

FCS525 Product Manual



Disclaimer

Before using the product, carefully read all contents of this "FCS525 Product Manual" to ensure safe and effective operation. Do not disassemble the product or remove the warranty seal on the device. Otherwise, Suzhou Fanxi Technology Co., Ltd. shall not bear any responsibility for warranty or product replacement.

Images in this manual are for reference only. If any image differs from the actual product, the physical product shall prevail. Suzhou Fanxi Technology Co., Ltd. reserves the right to modify this documentation at any time without prior notice for product upgrades and updates.

Users assume all risks associated with product usage. To the maximum extent permitted by applicable law, Suzhou Fanxi Technology Co., Ltd. shall not be liable for any damages or risks arising from the use or inability to use the product, including but not limited to:

1. Direct or indirect personal injury
2. Loss of business profits
3. Interruption of trade
4. Loss of commercial information
5. Any other economic losses

All rights of interpretation and revision of this manual belong to Suzhou Fanxi Technology Co., Ltd.

Revision History

Revision Date	Revision Version	Designated Personnel	Change Content
2025.07.08	V1.0		Initial Version Release

1. Preface

Thank you for choosing the FCS525 access control device provided by Suzhou Fanxi Technology Co., Ltd. Carefully reading this document will help you understand the device's features, functionalities, and quickly master its installation and operation methods.

Our company shall not be liable for any property damage or personal injury caused by improper user operation. Users must develop corresponding products in accordance with the technical specifications and reference designs provided in this manual, while adhering to general safety precautions for mobile device usage.

Unless otherwise stated, our company reserves the right to modify the content of this manual as needed to accommodate technological advancements.

1.1. Product Introduction

FCS525 Smart Access Control Terminal utilizes an IML laminated panel with an aluminum alloy frame, featuring a slim 6.8mm thickness. Its surface employs a soft-touch coating process, while the device achieves IP55 protection rating to ensure reliable performance in complex outdoor environments. The terminal integrates high-sensitivity touch keys, doorbell functionality, tamper-proof alarm, and an audible-visual alert system. Supporting dual-mode wireless connectivity (Bluetooth + WiFi), it meets diverse smart application scenario requirements.

1.2. Product Features

- ✓ The product features an ultra-slim 6.8mm design with an electroplated aluminum alloy frame, IML-injected housing, and soft-touch panel, achieving both refined aesthetics and rugged durability.
- ✓ Standard access methods include IC card swiping, Bluetooth-enabled mini-program unlocking, touch-key

password entry, and relay-triggered access.

- ✓ Tamper-evident alarms activate upon unauthorized disassembly.
- ✓ Wiegand 26/34 output (VG-D0/VG-D1 terminals) supports integration with third-party access controllers.
- ✓ Designed for standard 86 junction box installation with DC12V power supply for effortless deployment.
- ✓ IP55-rated housing effectively resists dust ingress and water splashes for reliable operation in diverse environments.

1.3. Important Precautions

1. Disassembly & Modification

Do not disassemble or modify device hardware without authorization. Our company shall not provide warranty coverage for damages caused by such actions.

2. Abnormal Conditions

Keep away from fire sources. If detecting unusual odors, overheating, or smoke, immediately power off the device, unplug it from the AC outlet, and contact your product distributor or our customer service center.

3. Fall Damage

If the device is damaged due to falling, power it off immediately and contact your product distributor or our customer service center.。

4. Placement

Do not place the device on unstable or uneven surfaces to prevent fall damage. Avoid locations with excessive humidity or dust to eliminate risks of electric leakage or fire.

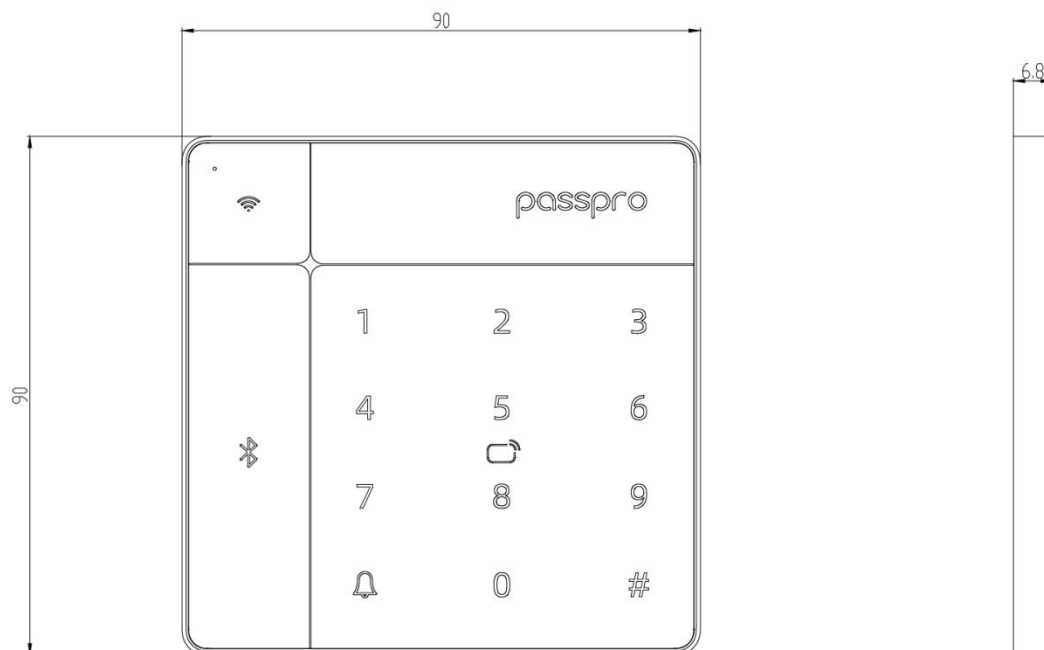
2. Physical Structure

2.1. Product Rendering



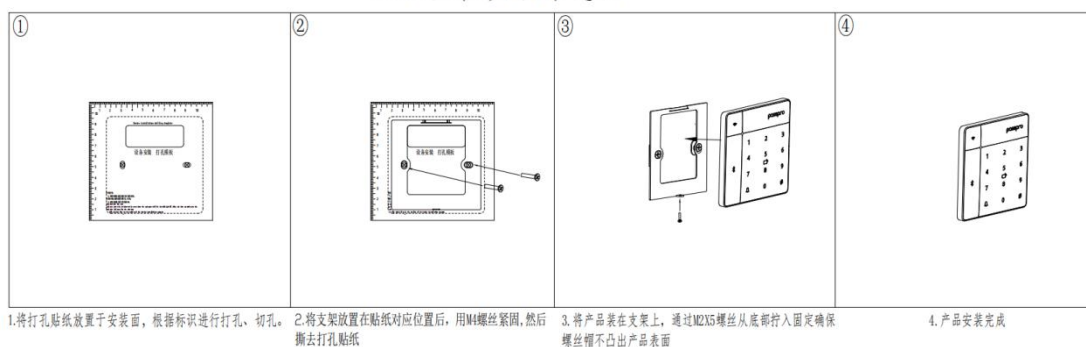
2.2. Product Dimensions

Note: All dimensions in the following diagrams are in millimeters (mm).

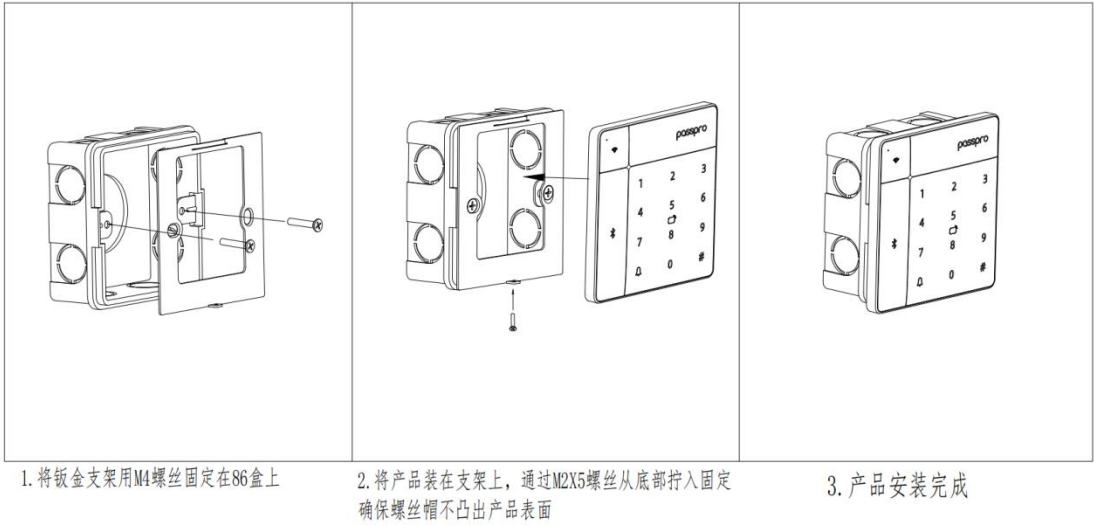


2.3. Installation Diagram

S430壁挂安装示意图



S430-86盒安装示意图



3. Product Specifications

3.1. Technical Specifications

Category	Configuration/Feature	Description/Parameter
Overall Machine	Product Type	Card-swiping access control
	Product Model	FCS525
	Material	Front shell: IML film-coated panel, aluminum alloy frame
		Rear shell bracket: Sheet metal bracket
External Interfaces/Lead-out Wires	Electrical Interface	Power supply, Wiegand, doorbell control, 30V/1A relay
	Physical Interface	2.0mm pitch bar connector
Password Buttons	Capacitive Touch	12-key capacitive touch, 0-9 digits, "doorbell", "#"

Category	Configuration/Feature	Description/Parameter
ID Card Swiping	Dummy Password	8-digit dummy password
	Distance	0~5cm (ordinary cards, mobile phones) 0~3cm (ID cards)
	Frequency	13.56MHz
	Distance	0~3cm
	Frequency	125KHz
Overall Protection	Waterproof and Dustproof	Regular model: IP55
	ESD Protection	Contact 8KV, air 10KV
	Surge	Regular standard
Environmental Characteristics	Operating Temperature	-40~80℃
	Storage Temperature	-40~85℃
	Humidity	10%~90%
Others	Configuration Method	Card-swiping configuration/Bluetooth configuration
	Environmental Protection	RoSH
	Application Scenarios	Indoor, outdoor
Installation Method	Wall-mounted	Supports 86-box, flat wall
	Gate	Requires the gate opening size to be larger than the device size, using internal installation

4. WEB End User Instructions

4.1. Platform Registration and Login

4.1.1. Registration and Login via the Register Button

Step 1: Click the [Register] button on the login page to enter the registration page.

Step 2: You can choose to register with a mobile phone number or email. Enter the correct mobile phone number/email, click to get the verification code, and accurately fill in the obtained verification code.

Step 3: Enter the password and confirm the password, check to agree to the agreement policy, and click [Confirm].

Step 4: Enter the organization creation page, enter the organization name, and click [Confirm].

Step 5: The page jumps to the office homepage, indicating successful registration and login.

Step 1



Language: English

Login

Account
14751694209

Password

Register [Forgot password?](#)

Login

☒ I have read and agree to "Duxian Office Access Pass Service Agreement", "Duxian Office Access Pass Privacy Policy", "Duxian IoT Service Agreement" and "Duxian IoT Privacy Policy"

step 2



← Register

Phone Email

Username

* Phone

* Verification code [Get](#)

* Password

* Confirm password

Confirm

☒ I have read and agree to "Duxian Office Access Pass Service Agreement", "Duxian Office Access Pass Privacy Policy", "Duxian IoT Service Agreement" and "Duxian IoT Privacy Policy"

step 3



dxiot.com

多弦物联

Register

Phone Email

Username Admin

* Phone 18888888888

* Verification code 99999 [Get](#)

* Password *****

* Confirm password *****

[Confirm](#)

☒ I have read and agree to "Duokian Office Access Pass Service Agreement", "Duokian Office Access Pass Privacy Policy", "Duokian IoT Service Agreement" and "Duokian IoT Privacy Policy".

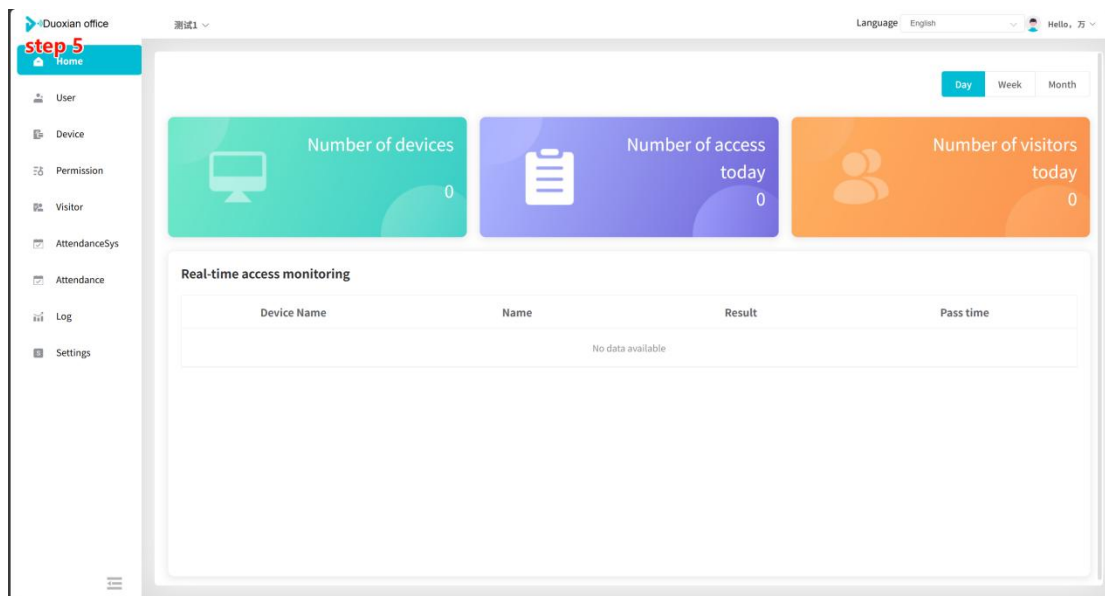
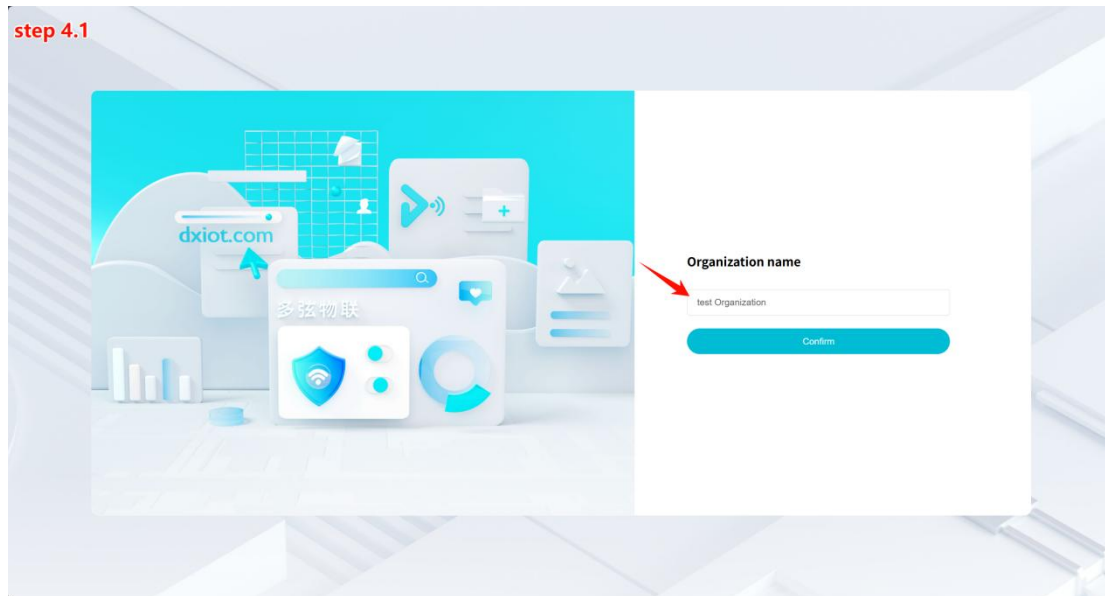
step 4



dxiot.com

多弦物联

[Create organization](#)

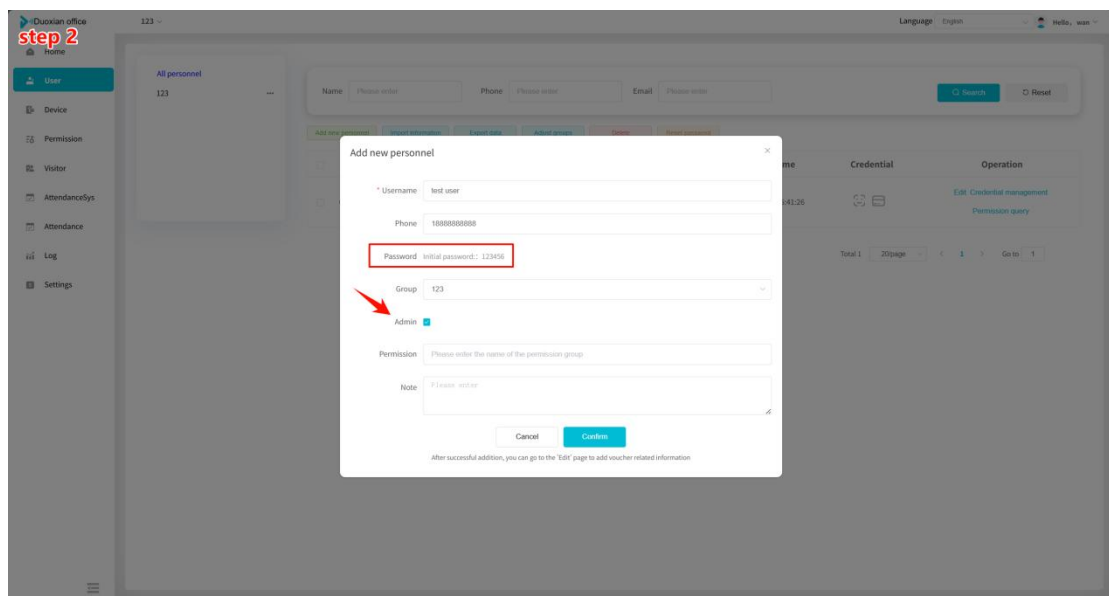
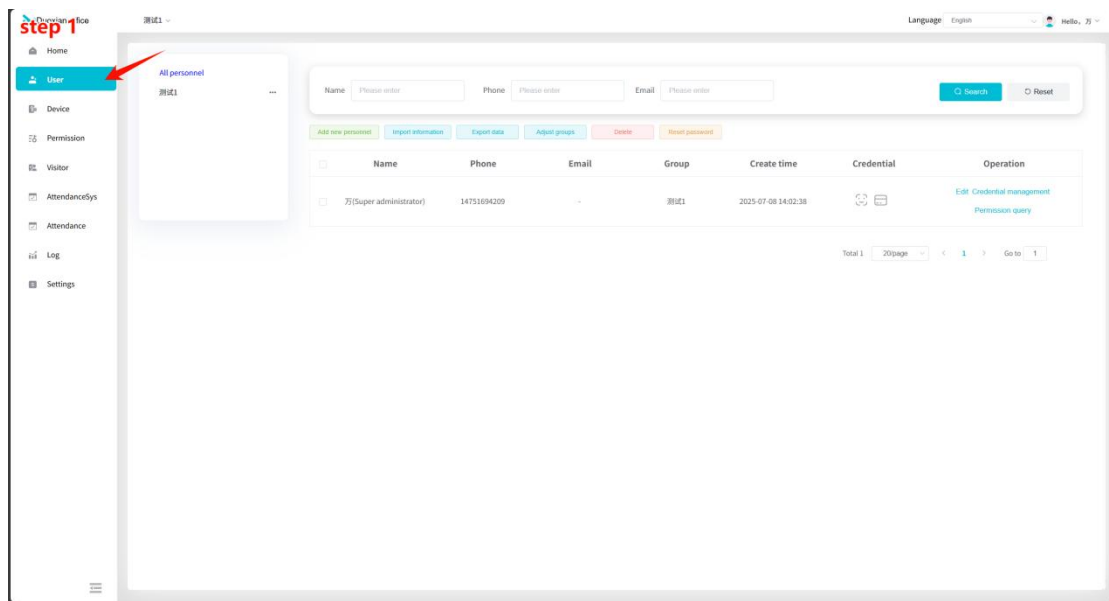


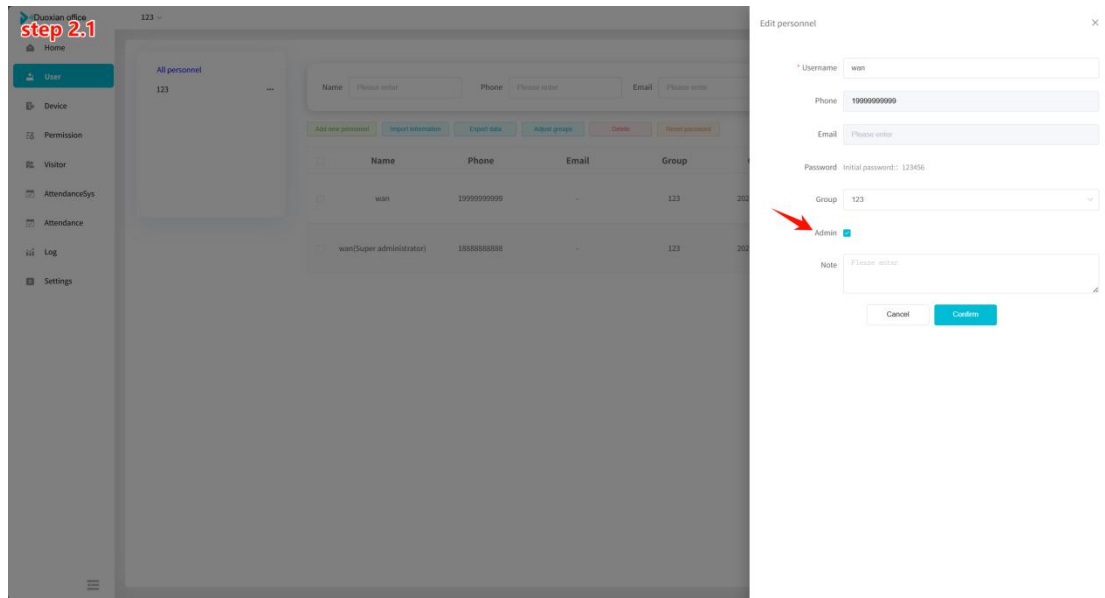
4.1.2. Administrator Sets Permissions for Login

Step 1: The administrator logs in to the system and enters the personnel management module.

Step 2: Click [Add New Member], enter the member information and check that the member is an administrator, then click [Confirm]; the person can log in as an administrator, and the

default login password is 123456; or select an existing member, click [Edit], pop up the personnel editing page, check that the person is an administrator, click confirm; the person can log in as an administrator, and the default login password is 123456.





4.2. Member Management

4.2.1. Member Information Import

Information import can export personnel templates, import templates, import personnel pictures, and import QR code pictures.

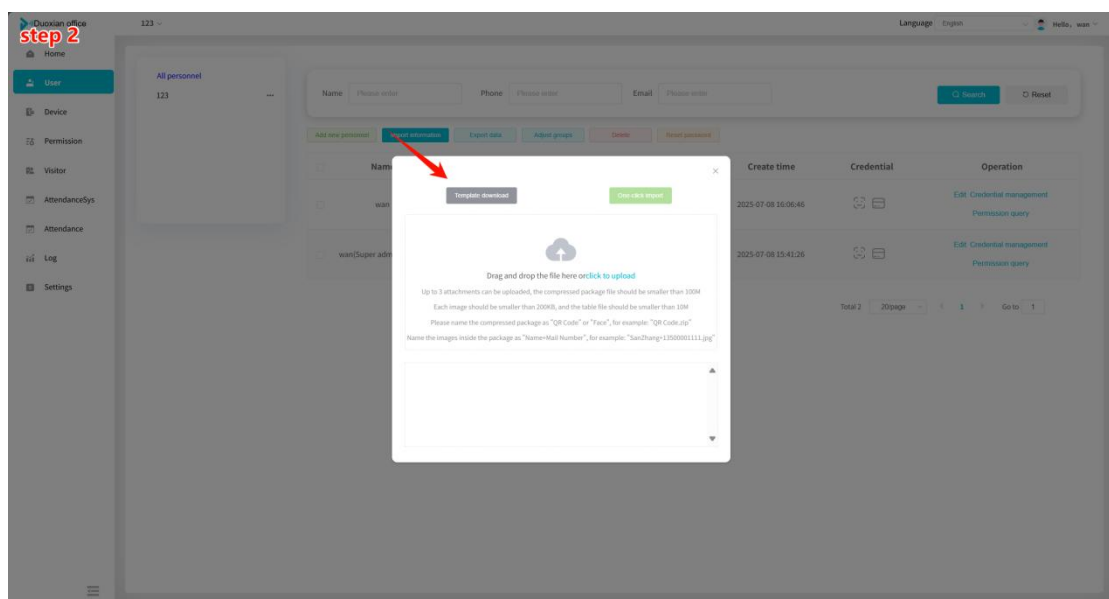
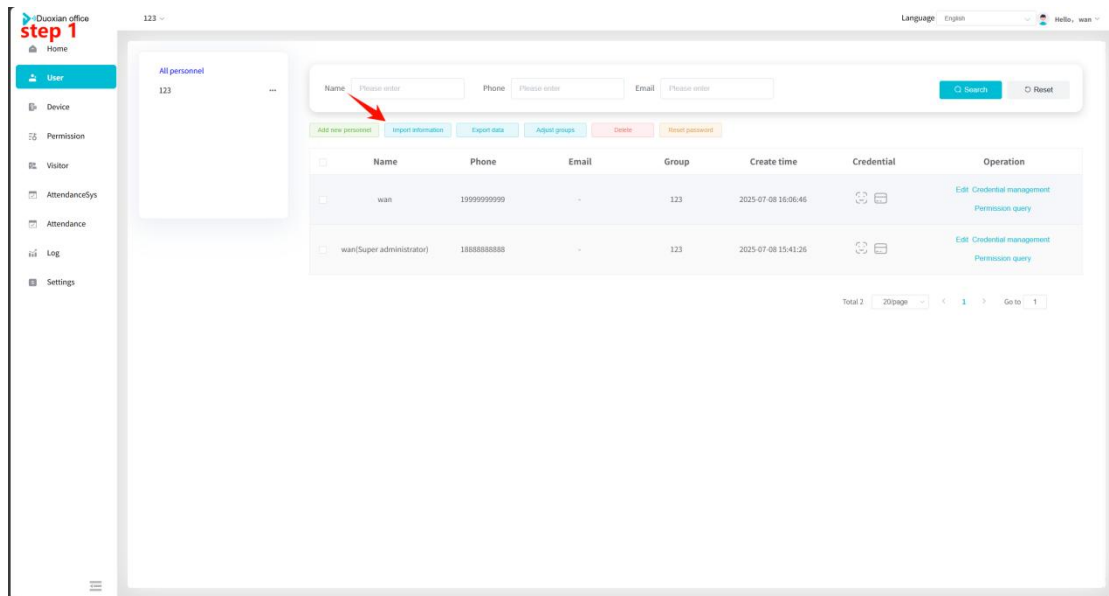
Step 1: Click the [Import Information] button.

Step 2: Click the [Template Download] button to download a personnel information template.

Step 3: Fill in according to the template information; the personnel's name and mobile phone number are required, and others are optional.

Step 4: Click [One-click Import], and you can choose to import the personnel template, face picture zip, or QR code zip (Note:

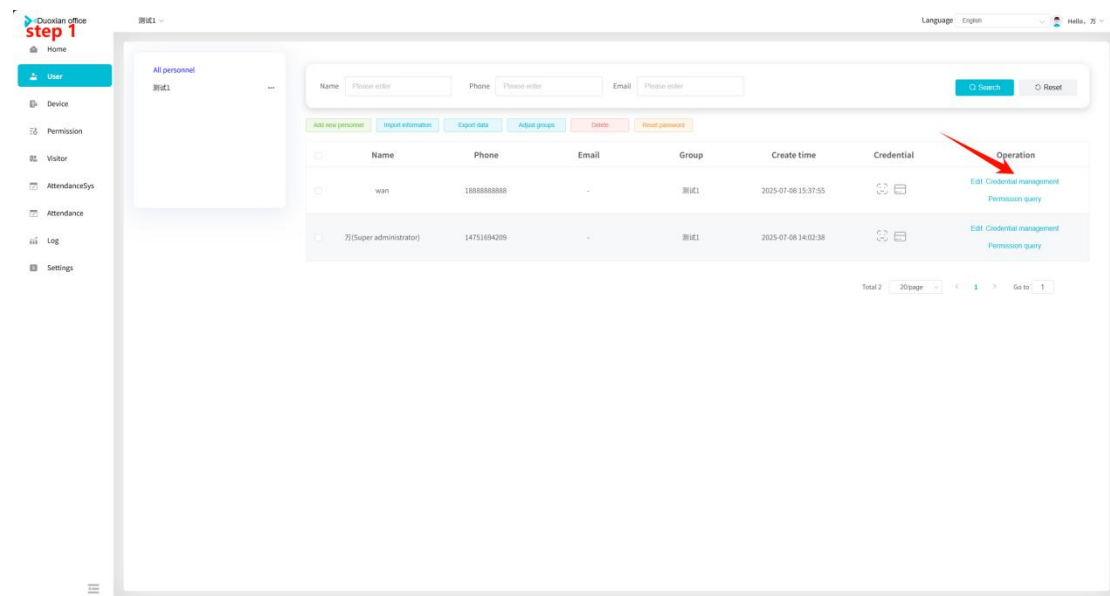
The pictures in the package must be named with name + mobile phone number, and the zip package must be named with face or QR code).

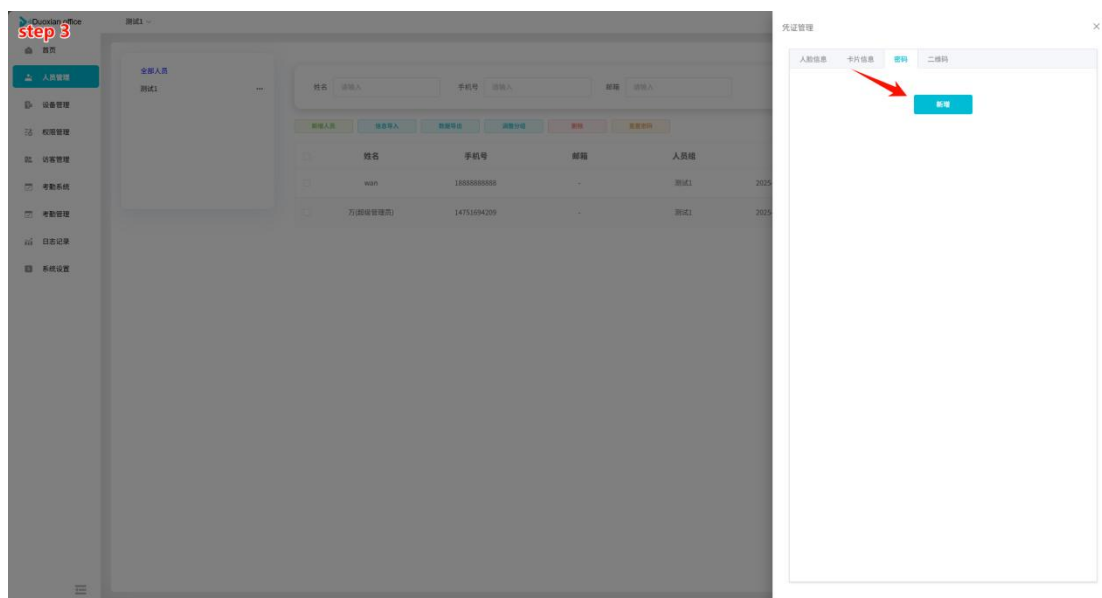
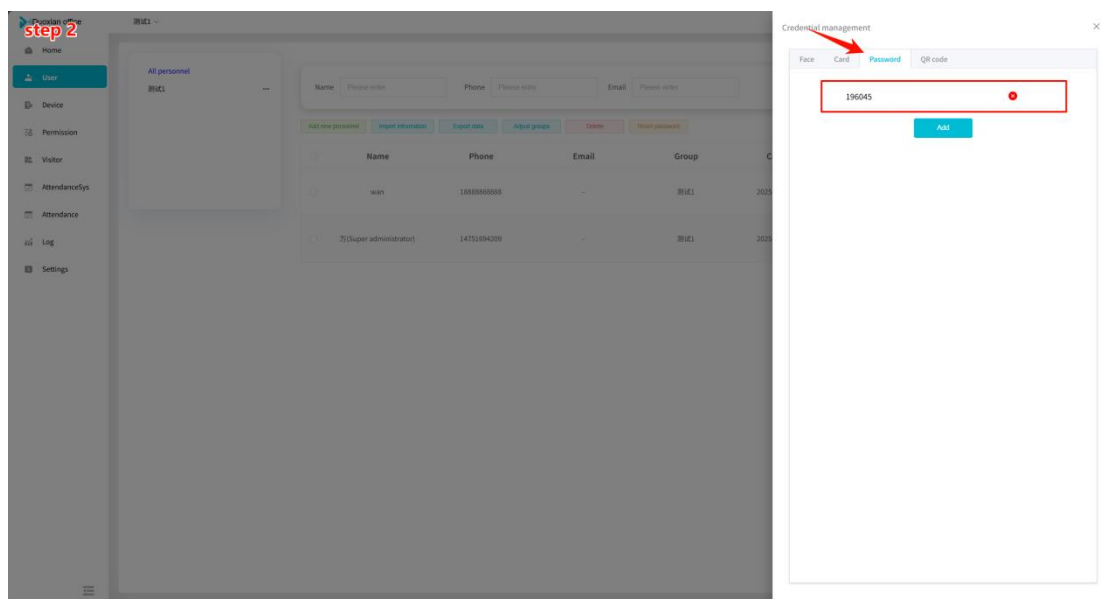


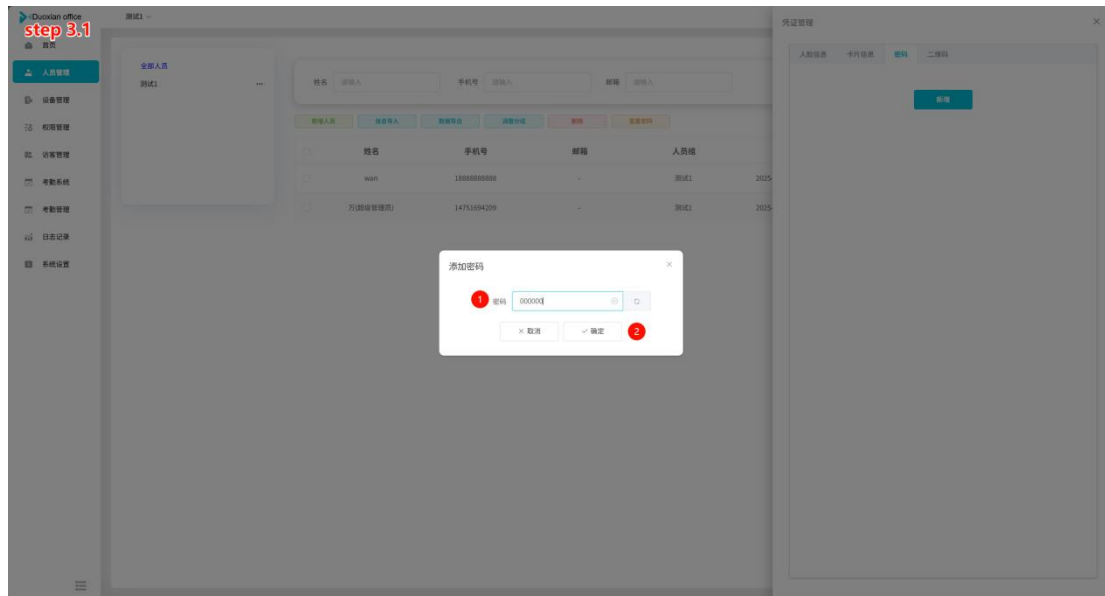
the password table to jump to the password setting page; each account has a default 6-digit password credential.

Step 3: Click the add button to add a custom digital password; click the delete button after the password to delete the existing password.

(Note: The Bluetooth credential is bound to the member's mobile phone number. After the member logs in to the Duoxian Office App with the registered mobile phone number, they can use the Bluetooth function to pass through the access control devices under the permission group.)







4.3. Device Management

4.3.1. Add/Edit Device

Devices can be added in two ways: adding a new device and importing devices.

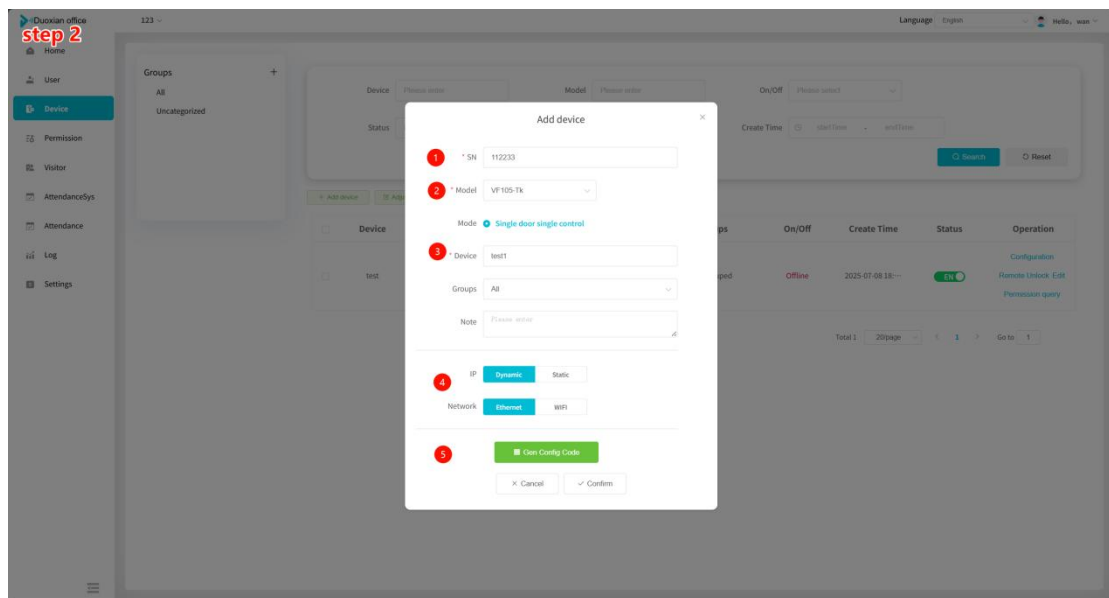
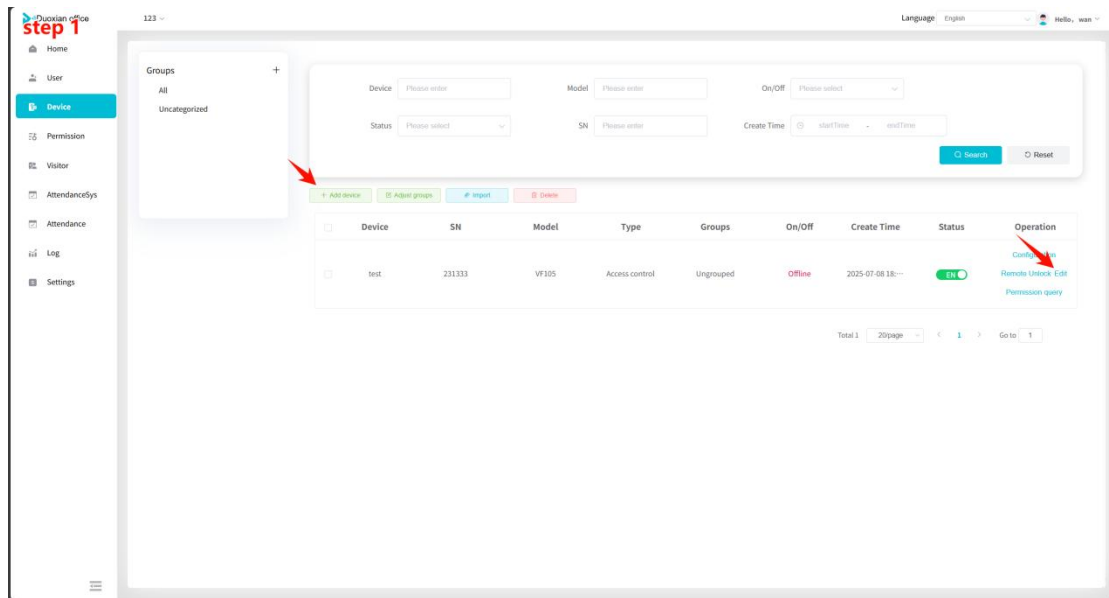
First method: Add a new device.

Step 1: Click [Add Device]/[Edit] to pop up the add device/edit device window.

Step 2: Enter the device SN code, select the device model, enter the device name, and others are optional.

Step 3: After verification, you can set the network and IP according to the actual on-site situation, click [Generate Configuration Code] to configure the device to connect to the network and server. If not configured, the device is offline.

After successful configuration, the device will restart. After connecting to the network and server, the device is online. Only online devices can remotely open the door successfully.



4.3.2. Import Devices

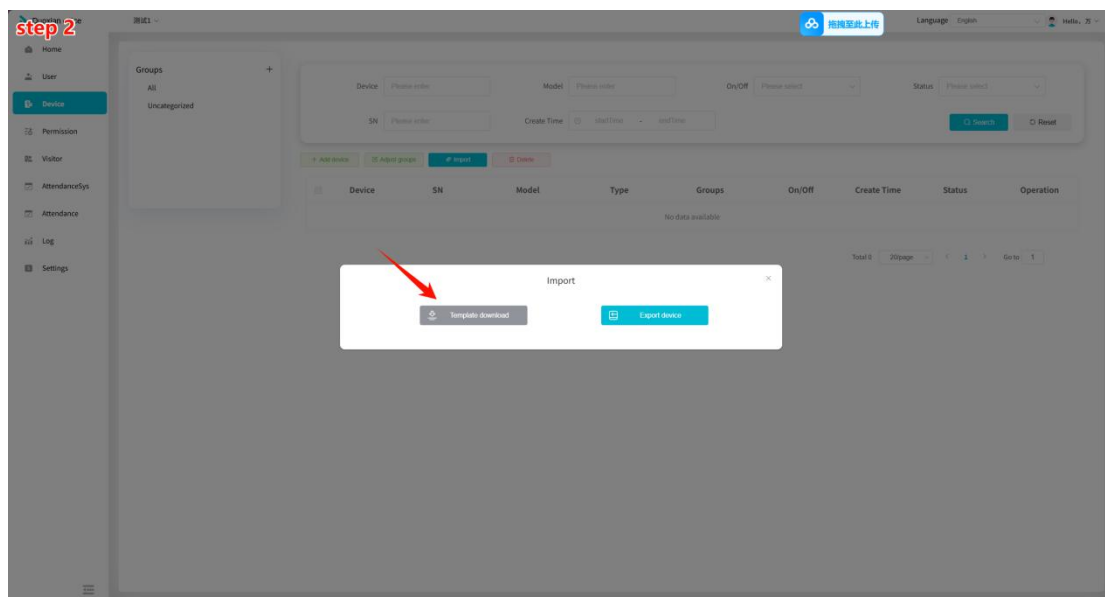
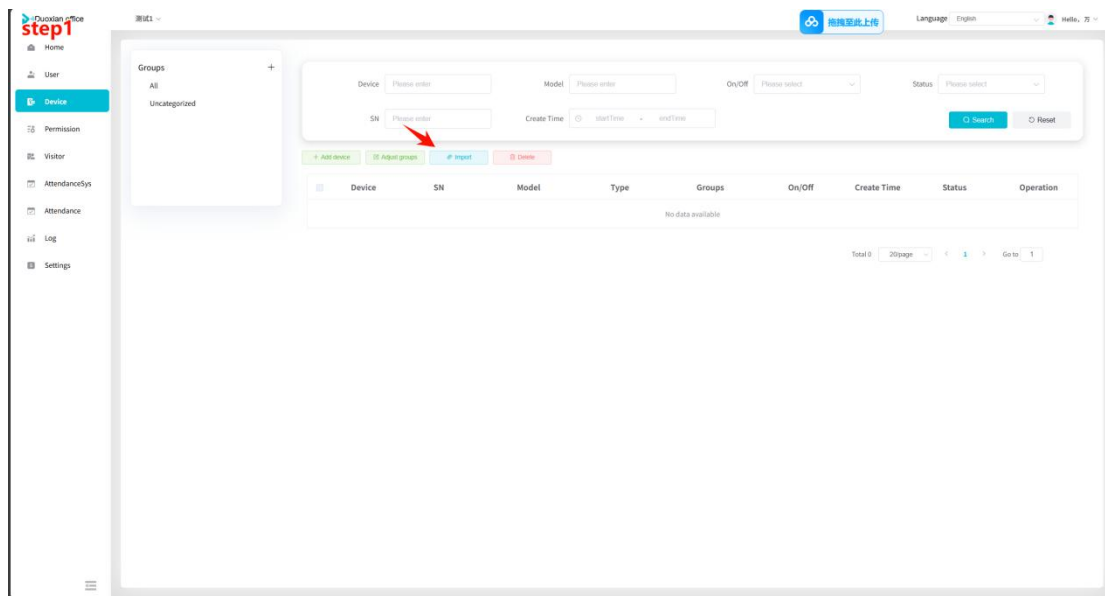
The second way to add devices: Import devices.

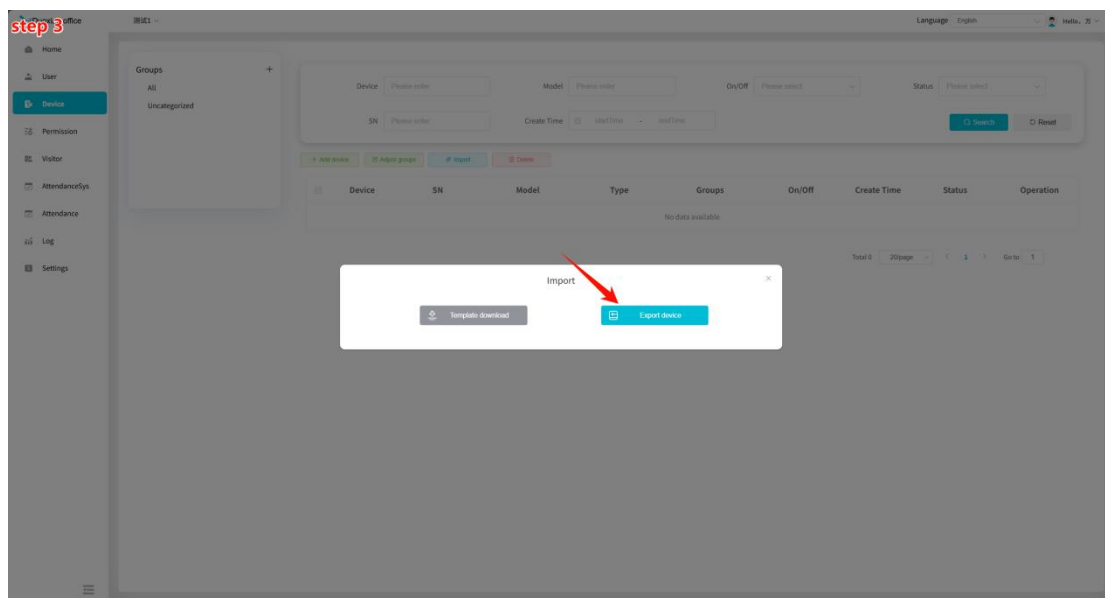
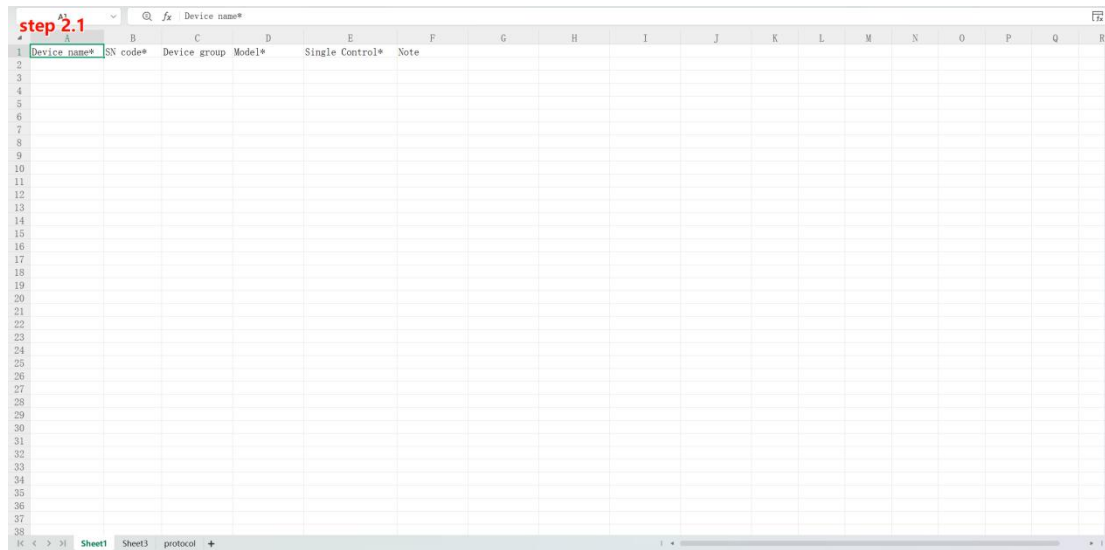
Step 1: Click [Import] to pop up the import window, where you

can choose template download and device import.

Step 2: Click [Template Download] to download the device template; the device name, SN code, device model, and single control are required, and others are optional.

Step 3: After filling in, click [Device Import], and select the filled .xlsx file to batch import the edited devices.





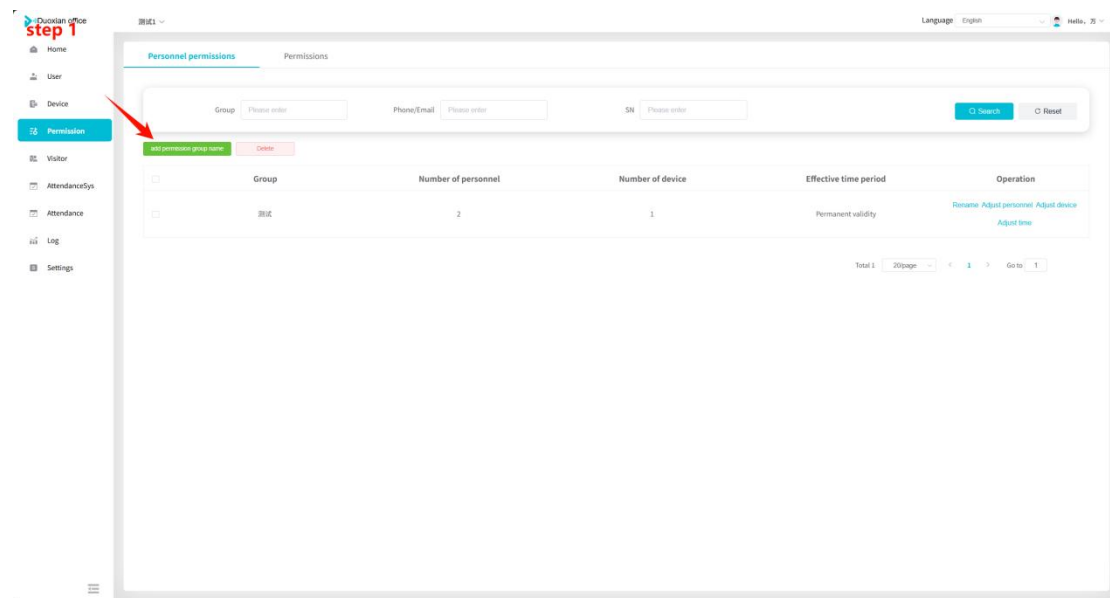
4.4. Permission Management

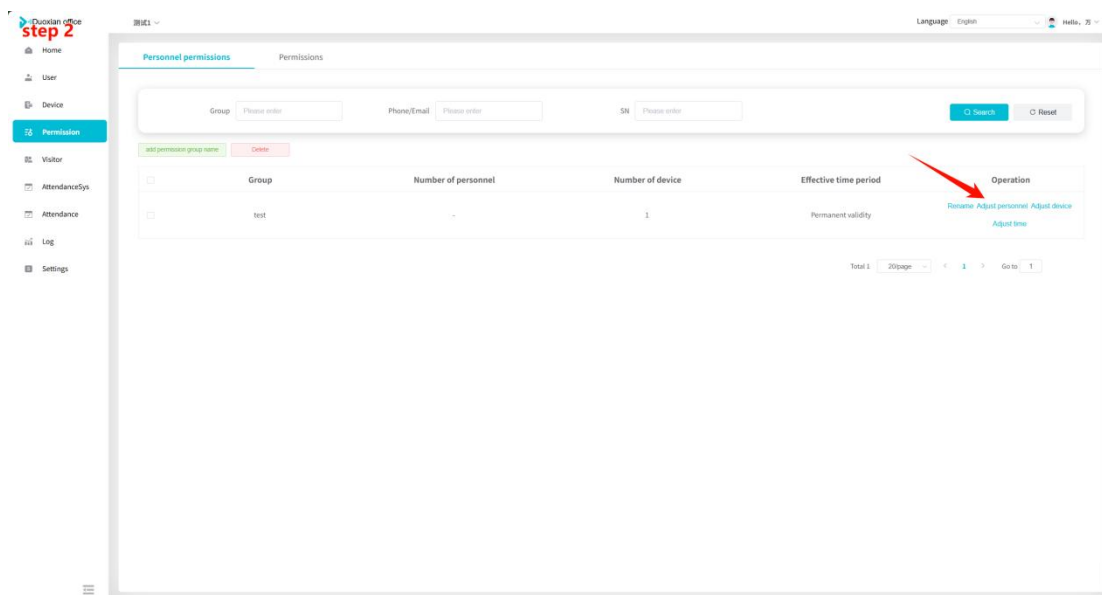
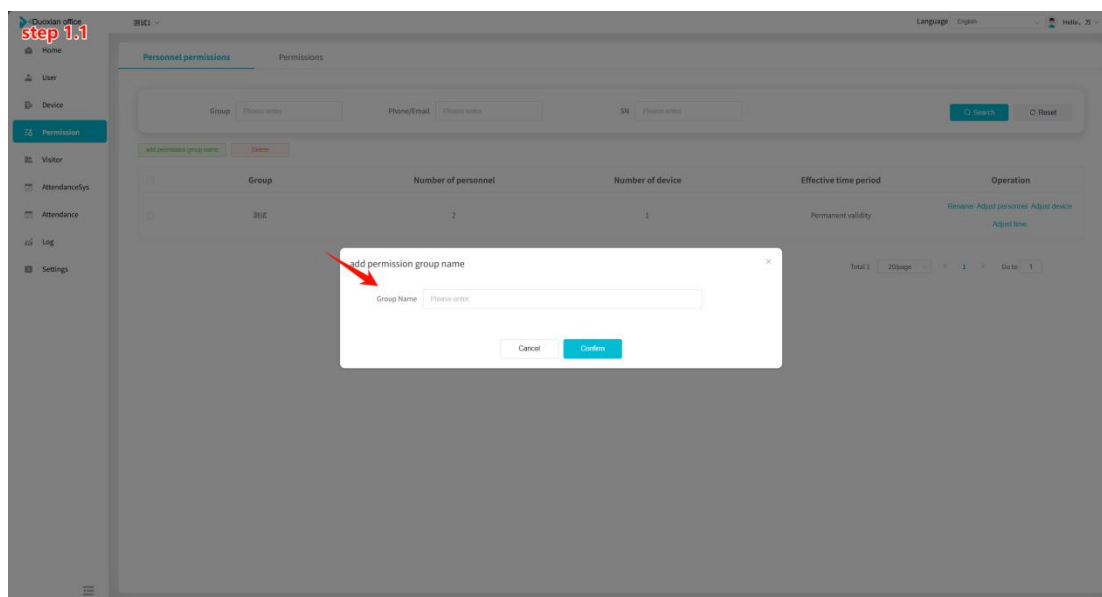
The system supports group management of permissions. The organization administrator can add, edit, and delete permission groups; members in the corresponding permission group can pass through devices in the same permission group through relevant credentials in [Personnel Management].

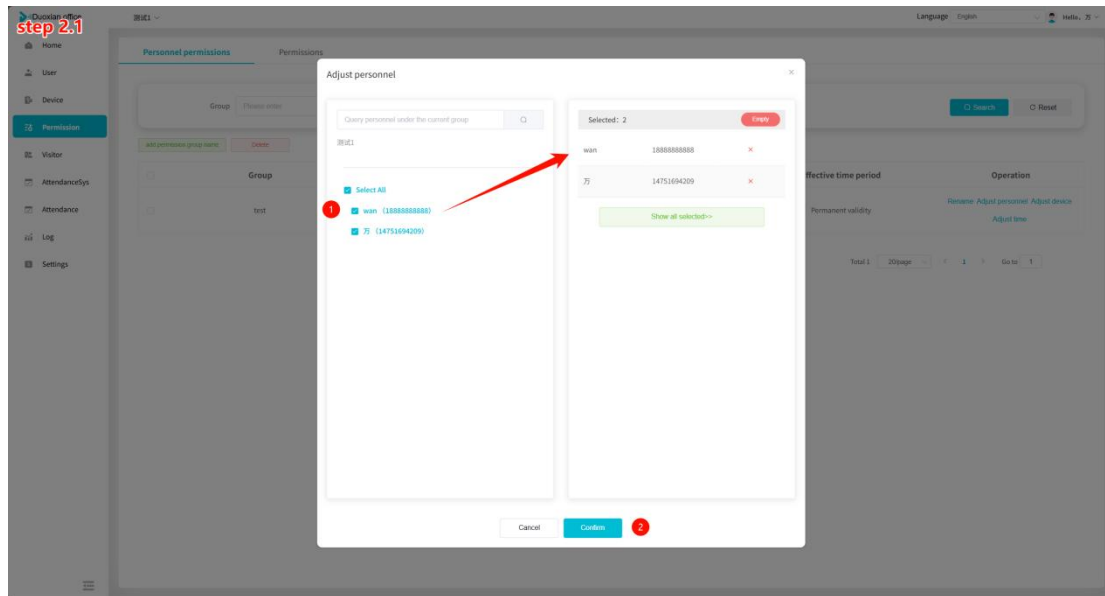
4.4.1. Add Permission Group

Step 1: Enter the Permission Management – Personnel Permissions page, click [Add Permission Group], pop up the add permission group window, enter the permission group name, click [Confirm], and a permission group can be added.

Step 2: Click [Adjust Personnel] to add or remove personnel from the permission group. Check the personnel you want to authorize and add them; the personnel are added successfully. Check the added personnel and click Remove Personnel to remove the personnel from the permission group.







4.4.2. Permission Group Device Management

Step 1: Click [Adjust Device] to jump to the device adjustment page.

Step 2: Click Add Device, pop up the add device window, check the devices to be added to the permission group and add them; the devices are added successfully. Check the added devices and click Remove Device to remove the devices from the permission group.

