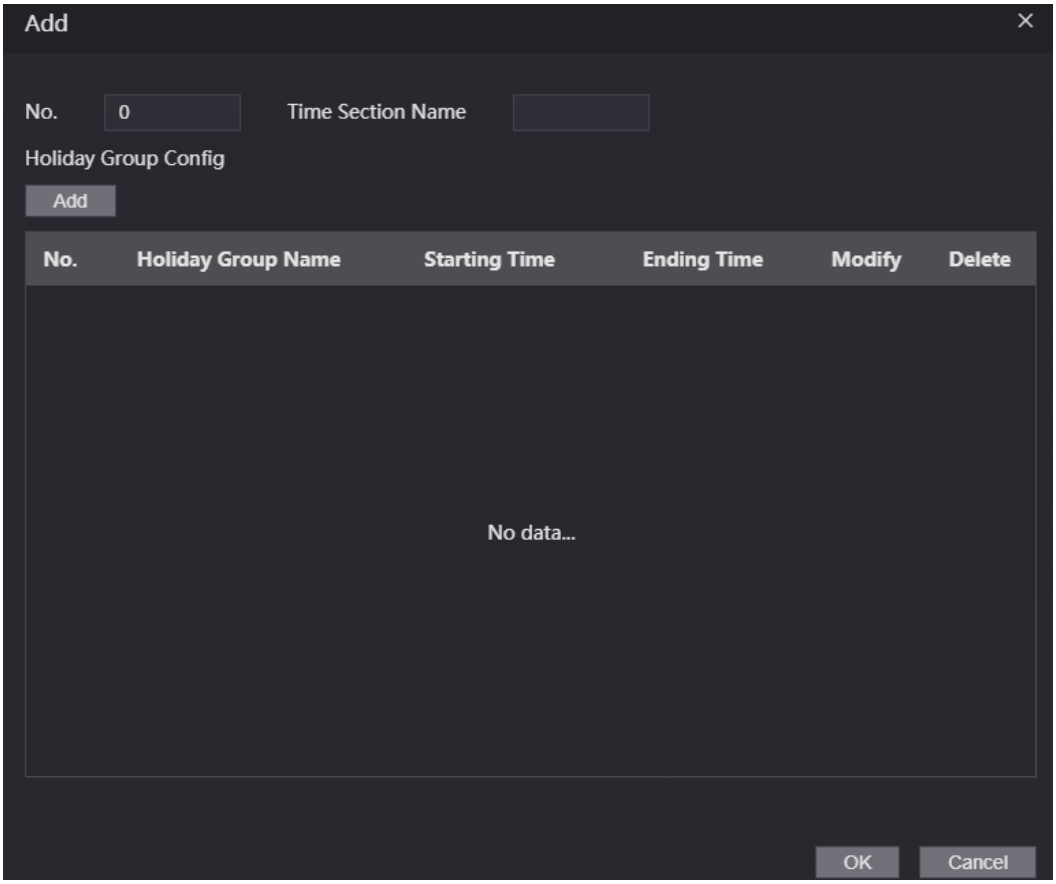
Set time sections for different holiday groups. You can configure up to 128 holiday groups (from No.0 through No.127). and up to 16 time sections for a single holiday group. Users can unlock doors in the defined time sections.

Step 1 Log in to the web page.

Step 2 Select **Time Section** > **Holiday Group Config**.

Step 3 Click **Add**.

Figure 3-15 Add a holiday group



Step 4 Enter a number and a name for the holiday group.

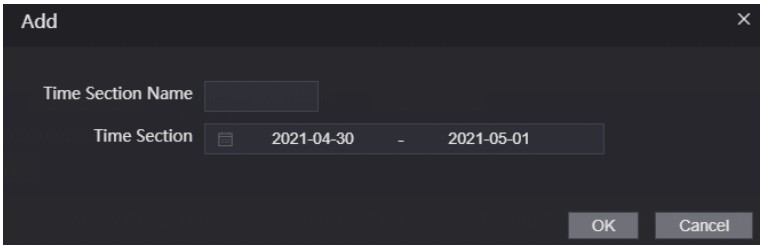
- **No.**: Enter a section number. It ranges from 0 through 127.
- **Time Section Name**: Enter a name for each time section. You can enter a maximum of 32 characters (contain numbers, special characters and English characters).

Step 5 Click **Add**.

Step 6 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 3-16 Add a holiday



Step 7 Click **OK**.

3.1.6.3 Configuring Holiday Plan

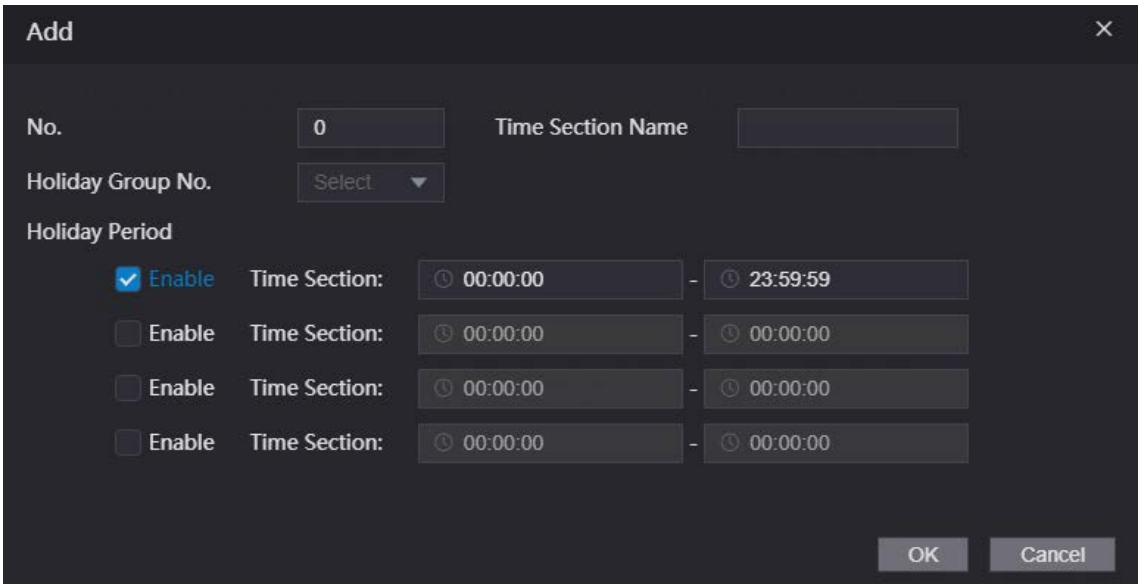
Assign the configured holiday groups to the holiday plan. Users can only unlock the door in the defined time in the holiday plan.

Step 1 Log in to the web page.

Step 2 Select **Time Section** > **Holiday Plan Config**.

Step 3 Click **Add**.

Figure 3-17 Add a holiday plan



Step 4 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 5 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 6 In the **Holiday Period** area, configure time sections in the holiday group. You can configure up to four time sections.

Step 7 Click **OK**.

3.1.7 Data Capacity

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

Step 1 Log in to the web page.

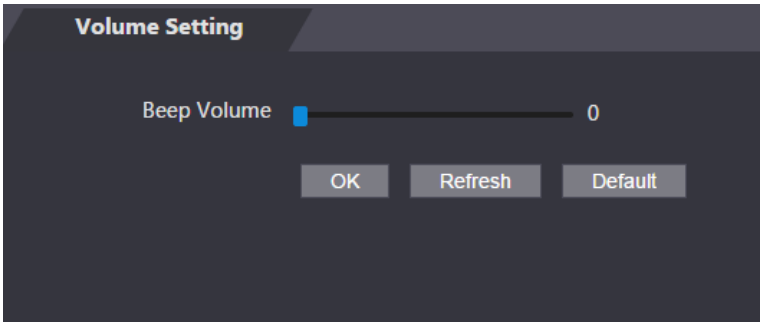
Step 2 Select **Data Capacity** on the navigation bar.

3.1.8 Setting Volume

Step 1 Log in to the web page.

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

Figure 3-18 Volume setting



Step 3 Click **OK**.

3.1.9 Configuring Network

3.1.9.1 Configuring TCP/IP

You need to configure IP address and DNS server so that the Device can communicate with other devices.

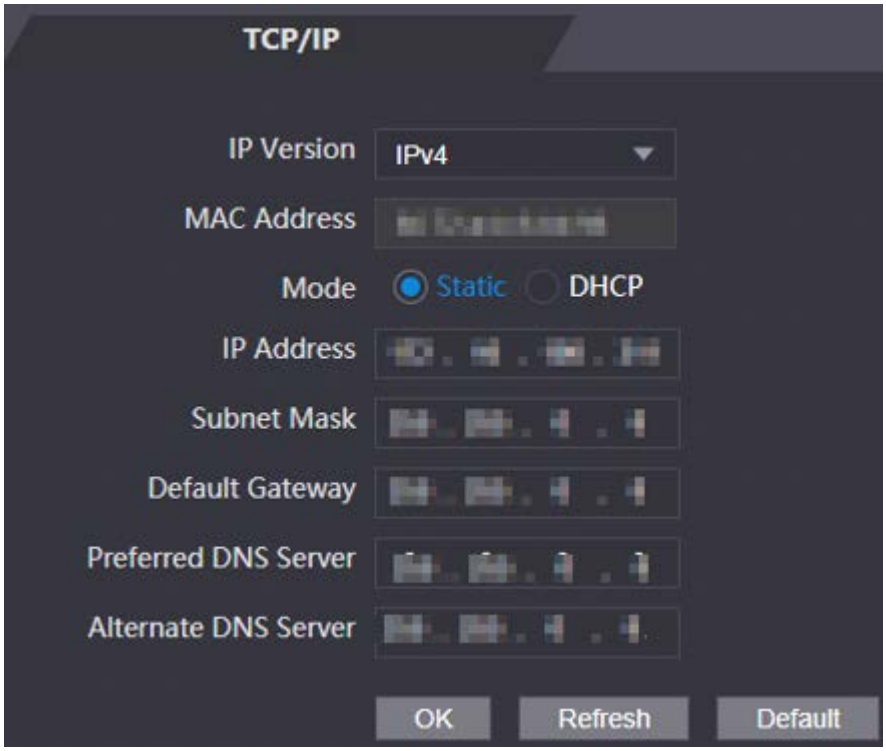
Prerequisite

Make sure that the Device is connected to the network.

Step 1 Log in to the web page.

Step 2 Select **Network Setting** > **TCP/IP**.

Figure 3-19 TCP/IP



Step 3 Configure parameters.

Table 3-3 Description of TCP/IP

Parameter	Description
IP Version	IPv4.
MAC Address	MAC address of the Device.
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 assigned by DHCP automatically. ◇ If you disable DHCP, the default IP will be displayed.
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	
Default Gateway	
Preferred/ Alternate DNS Server	Set IP address of the preferred DNS server.

Step 4 Click **OK** to complete the setting.

3.1.9.2 Configuring Port

You can limit access to the Device at the same time by web, software and phone, and configure port numbers of the Device.

Step 1 Log in to the web page.

Step 2 Select **Network Setting** > **Port**.

Step 3 Configure the port number.

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

Table 3-4 Description of ports

Parameter	Description
Max Connection	Set the maximum access to the Device via clients, such as web, software, and phone. Platform clients like SmartPSS AC are not counted.
TCP Port	Default value is 37777.
HTTP Port	Default value is 80. If you want to change the port number, add the changed port number after the address when you log in via a web browser.
HTTPS Port	Default value is 443.
RTSP Port	Default value is 554.

Step 4 Click **OK** to complete the setting.

3.1.9.3 Register

The Device reports its address to the designated server so that clients can access.

Step 1 Log in to the web page.

Step 2 Select **Network Setting** > **Auto Register**.

Step 3 Select **Enable**, and enter host IP, port, and sub device ID.

Table 3-5 Auto register description

Parameter	Description
Host IP	Server IP address or server domain name.
Port	Server port used for auto registeration.
Sub Device ID	Access controller ID assigned by the server.

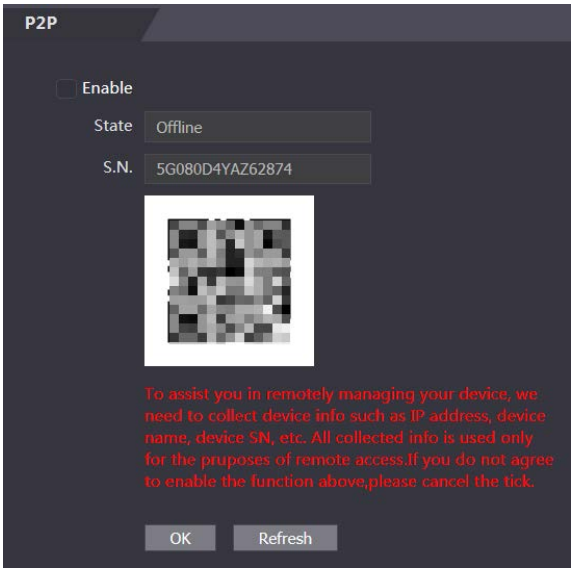
Step 4 Click **OK** to complete the setting.

3.1.9.4 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, you must connect the Device to the Internet; otherwise this function cannot work properly.

Figure 3-20 P2P



Step 1 Log in to the web page.

Step 2 Select **Network Setting** > **P2P**.

Step 3 Select **Enable** to enable the P2P function.

Step 4 Click **OK**.

Scan the QR code on your web page to get the serial number of the Device.

3.1.10 Setting Date

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 3-21 Date setting

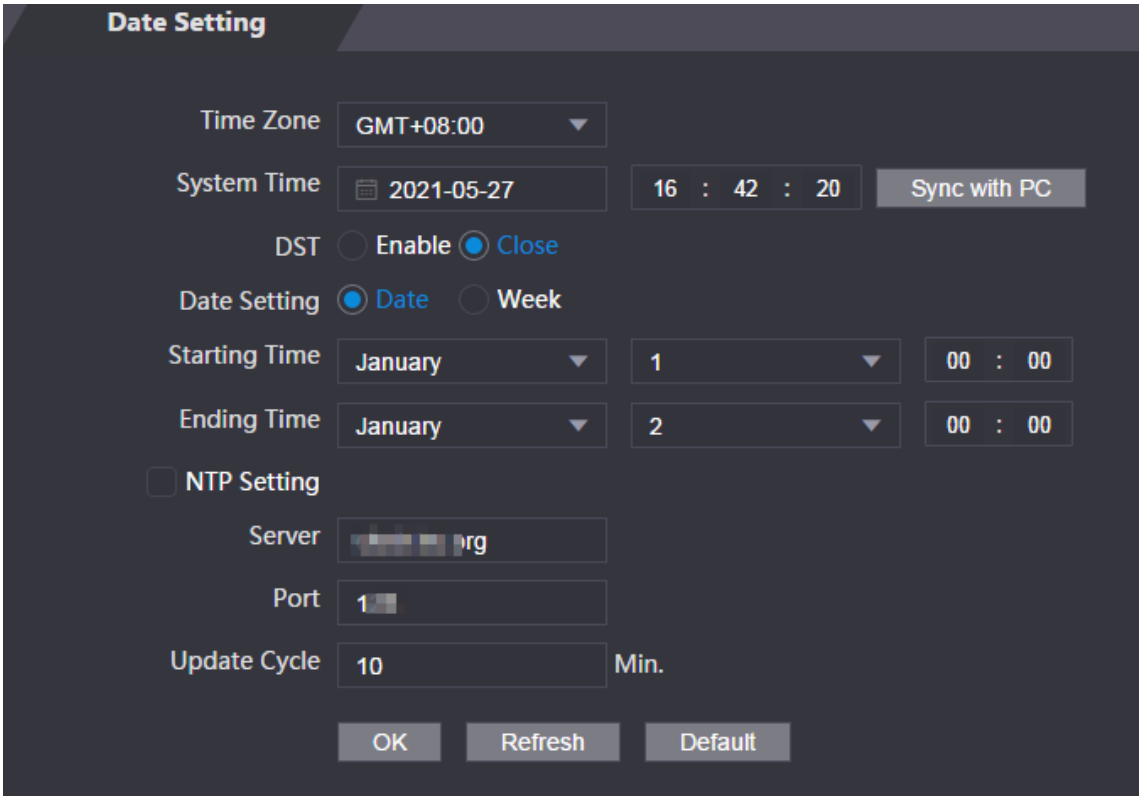


Table 3-6 Data setting description

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

Step 3 Click **OK**.

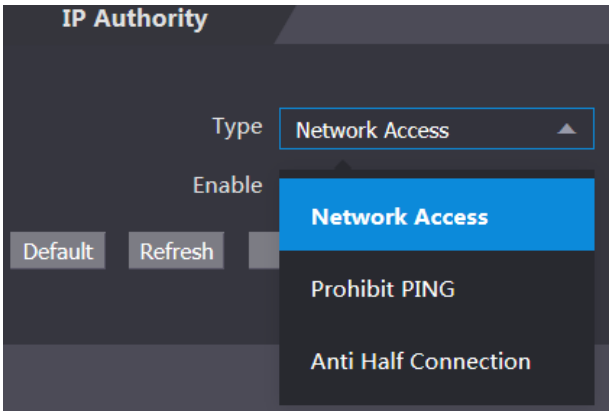
3.1.11 Safety Management

3.1.11.1 Configuring IP Authority

Step 1 Log in to the web page.

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

Figure 3-22 IP authority



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

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

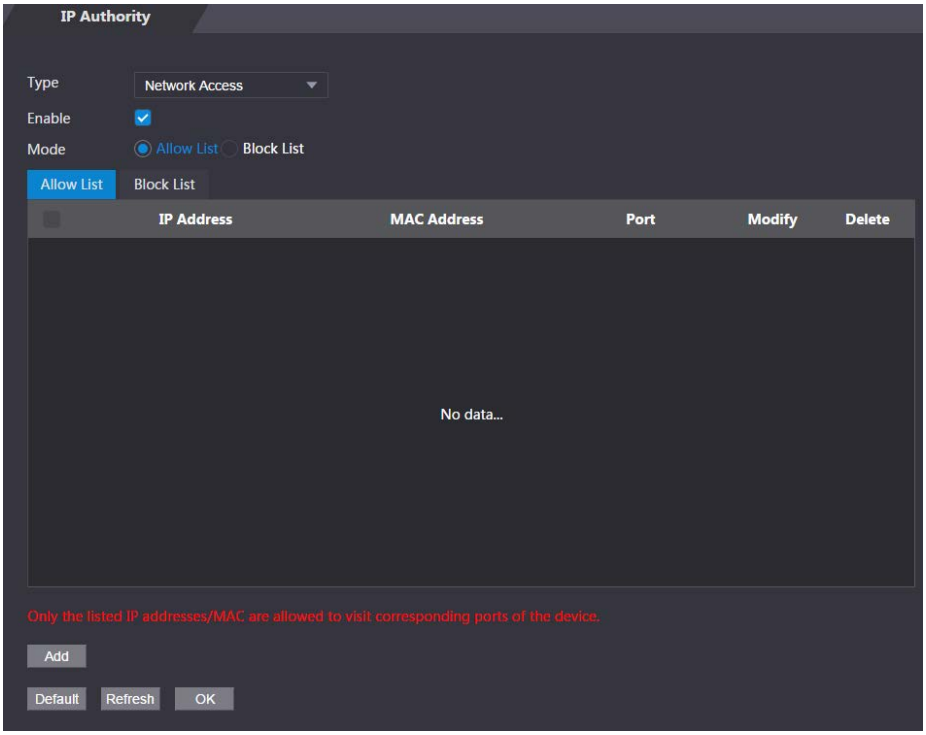
3.1.11.1.2 Network Access

Select **Network Access** in the **Type** list.

Procedure

Step 1 Select the **Enable** checkbox.

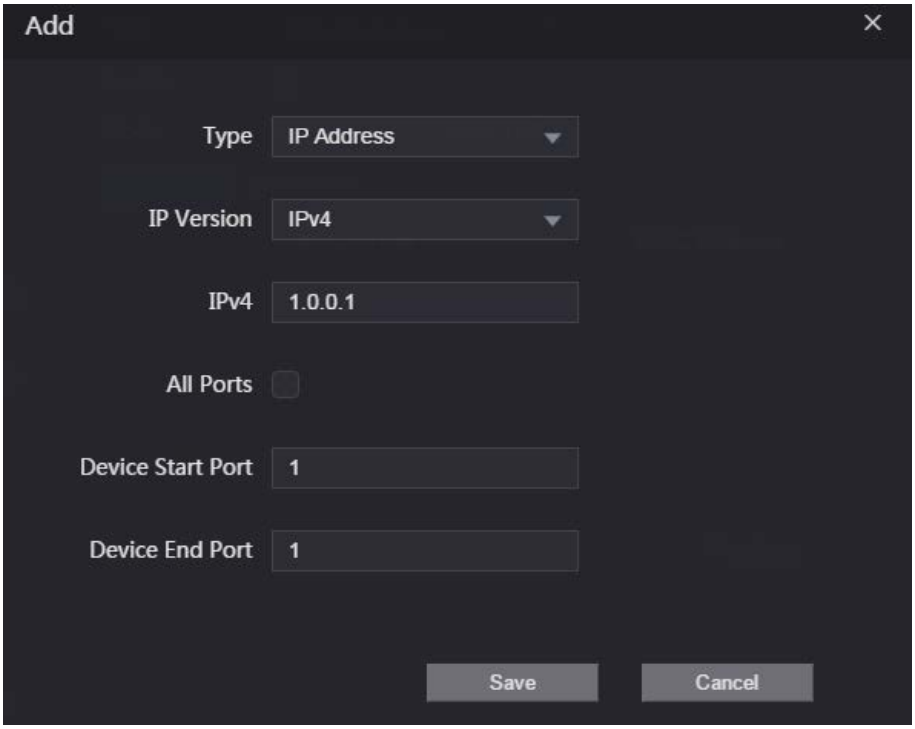
Figure 3-23 Network access



Step 2 Select **Allow List** or **Block List**.

Step 3 Click **Add**.

Figure 3-24 Add IP



Step 4 Configure parameters.

Table 3-7 Description of adding IP parameters

Parameter	Description
Type	Select the address type in the **Type** list.
IP Version	IPv4 by default.
All Ports	Select **All Ports** checkbox, and your settings will apply to all ports.

Parameter	Description
Device Start Port	If you clear **All Ports** checkbox, set the device start port and device end port.
Device End Port	

Step 5 Click **Save**, and the **IP Authority** window is displayed.

Step 6 Click **OK**.

Related Operations

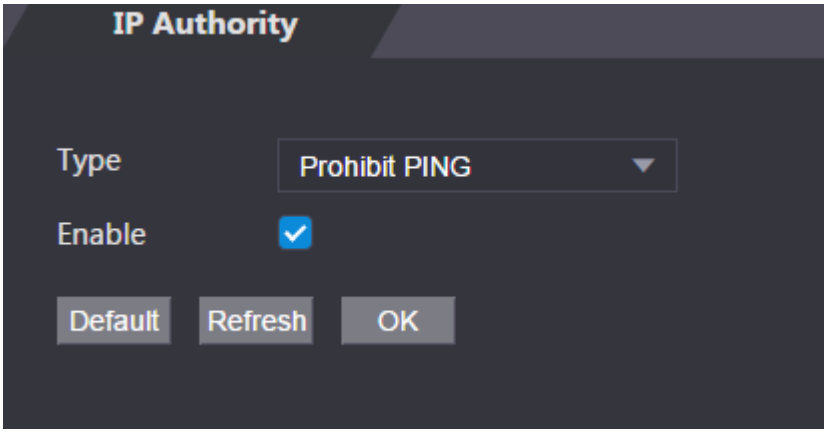
- Click to edit the allowlist or blocklist.
- Click to delete the allowlist or blocklist

3.1.11.1.3 Prohibit PING

Step 1 Select **Prohibit PING** in the **Type** list.

Step 2 Select the **Enable** checkbox.

Figure 3-25 Prohibit PING



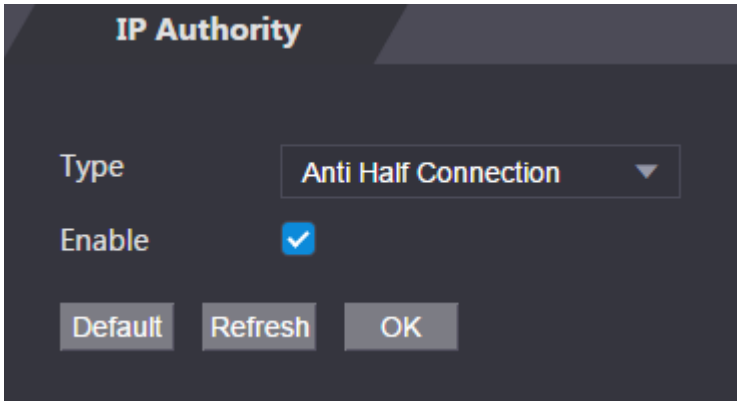
Step 3 Click **OK**.

3.1.11.1.4 Anti Half Connection

Step 1 Select the **Anti Half Connection** in the **Type** list.

Step 2 Select the **Enable** checkbox.

Figure 3-26 Network access



Step 3 Click **OK**.

3.1.11.2 Configuring System

3.1.11.2.1 System Service

Step 1 Log in to the web page.

Step 2 Select **Safety Mgmt.** > **System Service**.

Step 3 Enable or disable the system services.

Figure 3-27 System service

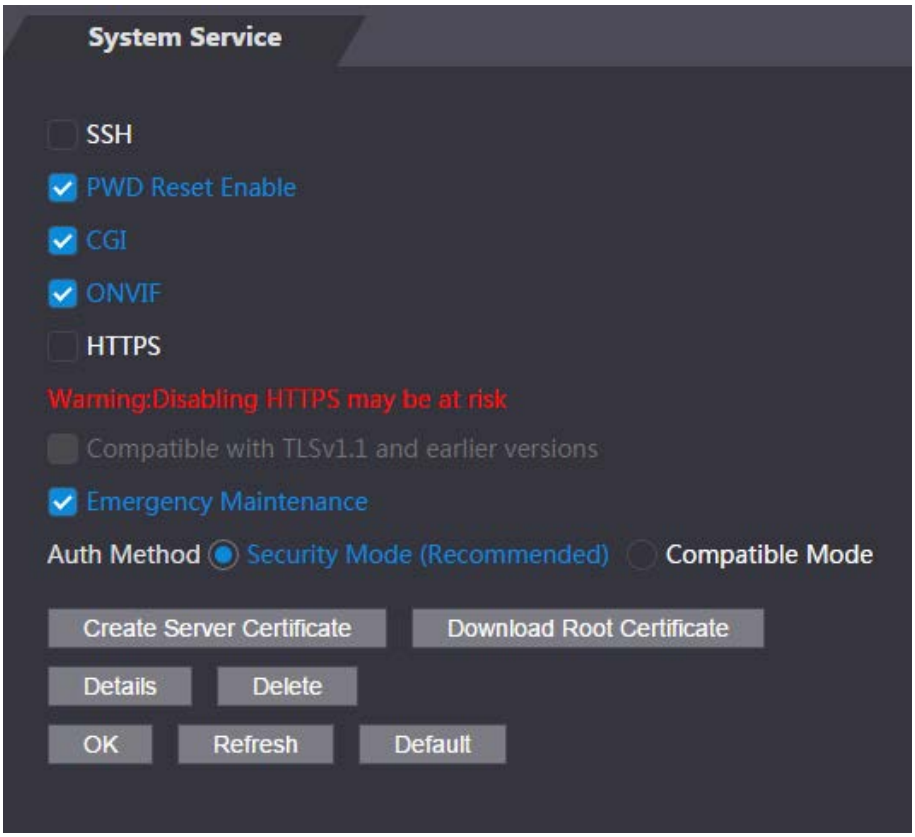


Table 3-8 Description of system service

Parameter	Description
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.
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.VR dne When CGI is enabled, CGI commands can be used. The CGI is enabled by default.
ONVIF	Enable other devices to pull video stream of the VTO through the ONVIF protocol.

Parameter	Description
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. When HTTPS is enabled, the Device will restart automatically.
Compatible with TLSv1.1 and earlier versions	Enable this function if your browser is using TLS V1.1 or earlier versions.
Emergency Maintenance	Enable it for faults analysis and maintenance.
Auth Method	● **Security Mode (recommended)**: Supports logging in with Digest authentication. ● **Compatible Mode**: Compatible with the login method of old devices.

3.1.11.2.2 Creating Server Certificate

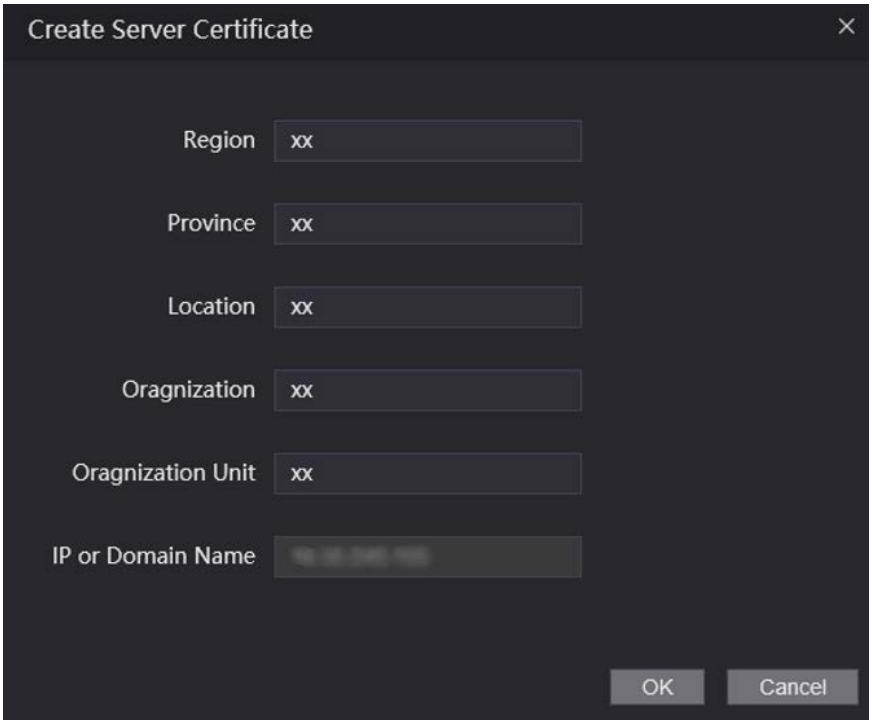
Configure HTTPS server to improve your website security with server certificate.

- If you use HTTPS for the first time or the IP address of the Device is changed, create a server certificate and install a root certificate.
- If you change PC to log in to web, you need to download and install the root certificate again on the new PC or copy it to the new PC.

Step 1 On the **System Service** page, click **Create Server Certificate**.

Step 2 Enter information and click **OK**, and then the Device will restart.

Figure 3-28 Create server certificate

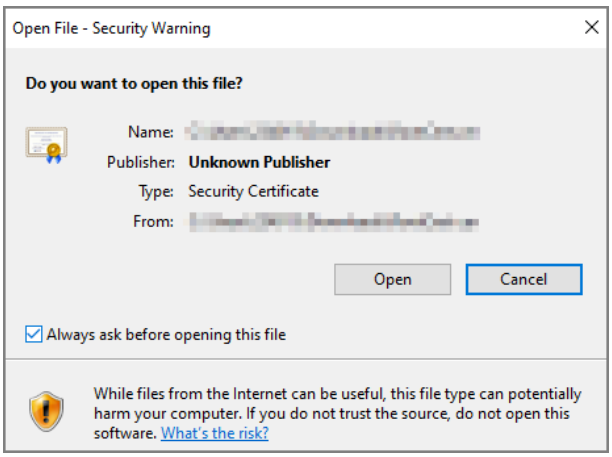


3.1.11.2.3 Downloading Root Certificate

Step 1 On the **System Service** page, click **Download Root Certificate**.

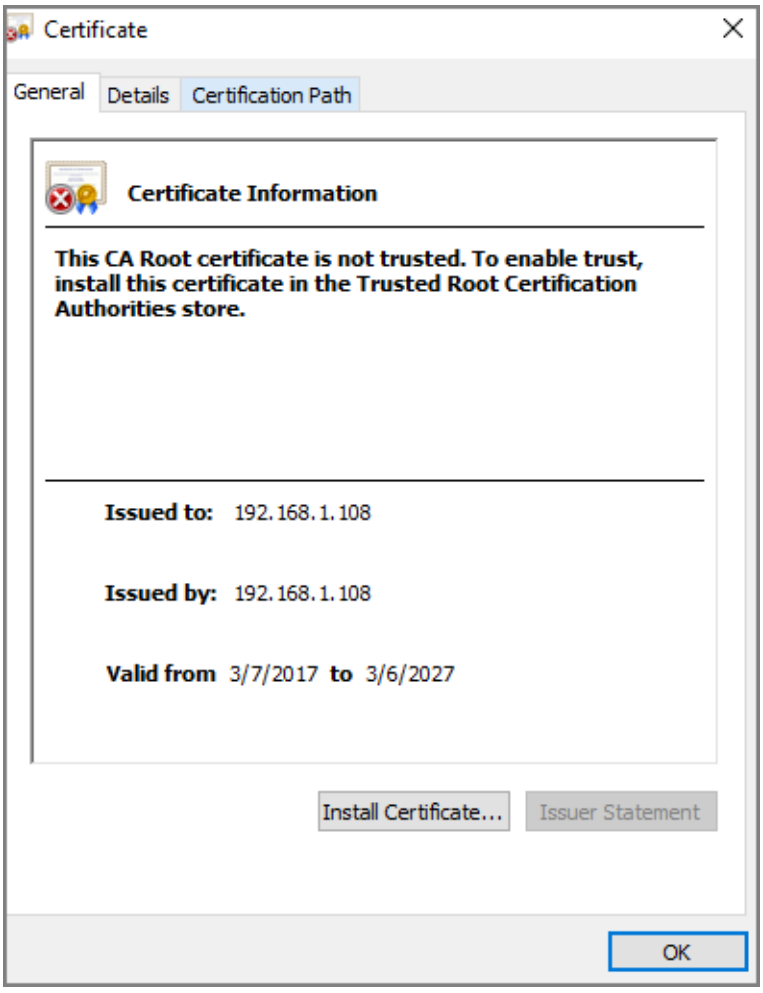
Step 2 Double-click the file that you have downloaded, and then click **Open**.

Figure 3-29 File download



Step 3 Click **Install Certificate**.

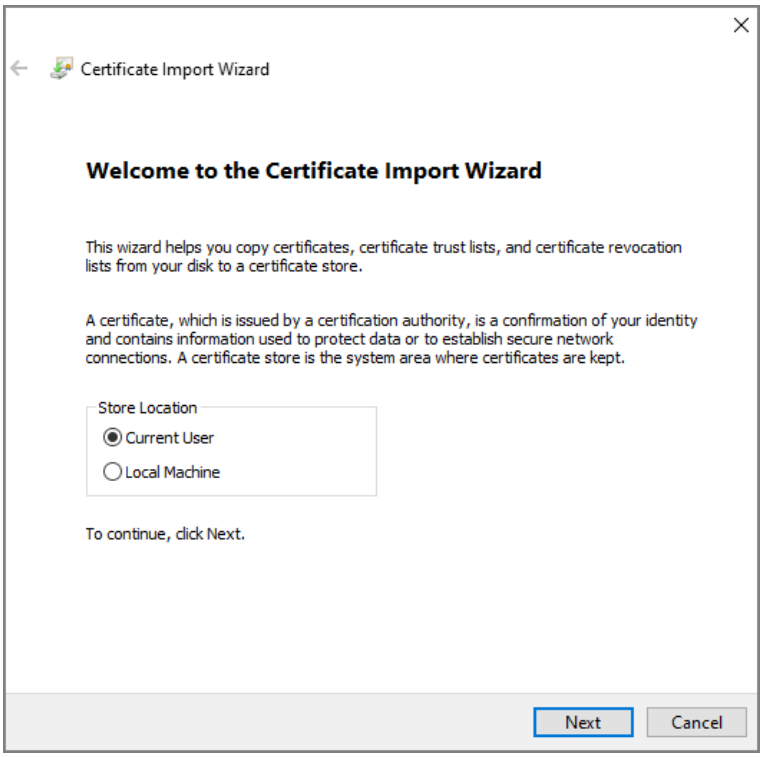
Figure 3-30 Certificate information



Step 4 Select **Current User** or **Local Machine**, and then click **Next**.

- **Current User**: Applies to the user that has logged in to the PC.
- **Local Machine**: Applies to all users that have logged in to the PC

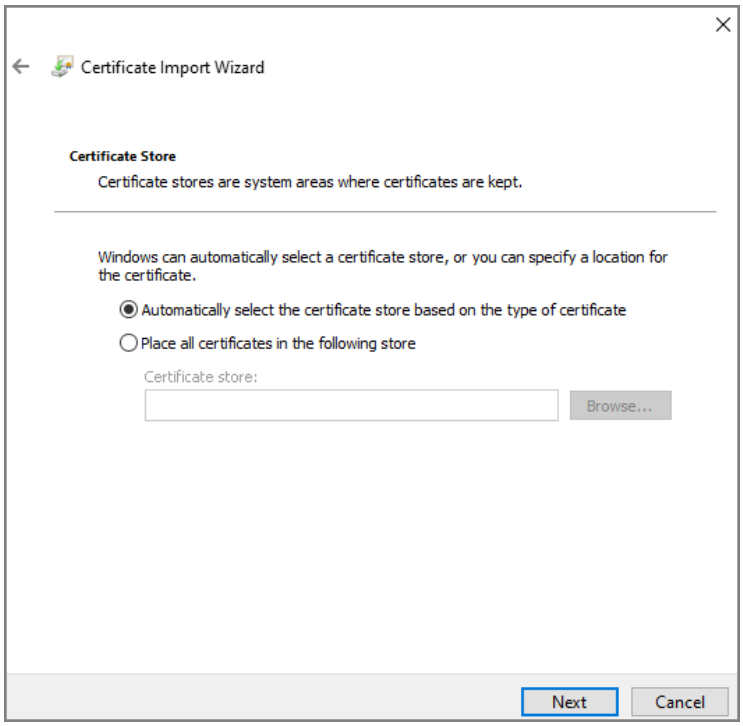
Figure 3-31 Store Location



Step 5 Select the appropriate storage location.

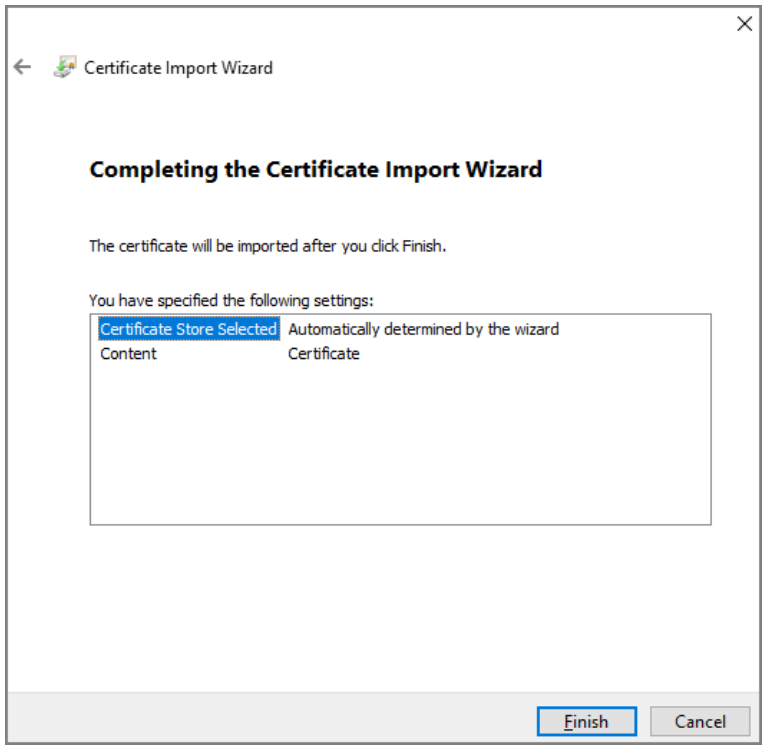
1) Select **Place all certificates in the following store**.
2) Click **Browse** to import the certificate to the **Trusted Root Certification Authorities** store, and then click **Next**.

Figure 3-32 Certificate store



Step 6 Click **Finish**.

Figure 3-33 Certificate store selected



3.1.12 User Management

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

User refers to the user who logs in to the web page.

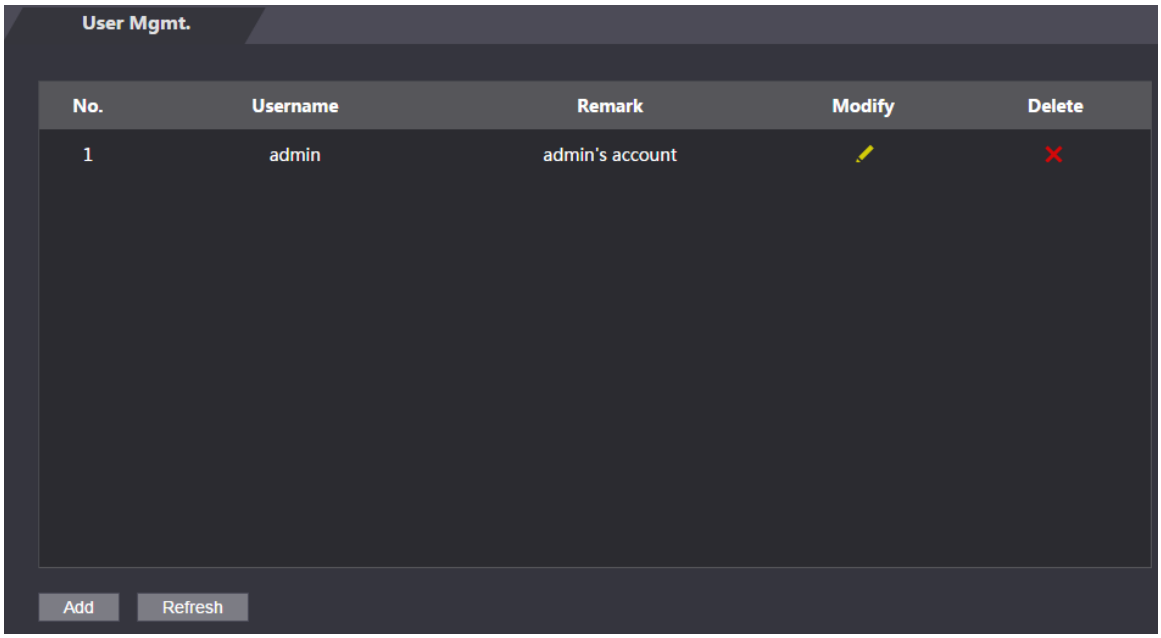
3.1.12.1 User

3.1.12.1.1 Adding Users

Step 1 Log in to the web page.

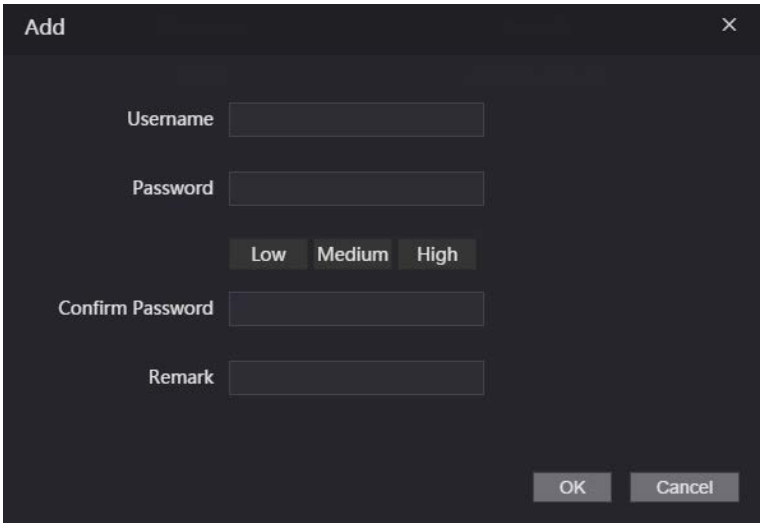
Step 2 Select **User Mgmt.** > **User Mgmt**.

Figure 3-34 User management



Step 3 Click **Add**.

Figure 3-35 Add user



Step 4 Enter username, password, confirm password, and remark.

Step 5 Click **OK**.

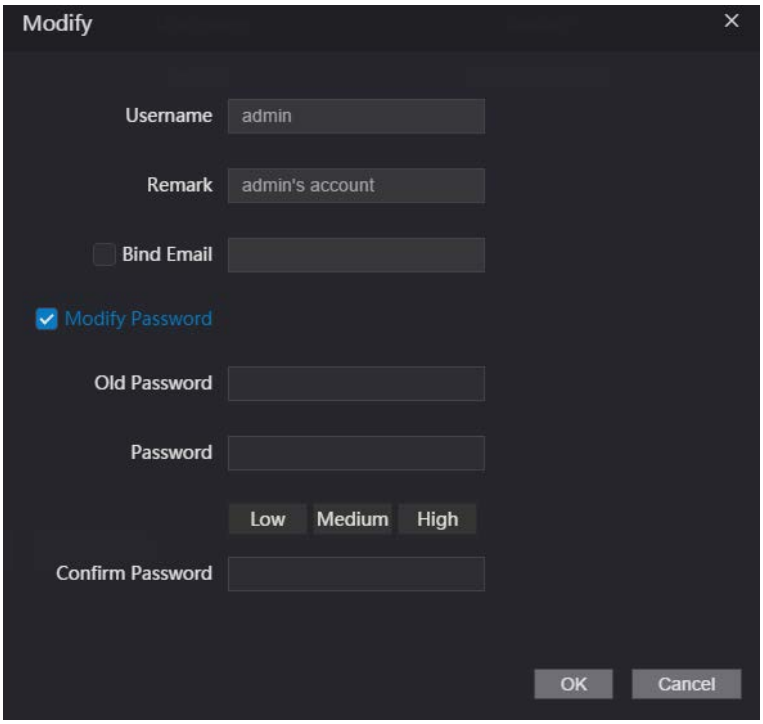
3.1.12.1.2 Changing Password

Step 1 Log in to the web page.

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

Step 3 Click .

Figure 3-36 Modify user information



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

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

Step 6 Click **OK**.

3.1.12.2 ONVIF User

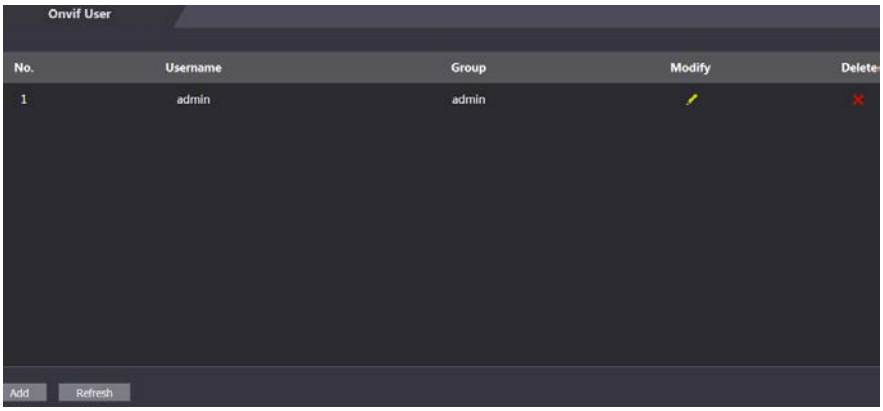
Open Network Video Interface Forum (ONVIF), a global and open industry forum that is established for the development of a global open standard for the interface of physical IP-based security products. Create ONVIF users and have their identities verified via ONVIF protocol.

3.1.12.2.1 Adding ONVIF User

Step 1 Log in to the web page.

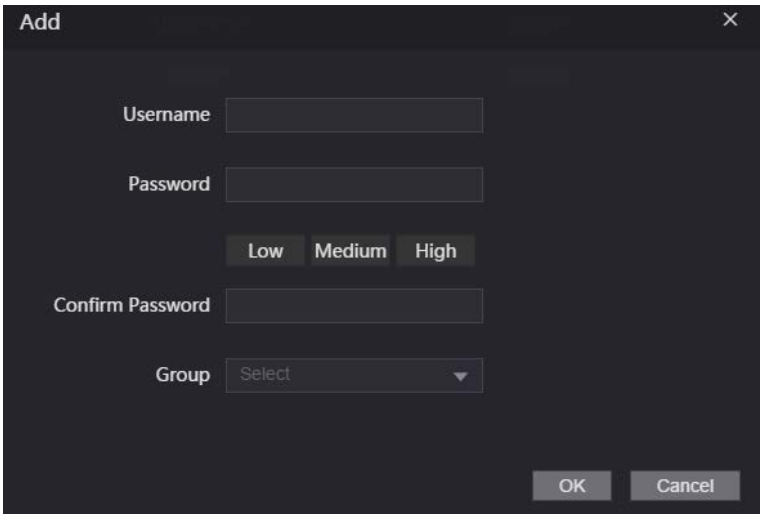
Step 2 Select **User Mgmt.** > **Onvif User**.

Figure 3-37 Onvif user



Step 3 Click **Add**.

Figure 3-38 Add ONVIF user



Step 4 Enter username, password, and confirm password.

Step 5 Select the group.

Step 6 Click **OK**.

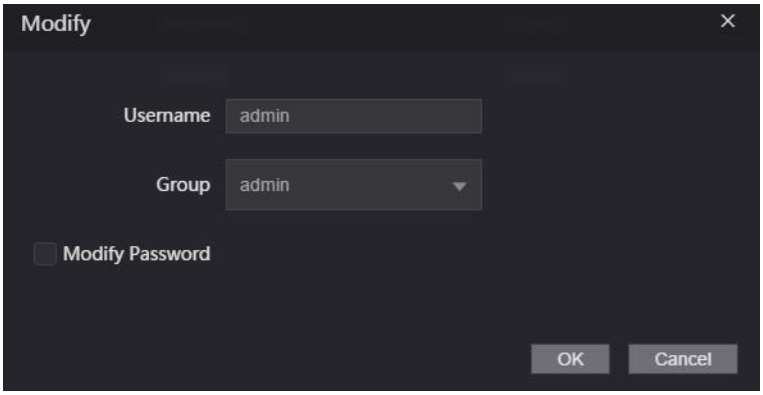
3.1.12.2.2 Changing Password

Step 1 Log in to the web page.

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

Step 3 Click .

Figure 3-39 Change the password (ONVIF user)



Step 4 Select the **Modify Password** checkbox, and then enter the old password, new password and confirm password.

Step 5 Click **OK**.

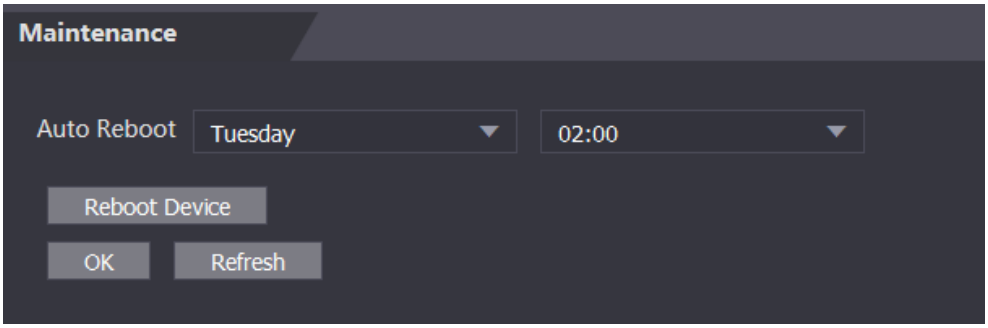
3.1.13 Maintenance

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

Step 1 Log in to the web page.

Step 2 Select **Maintenance**.

Figure 3-40 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 Device will restart immediately.

3.1.14 Configuration Management

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

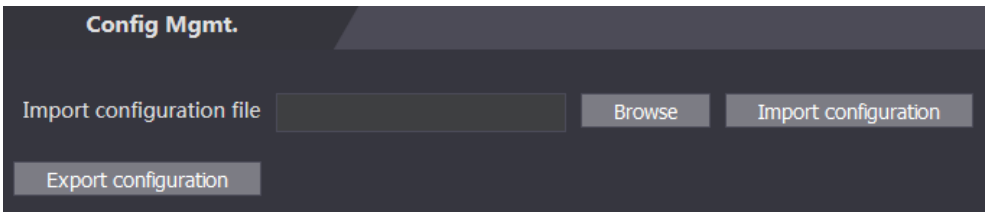
3.1.14.1 Exporting Configuration File

You can export the configuration file of the Device for backup.

Step 1 Log in to the web page.

Step 2 Select **Config Mgmt** > **Config Mgmt**.

Figure 3-41 Configuration management



Step 3 Click **Export configuration** to save the configuration file locally.

IP information of the Device will not be exported.

3.1.14.2 Importing Configuration File

You can export the configuration file from the Device to another one with the same device model.

Step 1 Log in to the web page.

Step 2 Select **Config Mgmt** > **Config Mgmt**.

Step 3 Click **Browse** to select the configuration file, and then click **Import configuration**.

The Device will restart after importing configuration file.

3.1.14.3 Setting Features

Step 1 Log in to the web page.

Step 2 Select **Config Mgmt** > **Config Mgmt**.

Step 3 In the **Features** area, set the features.

Figure 3-42 Features

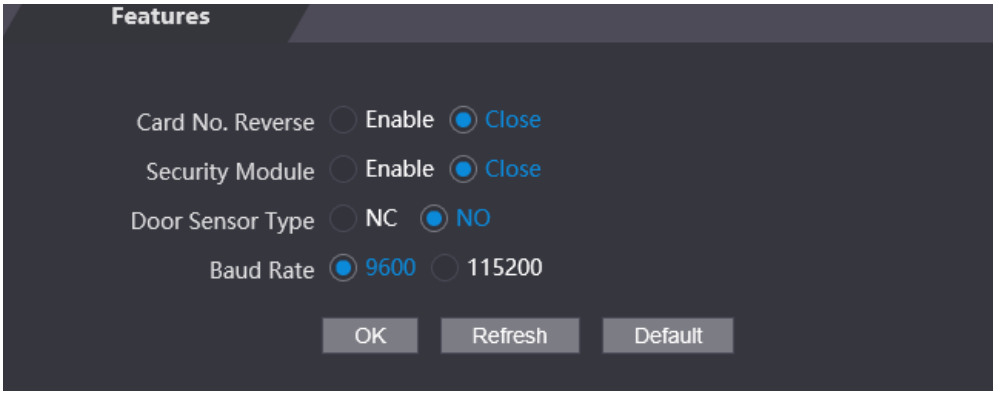


Table 3-9 Description of features

Parameter	Description
Card No. Reverse	Enable **Card No. Reverse** function, if you set Wiegand output and connect a external device, but the order of the received card number is inconsisent with that of the actual number.
Security Module	If **Security Module** is enabled, door exit button, lock and fire linkage are invalid.
Door Sensor Type	Set door sensor type: ● **NC**: Normally closed. ● **NO**: Normally open.
Baud Rate	Select baud rate according to the external device.

Step 4 Click **OK**.

3.1.14.4 Setting Fingerprint

You can set the fingerprint identity level to adjust recognition accuracy rate.

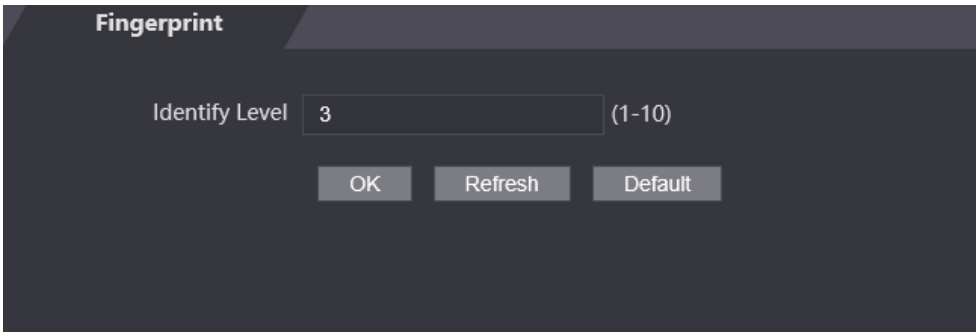
Step 1 Log in to the web page.

Step 2 Select **Config Mgmt** > **Config Mgmt**.

Step 3 In the **Fingerprint** area, set the identity level.

The higher identity level means higher recognition accuracy and higher recognition threshold.

Figure 3-43 Fingerprint identity level



Step 4 Click **OK**.

3.1.14.5 Restoring Factory Defaults

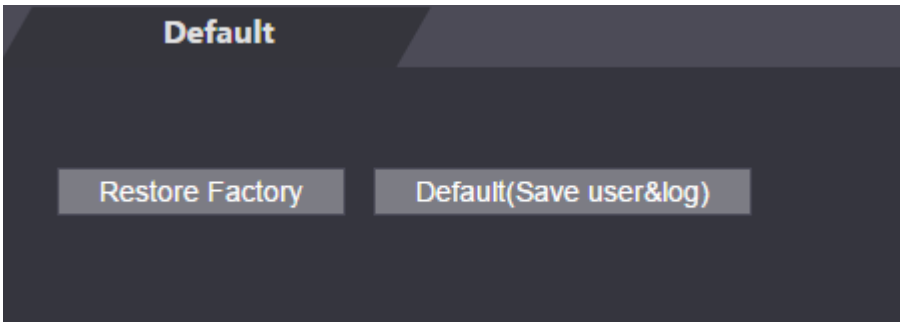
⚠

Restoring the Device to default configurations will cause data loss. Please be advised.

Step 1 Log in to the web page.

Step 2 Select **Config Mgmt.** >**Default**.

Figure 3-44 Default



Step 3 Restore factory defaults if necessary.

- **Restore Factory:** Resets configurations of the Device and deletes all data.
- **Restore Factory (Save user & log)**: Resets configurations of the Device and deletes all data except for user information and logs.

3.1.15 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.

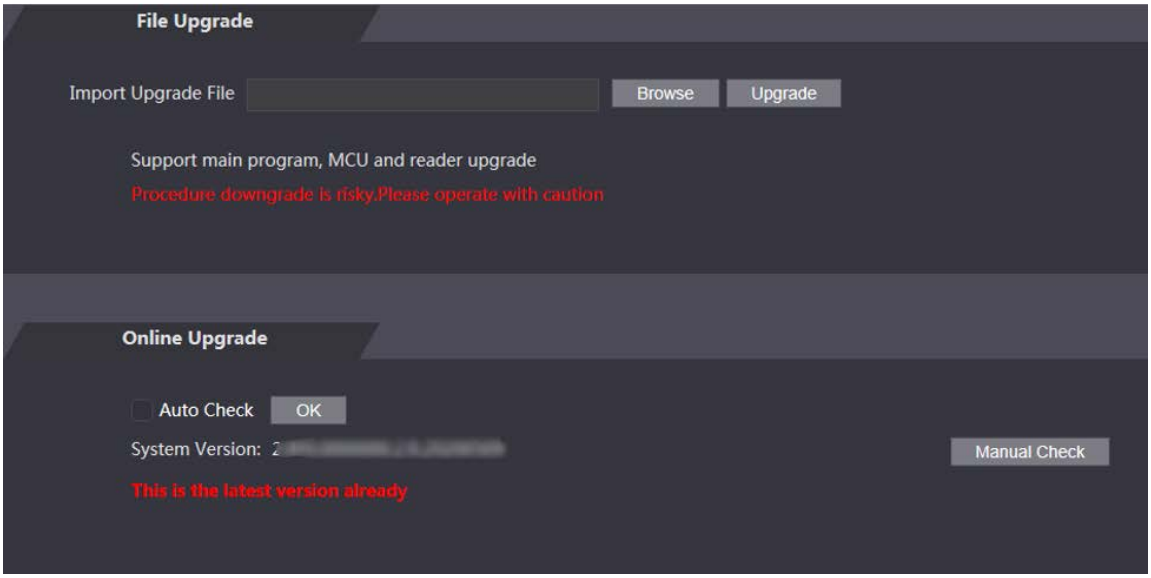
⚠

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

Step 1 Log in to the web page.

Step 2 Select **Upgrade**.

Figure 3-45 Upgrade



Step 3 Select 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 upgrading 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 Device will restart after the upgrading completes.

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

3.1.16 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.

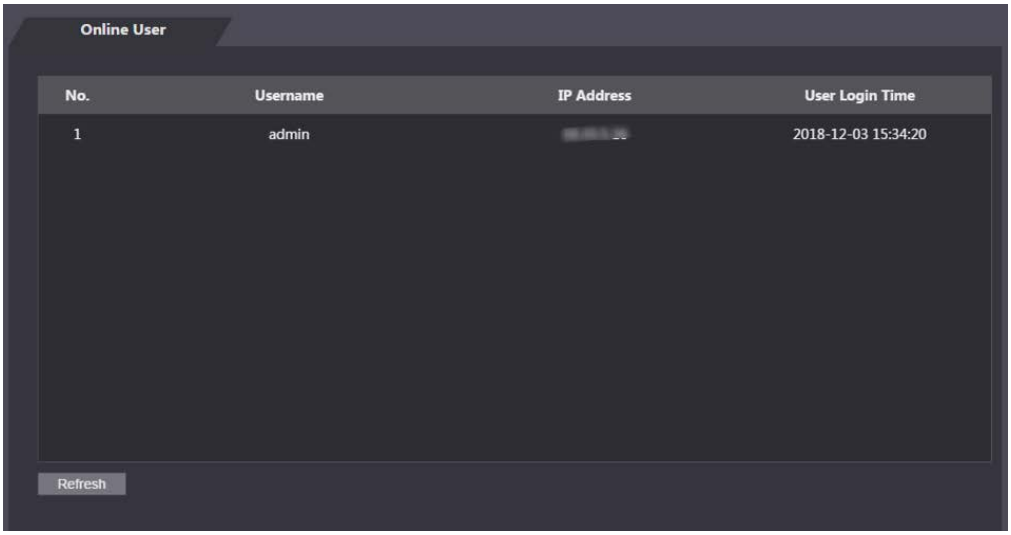
3.1.17 Viewing Online User

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 3-46 Online user



3.1.18 Viewing System Logs

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

3.1.18.1 System Logs

View and search for system logs.

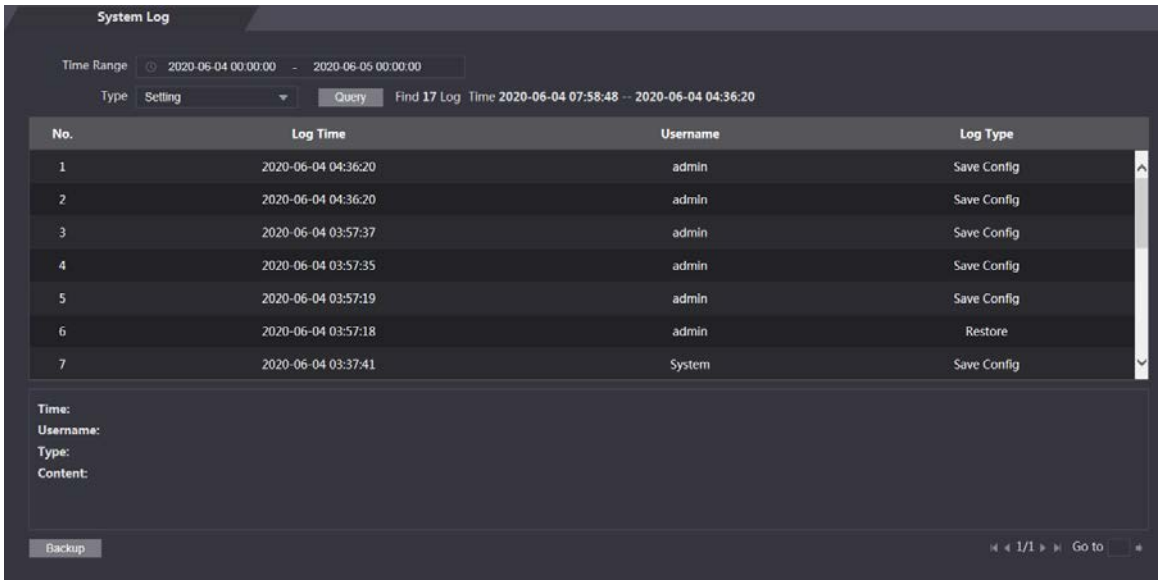
Step 1 Log in to the web page.

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 3-47 Search for logs



3.1.18.2 Admin Logs

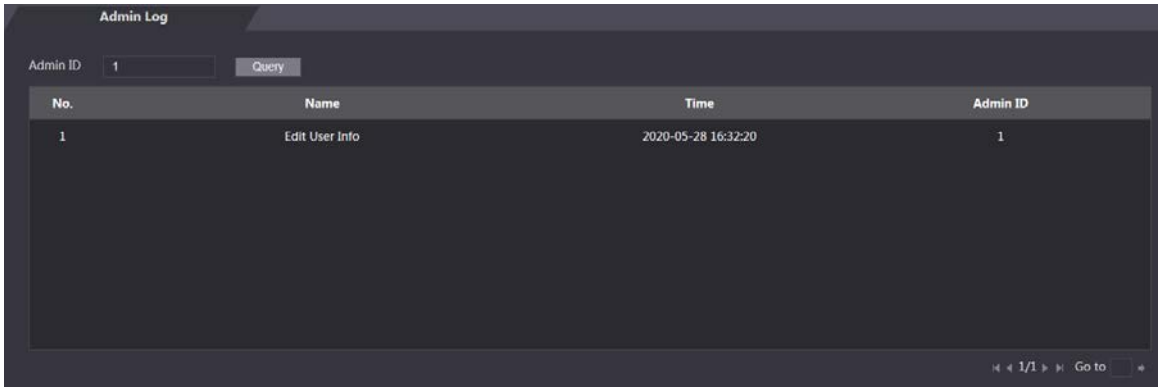
Search for admin logs by using admin ID.

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 3-48 Admin log



3.1.18.3 Unlock Records

Search for and export unlock records.

Step 1 Log in to the web page.

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

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

Step 4 Click **Export Data** to download the results.

3.1.19 Logging Out

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

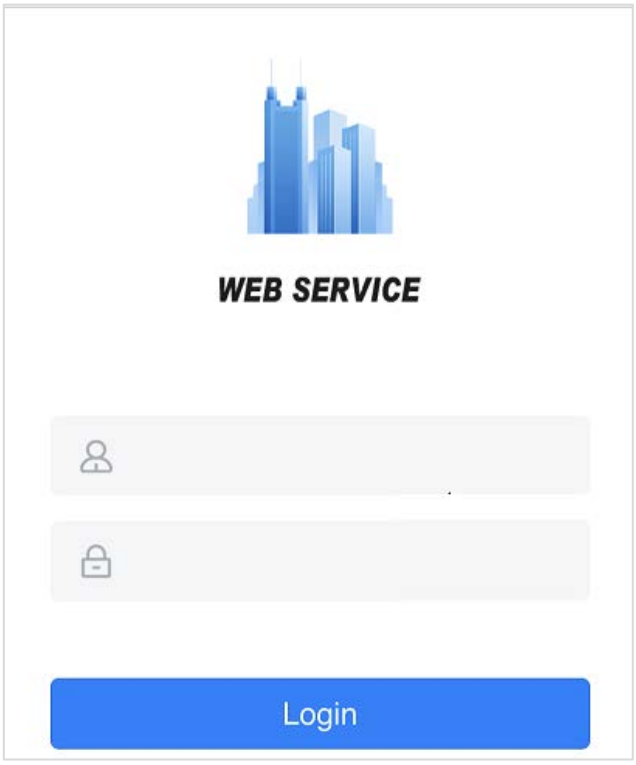
3.2 Web on Phone

Make sure the Device is on the same LAN as your phone. Connect the Device to your phone hotspot or connect the Device and your phone to the same router.

Only certain parameters can be configured on the web portal if you log in on a phone.

Step 1 Go to the IP address (192.168.1.108 by default) of the Device in the browser.

Figure 3-49 Login



Step 2 Enter the user name and password.

The default administrator name is admin, and the password is the one you set during initialization. We recommend you to change the administrator password regularly to increase security.

Step 3 Click **Login**.

4 SmartPSS AC Configuration

This chapter introduces how to manage and configure the Device by using SmartPSS AC. For details, see the user's manual of SmartPSS AC.

Use Smart PSS AC as an example for configurations. The windows in the user manual are only for reference, and might differ from the actual product.

4.1 Logging in

Step 1 Install SmartPSS AC.

Step 2 Double-click , and then follow the prompts to complete initialization and log in.

4.2 Adding Devices

You need to add the Device to SmartPSS AC. You can in batch or individually.

4.2.1 Adding Individually

Step 1 Log in to SmartPSS AC.

Step 2 Click **Device Manager**.

Step 3 Click **Add** on the **Device Manager** page.

Step 4 Enter the required information.

Figure 4-1 Enter device information

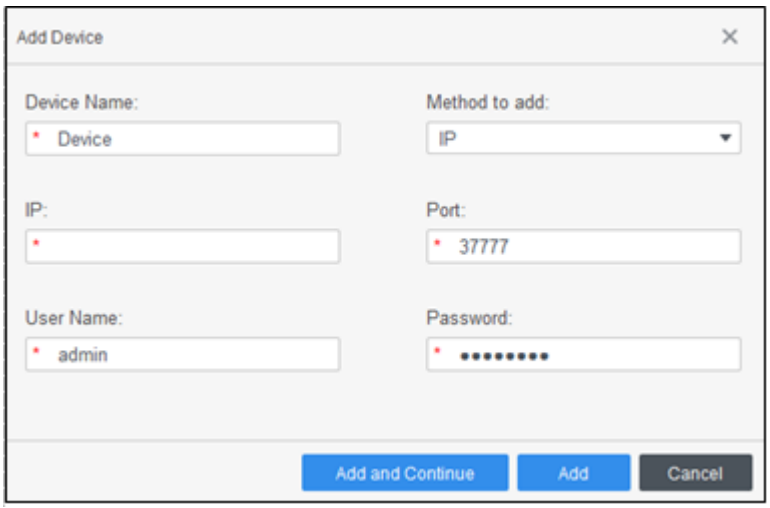


Table 4-1 Description of device parameters

Parameter	Description
Device Name	Enter a name of the device. We recommend naming the device according to its installation area.
Method to add	Select **IP** to add device through IP address.
IP	Enter IP address of the device.
Port	The port number is 37777 by default.
User Name, Password	Enter the username and password of the device.

Step 5 Click **Add**, and then you can see the added device on the **Devices** page.

The device automatically logs in after being added. **Online** is displayed after successful login.

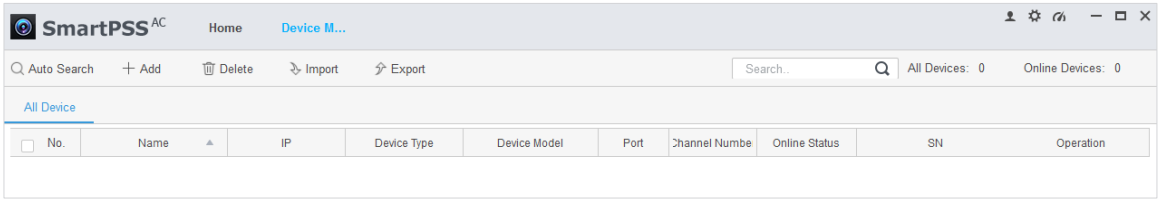
4.2.2 Adding in Batch

We recommend the auto-search function when you add devices in batch. The devices you add should be on the same network segment.

Step 1 Log in to SmartPSS AC.

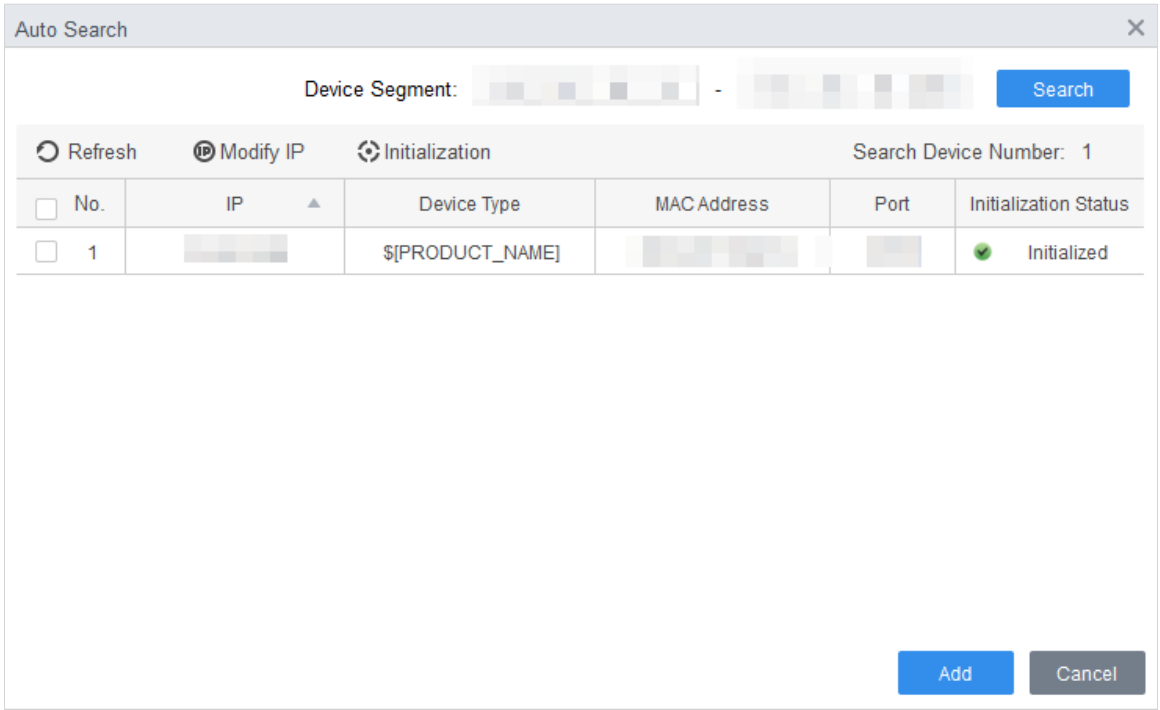
Step 2 Click **Device Manager**.

Figure 4-2 Devices



Step 3 Click **Auto Search**.

Figure 4-3 Auto search



Step 4 Enter the network segment, and then click **Search**.

A device list will be displayed.

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

Step 5 Select devices that you want to add to the SmartPSS AC, and then click **Add**.

Step 6 Enter the username and the password of the device.

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

- The device automatically logs in after being added. **Online** is displayed after successful login.

Related Operation

- : Edit the device information, including device name, IP address, port number, username, and password.
  You can also double-click the device to edit its information.
- : Configure the device. You can set up the time, update the device, restart the device, and extract user information or attendance records from the device.
- and : Log in to and out of the device.
- : Delete the device.

4.3 User Management

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

4.3.1 Setting Card Type

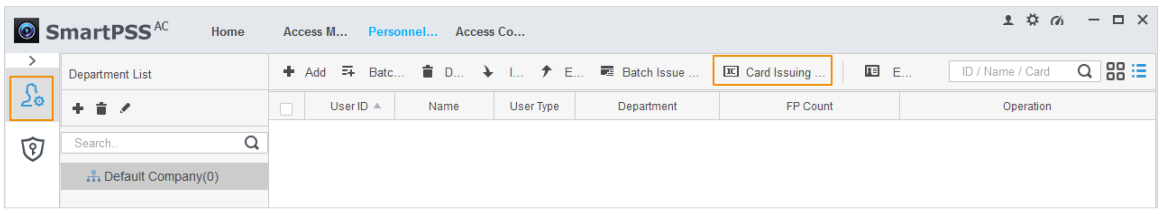
Before issuing card, set card type first. For example, if the issued card is ID card, set type to ID card.

Card types must be the same as card issuer types; otherwise, card numbers cannot be read.

Step 1 Log in to SmartPSS AC.

Step 2 Click **Personnel Manager**.

Figure 4-4 Personnel manager

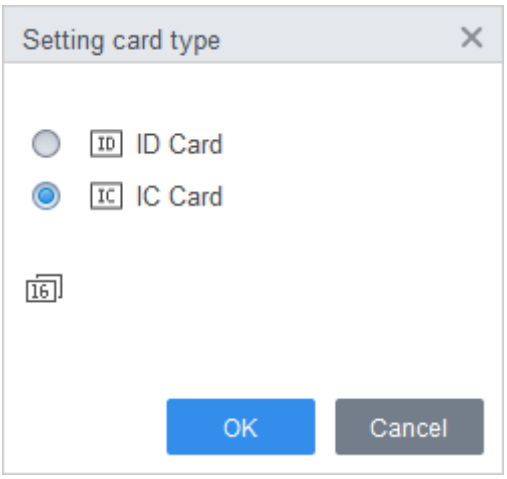


Step 3 Click , and then click .

Step 4 On the **Setting Card Type** window, select a card type.

Step 5 Click to select the display method of card number in decimal or in hex.

Figure 4-5 Setting card type



Step 6 Click **OK**.

4.3.2 Adding User

4.3.2.1 Adding Individually

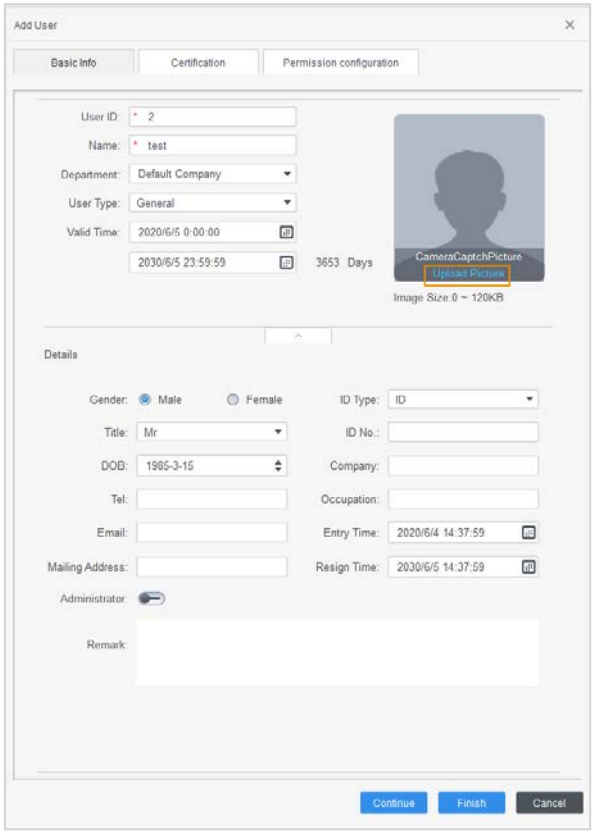
You can add users one by one manually.

Step 1 Log in to SmartPSS AC.

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

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

Figure 4-6 Add basic information



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

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

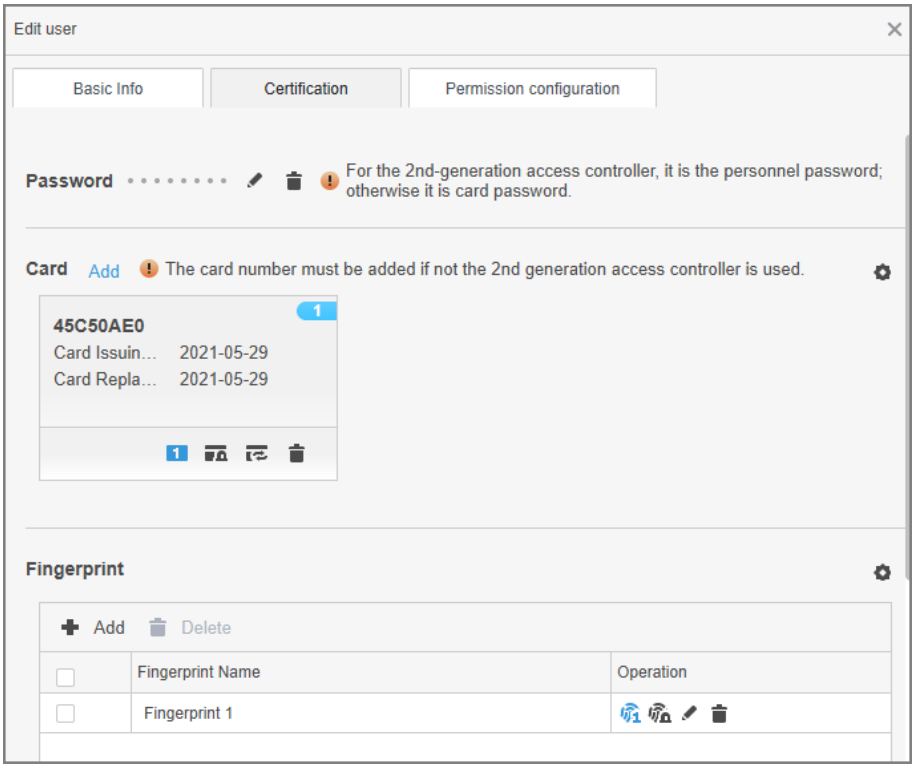
The card number can be read automatically or entered manually. To read the card number automatically, select a card reader, and then place the card on the card reader.

1) Click , set **Card Reader** to **Device**, and then select the device you add from **Device**.
2) Click **Add**, swipe a card on the device, and then the card number will be displayed.
3) Click **OK**.
4) (Optional) After adding a card, you can set the card to main card or duress card, or replace the card with a new one, or delete the card.

- Configure fingerprint.

1) Click , set **Fingerprint Collector** to **Device**.
2) Click **Add** and press your finger on the scanner three times continuously.

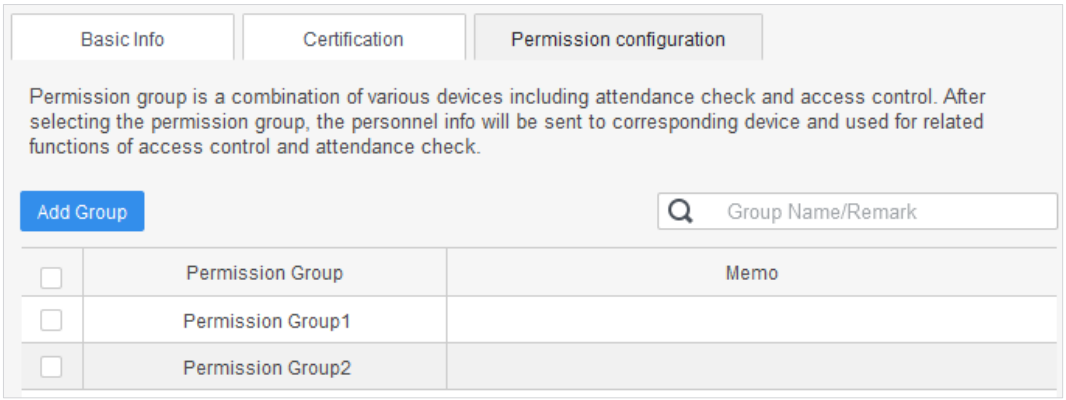
Figure 4-7 Add password, card, and fingerprint



Step 5 Configure permissions for the user.

For details, see "4.4 Assigning Permissions".

Figure 4-8 Permission configuration



Step 6 Click **Finish**.

4.3.2.2 Adding in Batch

You can add users in batches.

Step 1 Log in to SmartPSS AC.

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

Step 3 Select **Device** from **Device**, and then select the device that you add.

Step 4 Configure the following parameters.

- **Start No.**: The user ID starts with the number you defined.
- **Quantity**: The number of users you want to add.
- **Department**: Select the department that the user belongs to.

- **Effective Time** and **Expired Time**: The users can unlock the door within the defined period.

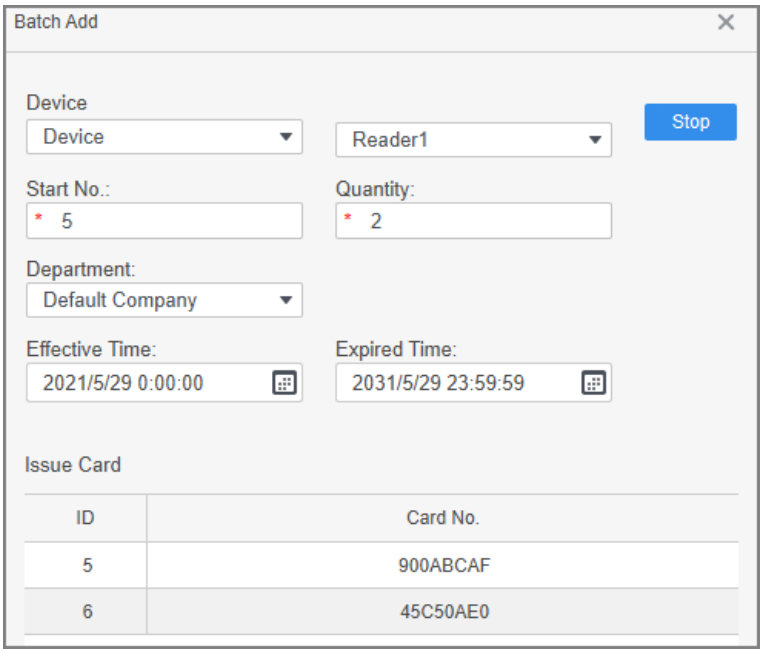
Step 5 Click **Issue**.

The card number will be read automatically.

Step 6 Click **Stop** when you finish issuing cards.

Step 7 Click **OK**.

Figure 4-9 Add users in batches



Step 8 In the user list, click to edit the information of the added users.

4.4 Assigning Permissions

Add devices to a permission group, and then users in the group can unlock corresponding doors.

Step 1 Log in to SmartPSS AC.

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

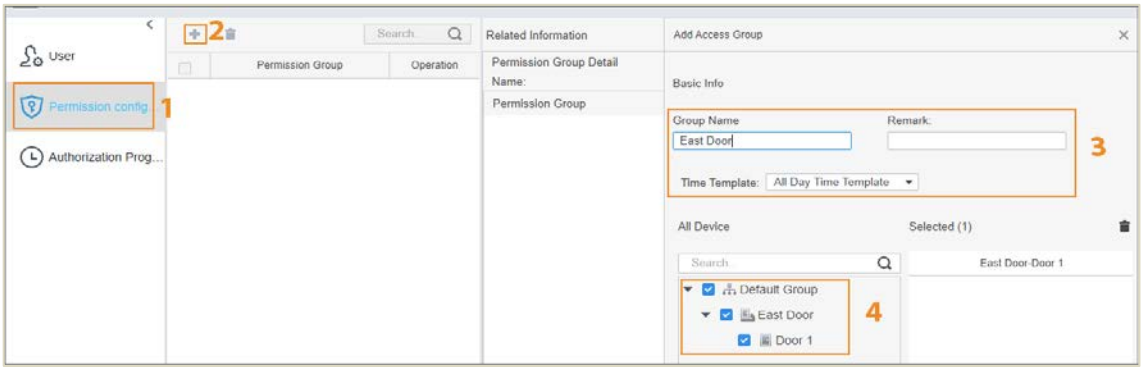
Step 3 Click .

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

Step 5 Select the devices.

Step 6 Click **OK**.

Figure 4-10 Create a permission group



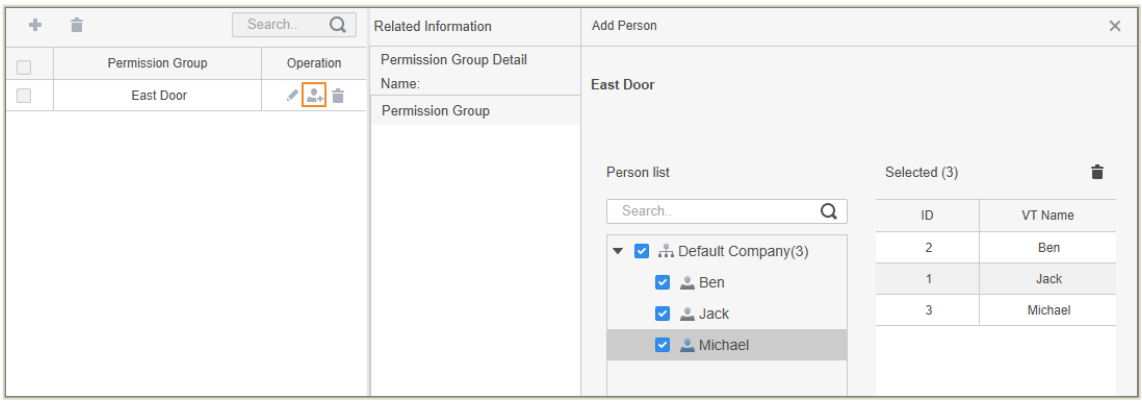
Step 7 Click of the permission group you added.

Step 8 Select the users you want to add to the permission group.

Step 9 Click **OK**.

Users in the permission group can swipe their cards, or use other unlock methods to unlock the door.

Figure 4-11 Add users to a permission group



Appendix 1 Fingerprint Registration Instructions

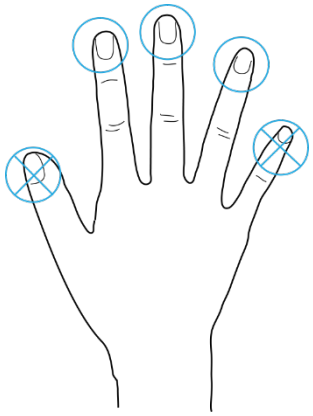
When you register the fingerprint, pay attention to the following points:

- Make sure that your fingers and the scanner surface are clean and dry.
- Press your finger on the center of the fingerprint scanner.
- Do not put the fingerprint sensor in a place with intense light, high temperature, and high humidity.
- If your fingerprints are unclear, use other unlocking methods.

Fingers Recommended

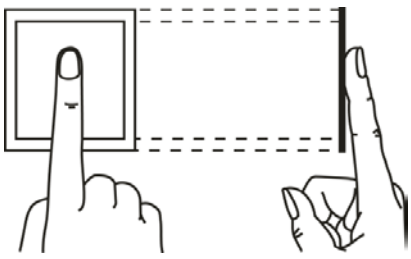
Forefingers, middle fingers, and ring fingers are recommended. Thumbs and little fingers cannot be put at the recording center easily.

Appendix Figure 1-1 Recommended fingers

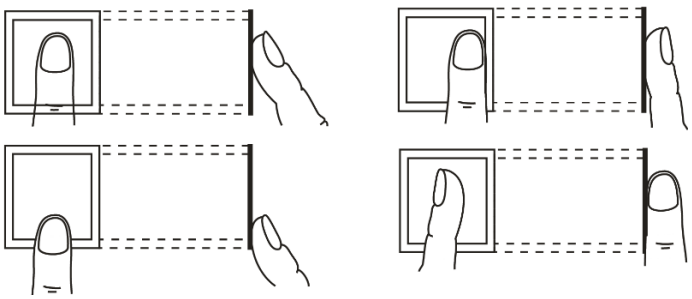


How to Press Your Fingerprint on the Scanner

Appendix Figure 1-2 Correct placement



Appendix Figure 1-3 Wrong placement



Appendix 2 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:

2. **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.

3. **Change Passwords Regularly**

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

4. **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.

5. **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.

6. **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.

7. **Enable HTTPS**

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

8. **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.

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 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.

13. **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.

14. **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.