Face Recognition Access Standalone

Quick Start Guide

V1.0.0

Cybersecurity Recommendations

Mandatory actions to be taken towards cybersecurity

1. Change Passwords and Use Strong Passwords:

The number one reason systems get "hacked" is due to having weak or default passwords. It is recommended to change default passwords immediately and choose a strong password whenever possible. A strong password should be made up of at least 8 characters and a combination of special characters, numbers, and upper and lower case letters.

2. Update Firmware

As is standard procedure in the tech-industry, we recommend keeping NVR, DVR, and IP camera firmware up-to-date to ensure the system is current with the latest security patches and fixes.

"Nice to have" recommendations to improve your network security

1. Change Passwords Regularly

Regularly change the credentials to your devices to help ensure that only authorized users are able to access the system.

2. Change Default HTTP and TCP Ports:

● Change default HTTP and TCP ports for systems. These are the two ports used to communicate and to view video feeds remotely.

● These ports can be changed to any set of numbers between 1025 -65535. Avoiding the default ports reduces the risk of outsiders being able to guess which ports you are using.

3. Enable HTTPS/SSL:

Set up an SSL Certificate to enable HTTPS. This will encrypt all communication between your devices and recorder.

4. Enable IP Filter:

Enabling your IP filter will prevent everyone, except those with specified IP addresses, from accessing the system.

5. Change ONVIF Password:

On older IP Camera firmware, the ONVIF password does not change when you change the system's credentials. You will need to either update the camera's firmware to the latest revision or manually change the ONVIF password.

6. Forward Only Ports You Need:

● Only forward the HTTP and TCP ports that you need to use. Do not forward a huge range of numbers to the device. Do not DMZ the device's IP address.

● You do not need to forward any ports for individual cameras if they are all connected to a recorder on site; just the NVR is needed.

7. Disable Auto-Login on SmartPSS:

Those using SmartPSS to view their system and on a computer that is used by multiple people should disable auto-login. This adds a layer of security to prevent users without the appropriate credentials from accessing the system.

8. Use a Different Username and Password for SmartPSS:

In the event that your social media, bank, email, etc. account is compromised, you would not want someone collecting those passwords and trying them out on your video surveillance system. Using a different username and password for your security system will make it more difficult for someone to guess their way into your system.

9. Limit Features of Guest Accounts:

If your system is set up for multiple users, ensure that each user only has rights to features and functions they need to use to perform their job.

10. UPnP:

● UPnP will automatically try to forward ports in your router or modem. Normally this would be a good thing. However, if your system automatically forwards the ports and you leave the credentials defaulted, you may end up with unwanted visitors.

● If you manually forwarded the HTTP and TCP ports in your router/modem, this feature should be turned off regardless. Disabling UPnP is recommended when the function is not used in real applications.

11. SNMP:

Disable SNMP if you are not using it. If you are using SNMP, you should do so only temporarily, for tracing and testing purposes only.

12. Multicast:

Multicast is used to share video streams between two recorders. Currently there are no known issues involving Multicast, but if you are not using this feature, deactivation can enhance your network security.

13. Check the Log:

If you suspect that someone has gained unauthorized access to your system, you can check the system log. The system log will show you which IP addresses were used to login to your system and what was accessed.

14. Physically Lock Down the Device:

Ideally, you want to prevent any unauthorized physical access to your system. The best way to achieve this is to install the recorder in a lockbox, locking server rack, or in a room that is behind a lock and key.

15. Connect IP Cameras to the PoE Ports on the Back of an NVR:

Cameras connected to the PoE ports on the back of an NVR are isolated from the outside world and cannot be accessed directly.

16. Isolate NVR and IP Camera Network

The network your NVR and IP camera resides on should not be the same network as your public computer network. This will prevent any visitors or unwanted guests from getting access to the same network the security system needs in order to function properly.

Regulatory Information

The regulatory information herein might vary according to the model you purchased. Some information is only applicable for the country or region where the product is sold.

FCC Information

⚠️ **CAUTION**

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

FCC conditions:

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

● This device may not cause harmful interference.
● This device must accept any interference received, including interference that may cause undesired operation.

FCC compliance:

This equipment has been tested and found to comply with the limits for a digital device, pursuant to part 15 of the FCC Rules. This equipment generate, uses and can radiate radio frequency energy and, if not installed and used in accordance with the guide, may cause harmful interference to radio communication.

● For class A device, these limits are designed to provide reasonable protection against harmful interference in a commercial environment. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.
● For class B device, these limits are designed to provide reasonable protection against harmful interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
  ● Reorient or relocate the receiving antenna.
  ● Increase the separation between the equipment and receiver.
  ● Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
  ● Consult the dealer or an experienced radio/TV technician for help.

Important Safeguards and Warnings

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

Operation Requirement

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

Electrical Safety

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

Foreword

General

This Quick Start Guide (hereinafter referred to as "Guide") introduces the installation and basic operation of the Face Recognition Access Standalone (hereinafter referred to as "access standalone").

Model

Model	Function
A	IC card, password and face unlock.
B	IC card, password, face and fingerprint unlock.
C	ID card, password, face unlock.
D	ID card, password, face and fingerprint unlock.

Safety Instructions

The following categorized signal words with defined meaning might appear in the Guide.

Signal Words	Meaning
□ NOTE	Provides additional information as the emphasis and supplement to the text.

Revision History

No.	Version	Revision Content	Release Date
1	V1.0.0	First Release	February 2019

Privacy Protection Notice

As the device user or data controller, you might collect personal data of other such as face, fingerprints, car plate number, Email address, phone number, GPS and so on. You need to be in compliance with the local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures include but not limited to: providing clear and visible identification to inform data subject the existence of surveillance area and providing related contact.

About the Guide

- The Guide is for reference only. If there is inconsistency between the Guide and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the Guide.
- The Guide would be updated according to the latest laws and regulations of related

regions. For detailed information, see the paper manual, CD-ROM, QR code or our official website. If there is inconsistency between paper manual and the electronic version, the electronic version shall prevail.

- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the Guide. Please contact the customer service for the latest program and supplementary documentation.
- There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, please refer to our final explanation.
- Upgrade the reader software or try other mainstream reader software if the Guide (in PDF format) cannot be opened.
- All trademarks, registered trademarks and the company names in the Guide are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurred when using the device.
- If there is any uncertainty or controversy, please refer to our final explanation.

Table of Contents

1 Overview

1.1 Introduction

The access standalone is an access control panel that supports unlock through faces, passwords, fingerprints, cards, Bluetooth, and supports unlock through their combinations.

1.2 Features

- Wall-mounted.
- 7 inch LCD, touchscreen.
- Face images and face modules (like face photos and videos) cannot be used to unlock the door with 2MP WDR camera.
- The largest face among faces that appear at the same time is recognized first.
- With deep learning algorithm applied human faces can be quickly and accurately analyzed.
- Industrial f1.6 camera lens and starlight sensor provide improved night vision in low light conditions.
- Support voice broadcast verification results.

1.3 Appearance

There are two types: with fingerprint reader and without fingerprint reader. See Figure 1-1.

Figure 1-1 Appearance
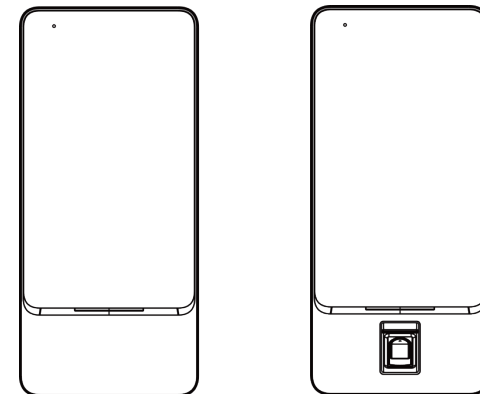
1.4 Dimensions
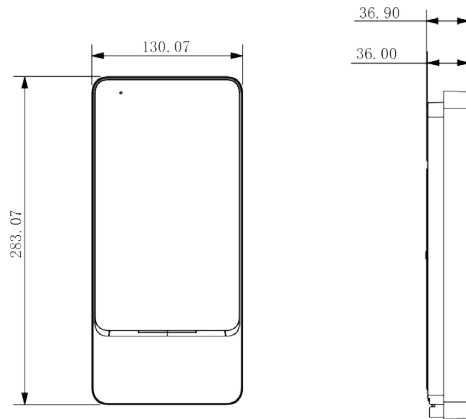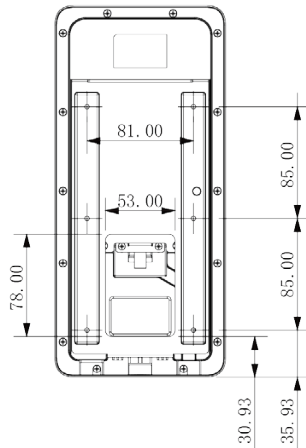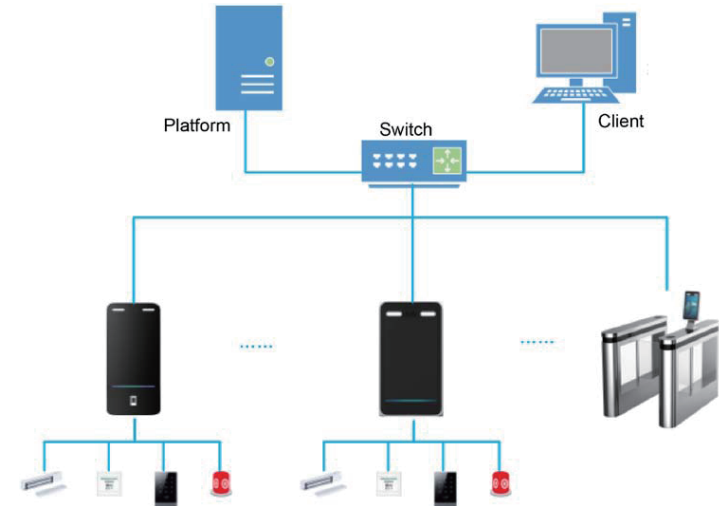
Figure 1-2 Dimension (mm)

Figure 1-3 Installation drawing (mm)

Figure 1-4 Application scenario

1.5 Application Scenario

Applicable to parks, scenic spots, schools, residential areas, office buildings and more. Faces can not only be imported into the access standalone, but also be sent from platforms to the access standalone. See Figure 1-4.

2 Installation

2.1 Cable Connections

The access standalone needs to be connected to devices like sirens, readers, and door contacts. For their cable connection, see Table 2-1 and Table 2-2.

Table 2-1 Port description

Port	Cable color	Cable name	Description
CON1	Black	RD–	Negative electrode of external reader power supply.
	Red	RD+	Positive electrode of external reader power supply.
	Blue	CASE	Tamper alarm input of the external reader.
	White	D1	Wiegand D1 in (connected to external reader)/out (connected to controller).
	Green	D0	Wiegand D0 in (connected to external reader)/out (connected to controller).
	Brown	LED	Wiegand D0 in (connected to external reader)/ out (connected to controller).
	Yellow	B	RS-485 negative electrode in (connected to external reader)/output (connected to controller).
	Purple	A	RS-485 positive electrode in (connected to external reader)/out (connected to controller).
CON2	White and red	ALARM1_NO	Alarm 1 normally on output port·
	White and orange	ALARM1_COM	Alarm 1 public output port.
	White and blue	ALARM2_NO	Alarm 2 normally on output port.
	White and gray	ALARM2_COM	Alarm 2 public output port.
	White and green	GND	Connected to the ground cable.
	White Brown	ALARM1	Alarm 1 input port.
	White and yellow	GND	Connected to the ground cable.
	White and purple	ALARM2	Alarm 2 input port.
CON3	Black and red	RX	RS-232 receiving port.

Port	Cable color	Cable name	Description
	Black and orange	TX	RS-232 sending port.
	Black and blue	GND	Connected to the ground cable.
	Black and gray	SR1	Used for door contact detection, this function is not available in model D.
	Black and green	PUSH1	Door open button of door No.1
	Black and brown	DOOR1_COM	Connected to the controller to control door locks.
	Black and yellow	DOOR1_NO	Connected to the controller to control door locks.
	Black and purple	DOOR1_NC	Connected to the controller to control door locks.

2.2 Installation Method

The installation of access standalone A, B, C and D are the same.
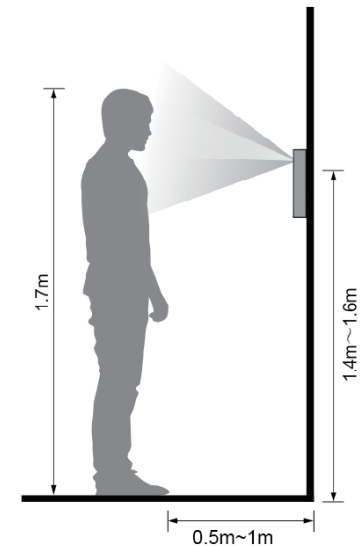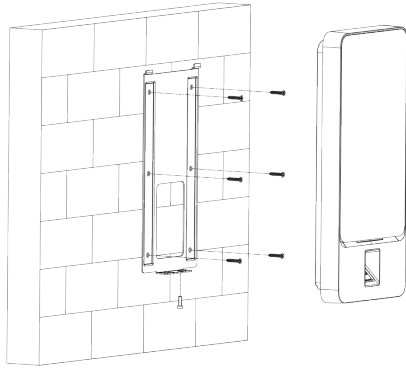
Figure 2-1 Installation drawings

Figure 2-2 Wall mounted

Installation procedure

Step 1 Drill seven holes (six bracket installation holes and one cable entry) in the wall according to holes in the bracket.

Step 2 Fix the bracket on the wall by installing the expansion screws into the six bracket installation holes.

Step 3 Connect cables for access standalone.
See "2.1 Cable Connections".

Step 4 Hang the access standalone on the bracket hook.

Step 5 Tighten the screws at the bottom of the access standalone.
The installation is completed.

3 System Operation

3.1 Basic Configuration Flow Chart

Figure 3-1
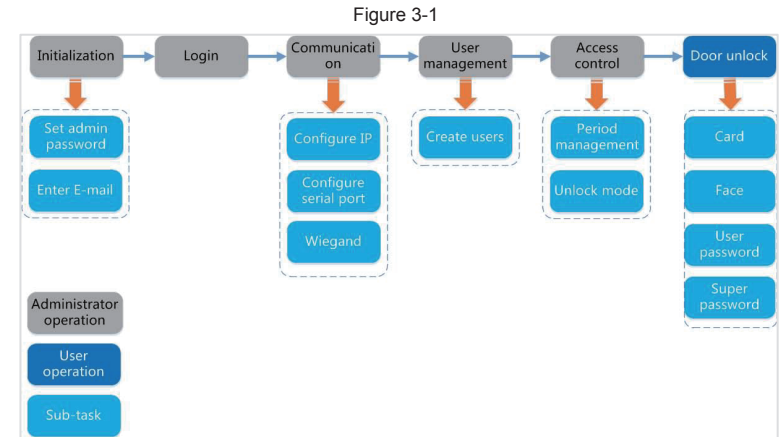
3.2 Button Description

See Table 3-1.

Table 3-1 Button description

Button	Description
⏮	Go to the first page.
⏭	Go to the last page.
‹	Go to the previous page.
›	Go to the next page.
←	Go to the previous menu.
→	Go to the next menu.

3.3 Initialization

Administrator password and an e-mail need to be set the first time the access standalone is turned on; otherwise the access standalone cannot be used. See Figure 3-1.

Figure 3-2 Initialization

Figure 3-3 Standby interface

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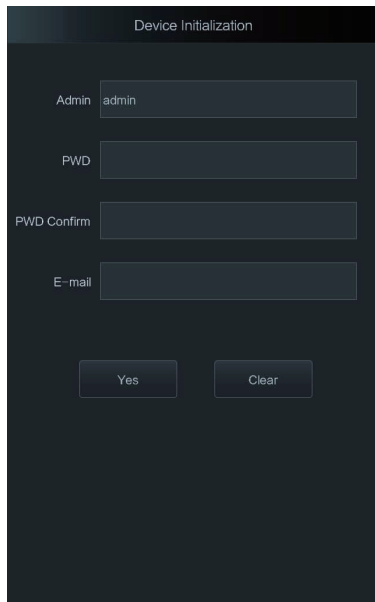
- The administrator password can be reset through the e-mail address you entered if the administrator forgets the administrator password.
- The password should consist of 8 to 32 non-blank characters and contain at least two types of characters among upper case, lower case, number, and special character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

3.4 Standby Interface

You can unlock the door through cards, fingerprints, faces, and passwords. See Table 3-2.

📖

The interface will go to the standby interface if there are no operations in 30 seconds.

Table 3-2 Standby interface description

Name	Description
Status bar	Displays the status of Wi-Fi, wired network, and flash drive.
Door unlocking methods	Displays the methods of unlocking the door.
Face recognition area	Human faces can be recognized in this area.
PWD Unlock icon	You can unlock the door by entering passwords and super passwords.
Super PWD	The super password can unlock the door without being subject to user levels, unlock modes, periods, holiday plans, and anti-passback.
Main menu icon	Tap the icon, and then you can enter the main menu. 📖 - Only the administrator can enter the main menu. - Before you create administrators, anyone can enter the main menu.
Date & Time	Displays the current date and time.

3.5 Unlocking Methods

You can unlock the door through cards, passwords, fingerprints (Model A and C do not support), and face recognition.

3.5.1 Swiping Cards

Put the card at the card swiping area to unlock the door.

3.5.2 Face Recognition

Make sure that your face is centered on the face recognition frame, and then you can unlock the door.

3.5.3 Unlocking through User Passwords

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

Step 1 Tap the PWD Unlock icon on the standby interface.

A PWD Unlock icon and a Super PWD Unlock icon are displayed.

Step 2 Tap the PWD Unlock icon.

Step 3 Enter the User ID, tap OK, and then tap ▣.

Step 4 Enter the User password, tap OK, and then tap ▣.

The door is unlocked.

3.5.4 Unlocking through Super Password

Enter the super passwords, and then you can unlock the door. There is only one super password for one access standalone. The super password can unlock the door without being subject to user levels, unlock modes, periods, holiday plans, and anti-passback.

Step 1 Tap PWD Unlock icon on the main interface.

A PWD Unlock icon and a Super PWD Unlock icon are displayed.

Step 2 Tap the Super PWD Unlock icon.

Step 3 Enter the super password, tap OK, and then tap ▣.

The door is unlocked.

3.6 Main Menu

If administrators are created, then only administrators can add users of different levels, set access-related parameters, do network configuration, view access records and system information, and more in the main menu.
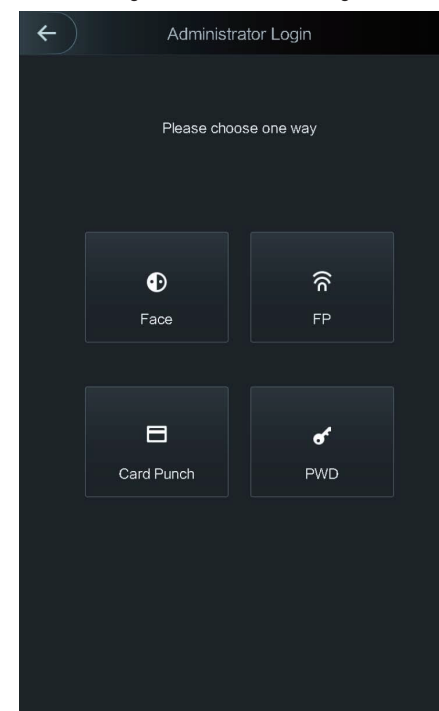
Step 1 Tap ⌂ on the standby interface.

The Administrator Login interface is displayed. See Figure 3-3.

📖

Different modes support different unlock methods, and the actual interface shall prevail.

Figure 3-4 Administrator Login

Step 2 Select a main menu entering method.

The main menu interface is displayed. See Figure 3-4.
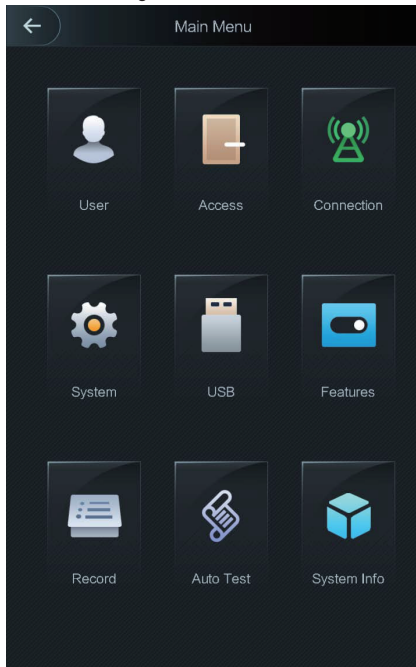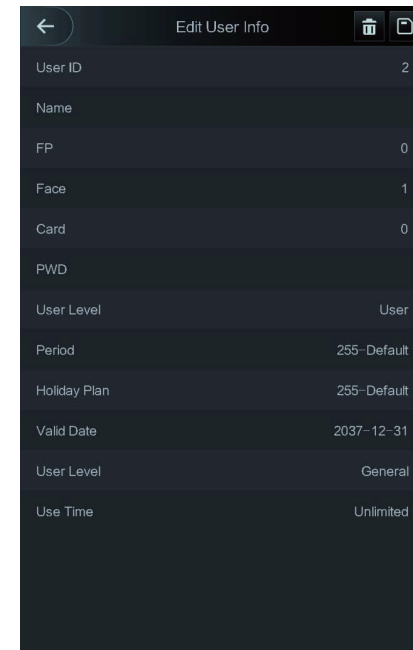
Figure 3-5 Main Menu

Figure 3-6 New user

3.7 User Management

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

3.7.1 Adding New Users

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

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

Step 1   Select **User > New User**.

The new user interface is displayed. See Figure 3-5.

Step 2   Configure parameters on the interface. See Table 3-2.

Table 3-3 New user parameter description

Parameter	Description
No.	You can enter user IDs. The IDs can only be numbers, and the maximum length of the ID digits is 8.
Name	You can enter names with at least 32 characters (including numbers, symbols, and letters).
Fingerprint	At most three fingerprints of one user can be recorded, and one fingerprints need to be verified three times. You can enable the Duress FP function under each fingerprint, and only one of the three fingerprints can be the duress fingerprint. Alarms will be triggered if a duress fingerprint is used to unlock the door. It is not recommended that you select the first fingerprint as the duress fingerprint.
Face Recognition	Make sure that your face is centered on the picture capturing frame and then tap to take a picture of the new user's face. See "Appendix 1 Notes of Face Recording".

Parameter	Description
Card	You can register five cards for each user. On the card registration interface, enter your card number or swipe your card, and then the card information will be read by the access standalone. You can enable the Duress Card function on the card registration interface. Alarms will be triggered if a duress card is used to unlock the door.
Password	The door unlocking password. The maximum length of the ID digits is 8.
User level	You can select a user level for new users. There are two options: ● User: Users only have door unlock authority. ● Admin: Administrators can not only unlock the door but also have parameter configuration authority. 📖 ● If there is an administrator in the access standalone, administrator identity authentication is needed. ● In case that you forget the administrator password, you had better create more than one administrator.
Period	You can set a period in which the user can unlock the door. For detailed period settings, see the configuration manual.
Holiday plan	You can set a holiday plan in which the user can unlock the door. For detailed holiday plan settings, see the configuration manual.
Valid date	You can set a period during which the unlocking information of the user is valid.
User level	There are six levels: ● General: General users can unlock the door normally. ● Blacklist: When users in the blacklist unlock the door, service personnel will get a prompt. ● Guest: Guests are allowed to unlock the door certain times. Once they exceed the maximum times, they cannot unlock the door again. ● Patrol: Paroling users can get their attendance tracked, but they have no unlock authority. ● VIP: When VIP unlocks the door, service personnel will get a prompt. ● Disable: When the disabled unlock the door, there will be a delay of 5 seconds before the door is closed.
Use time	When the user level is Guest, you can set the maximum number of times that he or she can unlock the door.

Step 3 After you have configured all the parameters, tap 💾 to save the configuration.
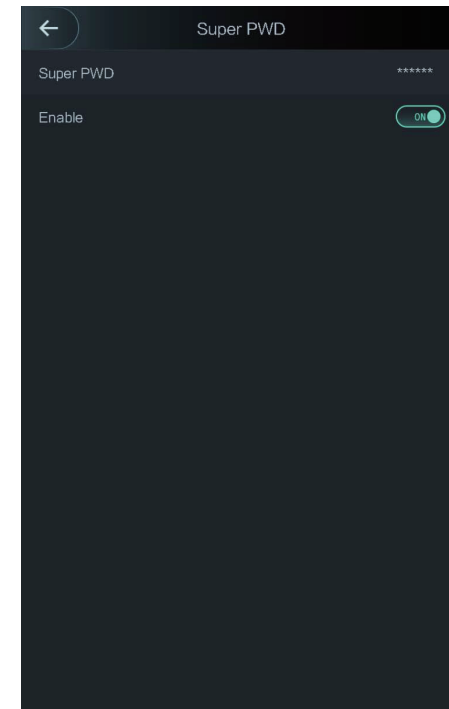
3.7.2 Super Password

● There is only one super password for one access standalone. The super password can unlock the door without being subject to user levels, unlock modes, periods, holiday plans, and more.
● When unlocking the door through the super password, User ID is not needed.

Step 1 Select **User > Super PWD**.
The Super PWD interface is displayed. See Figure 3-6.

Figure 3-7 Super Password

Step 2 Tap **Super PWD**, enter the super password, and then tap 💾 to save it.

Step 3 Enabling the Super PWD.

● [ON] means enabled.

● [OFF] means not enabled.

3.7.3 Unlock Mode

There are three unlock modes: unlock mode, unlock by period, and group combination. Unlock modes vary with standalone access models, and the actual standalone access shall prevail.
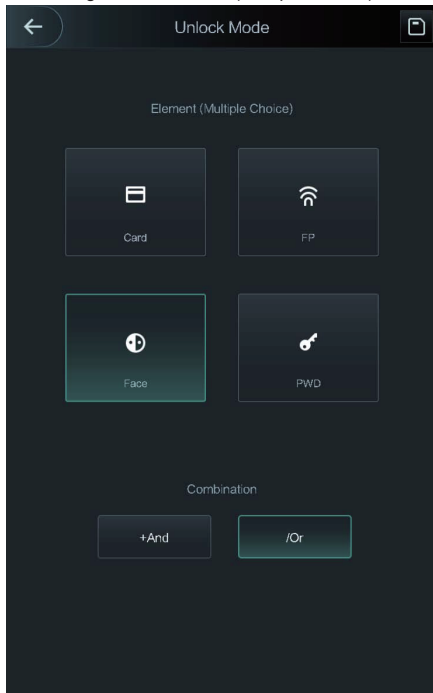
3.7.3.1 Unlock Mode

When the Unlock Mode is on, users can unlock through cards, fingerprints, faces, passwords, or one or any one of all the unlocking methods.

Step 1 Select **Assess > Unlock Mode > Unlock Mode**.
The **Element (Multiple Choice)** interface is displayed. See Figure 3-7.

Figure 3-8 Element (Multiple Choice)

Step 1 Select unlock mode(s).

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

Step 2 Select a combination mode.

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

Step 3 Tap 🖫 to save the settings.

And then the **Unlock Mode** interface is displayed.

Step 4 Enable the **Unlock Mode**.
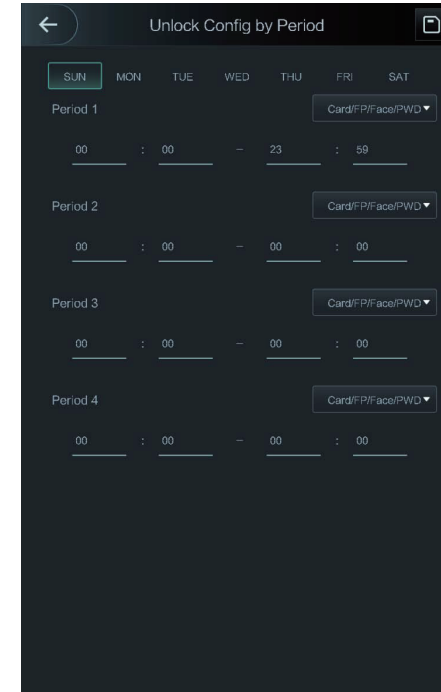
- ⬤ means enabled.

- ⬤ means not enabled.

3.7.3.2 Unlock by Period

Doors can be unlocked through different unlock modes in different periods. For example, in period 1, the door can only unlocked through card; and in period 2, doors can only be locked through fingerprints.

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

The **Unlock Config by Period** interface is displayed. See Figure 3-8.

Figure 3-9 Unlock by Period

Step 2 Set starting time and end time for a period, and then select a unlock mode.

Step 3 Tap 🖫 to save the settings.

And then the Unlock Mode interface is displayed.

Step 4 Enable the **Unlock by Period** function.

- ⬤ means enabled.

- ⬤ means not enabled.

3.7.3.3 Group Combination

Doors can only be unlocked by a group or groups that consist of more than two users if the Group Combination is enabled.

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

The **Group Combination Config** interface is displayed. See Figure 3-10.
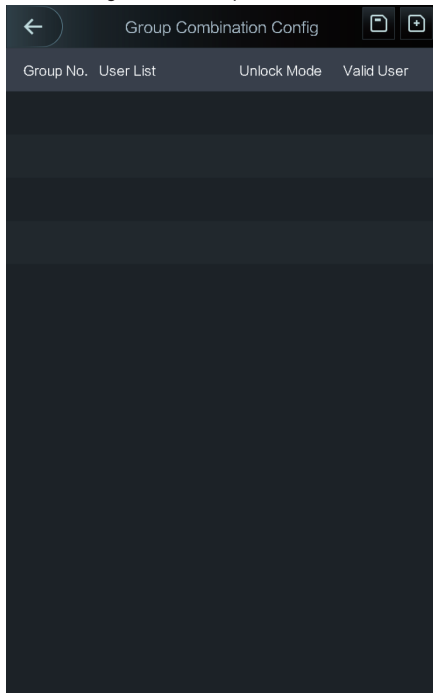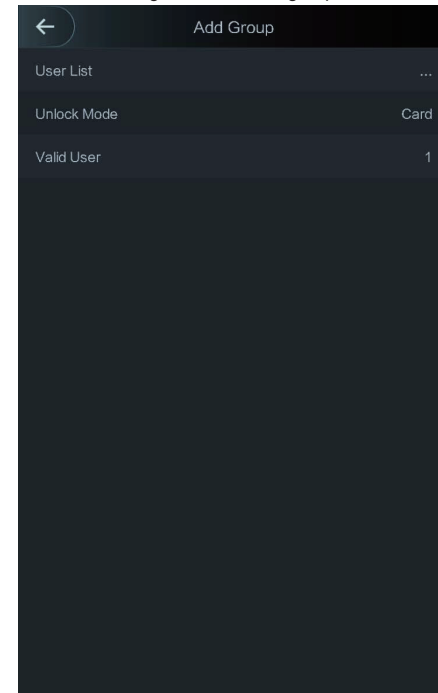
Figure 3-10 Group Combination

Step 2   Tap to create a group. See Table 3-4.

The **Add Group** interface is displayed. See Figure 3-11.

Figure 3-11 Add a group

Table 3-4 Group parameter

Parameter	Description
User List	Add users to the newly created group. 1. Tap User List. The User List interface is displayed. 1. Tap , and then enter a user ID. 2. Tap to save the settings.
Unlock Mode	There are four options: Card, FP, PWD, and Face.
Valid User	Valid users are the ones that have unlock authority. Doors can be unlocked only when the number of users to unlock the doors equals the valid user number. ● Valid users cannot exceed the total number of users in a group. ● If valid users equal total user numbers in a group, doors can only be unlocked by all the users in the group. ● If valid users are less than the total number of users in a group, doors can be unlocked by any users whose number equals the valid user number.

Step 3   Tap to go back to the previous interface.

Step 4 Tap 💾 to save the settings.

Step 5 Enable the Group Combination.

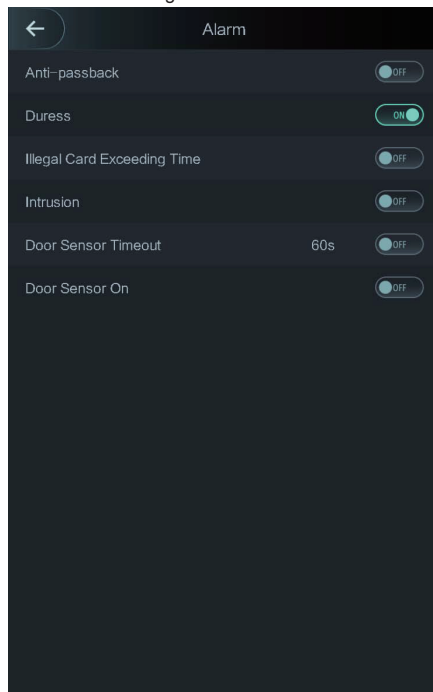- ON⬤ means enabled.

- ⬤OFF means not enabled.

3.7.4 Alarm Configuration

Administrators can manage visitors' unlock authority through alarm configuration.

Step 1 Select **Access > Alarm**.

The **Alarm** interface is displayed. See Figure 3-12.

Figure 3-12 Alarm

Step 2 See Table 3-5.

- ON⬤ means enabled.

- ⬤OFF means not enabled.

Table 3-5 Parameters on the Alarm interface

Parameter	Description
Anti-passback	If a person unlocks the door with his or her identity checked by the access standalone, but when he or she gets out without getting his or her identity checked by the access standalone, an alarm will be triggered and the person will have no authority to unlock the door any more.
Duress	An alarm will be triggered when a duress card, duress password, or duress fingerprint is used to unlock the door.
Illegal Card Exceeding Time	After an unauthorized card is used to unlock the door more than 5 times in 50 seconds, an alarm will be triggered.
Intrusion	An intrusion alarm will be triggered if a door is unlocked without having the door contact released.
Door Sensor Timeout	A timeout alarm will be triggered if the time that a user takes to unlock the door exceeds the Door Sensor Timeout time. The Door Sensor Timeout time range is 1–9999 seconds.
Door Sensor On	Only when the Door Sensor On is enabled can the intrusion alarm and door sensor timeout alarm be triggered.

3.7.5 Door Status

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

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

3.7.6 Lock Holding Time

If the door has been unlocked for longer than the defined lock holding time, the door will be automatically locked.

3.8 Network Connection

3.8.1 IP Configuration

Configure an IP address for the access standalone to make it be connected to the network. See Figure 3-13 and Table 3-6.
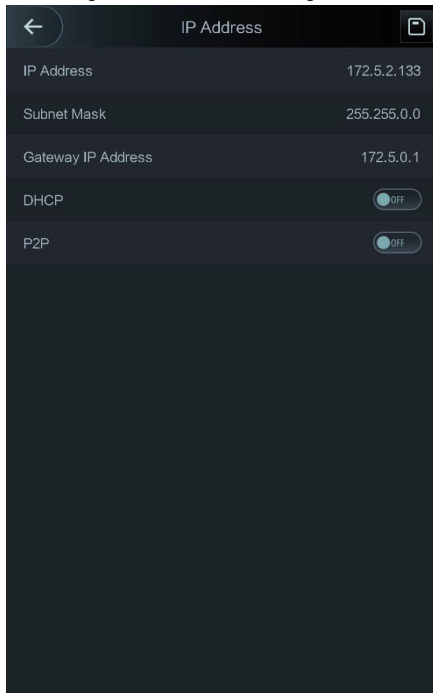
Figure 3-13 IP address configuration
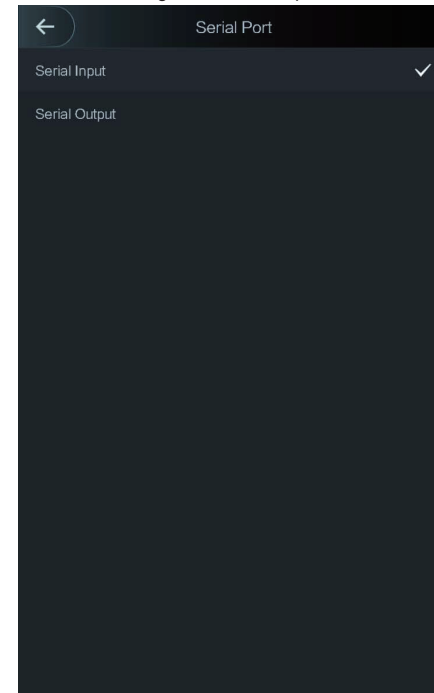

Figure 3-14 Serial port

Table 3-6 IP configuration parameters

Parameter	Description
IP Address/Subnet Mask/Gateway IP Address	The IP address, subnet mask, and gateway IP address should be on the same network segment. After configuration, tap [icon] to save the configurations.
DHCP	DHCP (Dynamic Host Configuration Protocol). When the DHCP is enabled, the IP address can be automatically acquired, and the IP address, subnet mask and gateway IP address cannot be manually configured.
P2P	P2P is a private network traversal technology which enables user to manage devices without requiring DDNS, port mapping or transit server.

3.8.2 Serial Port Settings

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

Select **Connection > Serial Port**, and then the **Serial Port** interface is displayed. See Figure 3-14.

- You should select Serial Input when external devices that are with face recognition, fingerprint recognition, card reading and writing functions are connected to the access standalone. Serial Input is selected to enable access card information to be sent to the access standalone and the management platform.

- For access standalones with face recognition, fingerprint recognition, card reading and writing functions, if you select Serial Output, access standalone information will be sent by the access standalone to the access controller. There are two types of access standalone information:
  - ◇ User ID.
  - ◇ Card No.

- When card reader with OSDP protocol is connected, select OSDP Input, and then card information can be sent to the management platform through the card reader.

3.8.3 Wiegand Configuration

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

Select **Connection > Wiegand**, and then the Wiegand interface is displayed. See Figure 3-15.

Figure 3-15 Wiegand
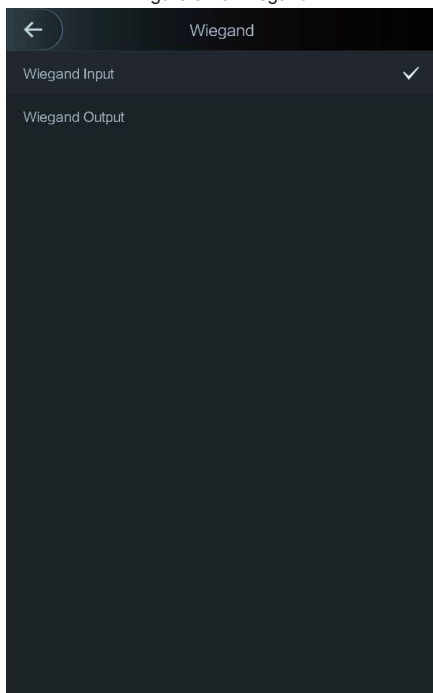
- Select Wiegand Input when an external card swipe mechanism is connected to the access standalone.

- Select Wiegand Output when the access standalone works as a reader that can be connected to the controller. Specifically, when face images with user ID or card No. are verified, the user IDs and card numbers can be transmitted to other access controls through Wiegand. See Table 3-7.

Table 3-7 Wiegand output

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

3.9 Face Parameter

Face recognition accuracy can be adjusted through face parameter configuration.
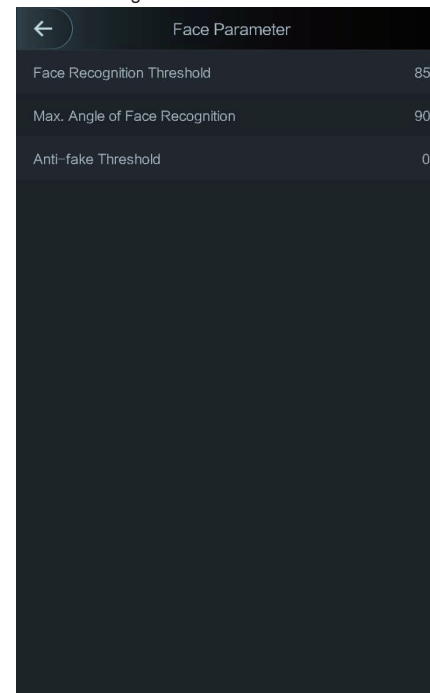
📖

Face recognition parameter should be configured by professional personnel.

Step 1 Select **System > Face Parameter**.

The **Face Parameter** interface is displayed. See Figure 3-16.

Figure 3-16 Face Parameter

Step 2 Tap and configure a parameter, and then tap 💾. See Table 3-8.

Table 3-8 Face Parameter

Name	Description
Face Recognition Threshold	Face recognition accuracy can be adjusted. The larger the value is, the higher the accuracy will be. 📖 For convenience, you can set the Face Recognition Threshold of Model C to 60.
Max. Angle of Face Recognition	You can set the access standalone shooting angle of profiles. The larger the value is, the wider range of the profiles will be recognized.

| Name	Description
Anti-fake Threshold	This function prevents people from unlocking by human face images. The larger the value is, the more difficult face images can unlock the door. The recommended value range is above 80.

3.10 USB

⚠️

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

3.10.1 USB Export

You can export data from the access standalone to the USB after inserting the USB. The data exported is encrypted and cannot be edited.

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

The **USB Export** interface is displayed. See Figure 3-17.

Figure 3-17 USB Export
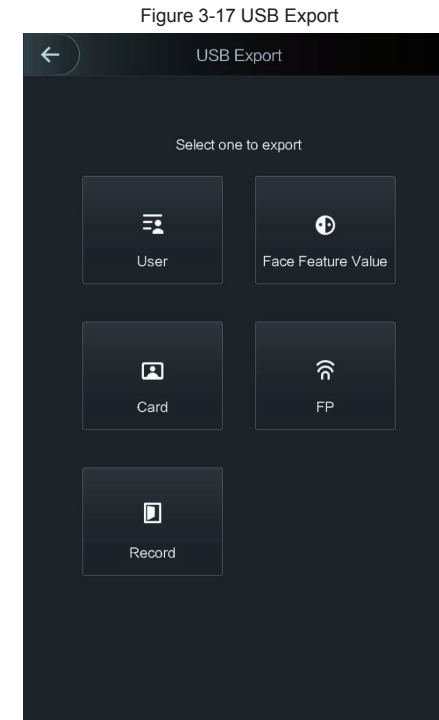
Step 2 Select the data type that you want to export.

Confirm to export is displayed.

Step 3 Tap **OK**.
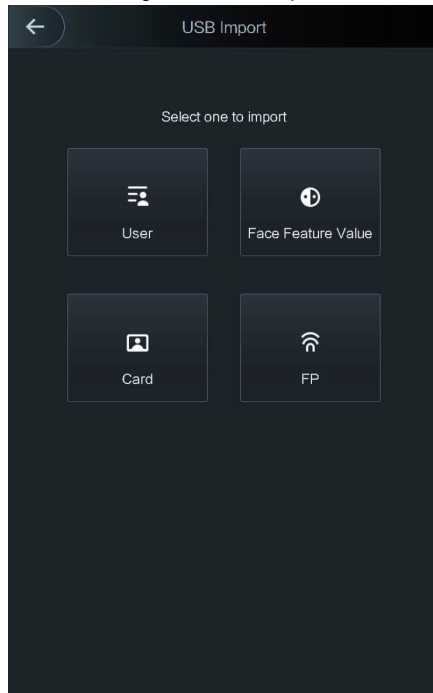
Data exported will be saved in the USB.

3.10.2 USB Import

Only data in the USB that was exported from one access standalone can be imported into another access standalone.

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

The **USB Import** interface is displayed. See Figure 3-18.

Figure 3-18 USB Import

Step 2 Select the data type that you want to import.
        Confirm to import is displayed.
Step 3 Tap **OK**.
        Data in the USB will be imported into the access standalone.

3.10.3 USB Update

USB can be used to update the system.
Step 1 Rename the updating file "update.bin", and save the "update.bin" file in the root
        directory of the USB.
Step 2 Select **USB > USB Update**.
        "Confirm to Update" is displayed.
Step 3 Tap **OK**.
        The update starts, and the access standalone reboots after the update is finished.

4 Web Operation

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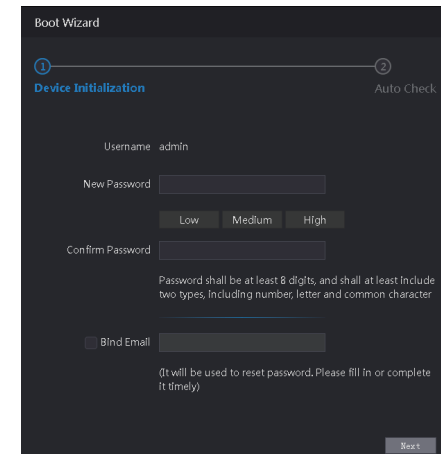
4.1 Initialization

You need to initialize the Web first before logging in the Web for the first time or logging in the Web after you have restored the access standalone to the factory settings.
Step 1 Open IE web browser, and enter the IP address (the default address is 192.168.1.108) of the access standalone in the address bar and press Enter.
        The **Initialization** interface is displayed. See Figure 4-1.

Use browser newer than IE 8, or you might not login the web.

Figure 4-1 Initialization

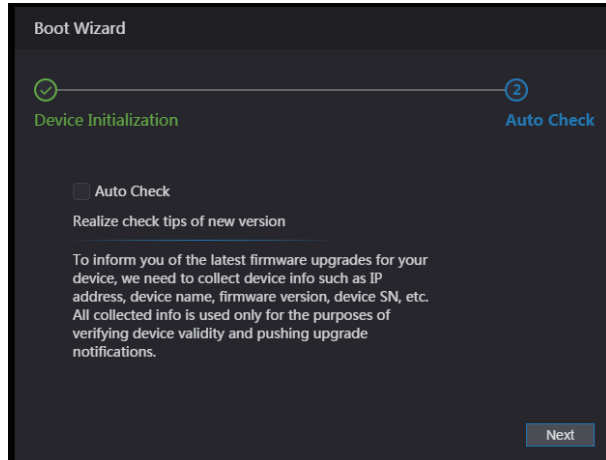Step 2 Enter the new password, confirm password, enter an e-mail address, and then tap **Next**.

- For the sake of security, keep the password properly after initialization and change the password regularly.
- The password should consist of 8 to 32 non-blank characters and contain at least two types of characters among upper case, lower case, number, and special character (excluding ' " ; : & and &). Set a password of high security level according to the password strength prompt.

- When you need to reset the administrator password by scanning the QR code, you need an e-mail address to receive the security code.

Step 3 Click **Next**.

The **Auto Test** interface is displayed. See Figure 4-2.

Figure 4-2 Auto Test

Boot Wizard

Device Initialization — ② Auto Check

☐ Auto Check

Realize check tips of new version

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

Next

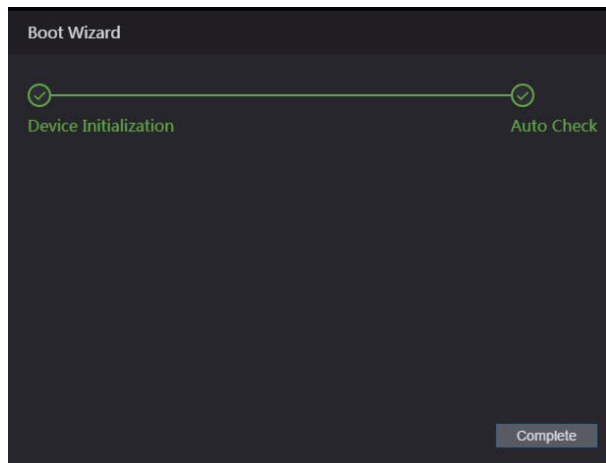Step 4 You can decide whether to select Auto Test or not.

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

Step 5 Click **Next**.

The **Finished configuration** interface is displayed. See Figure 4-3.

Figure 4-3 Finished Configuration

Boot Wizard

Device Initialization — Auto Check

Complete

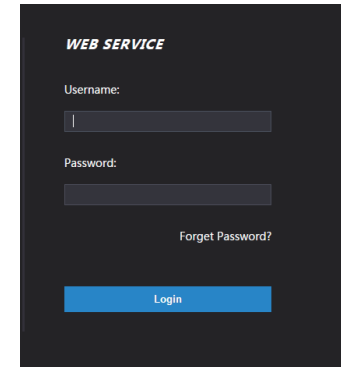Step 6 Click **Complete**, and the initialization is completed.

The Web login interface is displayed.

4.2 Login

Step 1 Open IE web browser, and enter the IP address of the access standalone in the address bar and press **Enter**.

See Figure 4-4.

Figure 4-4 Login

WEB SERVICE

Username:

|

Password:

Forget Password?

Login

Step 2 Enter the user name and password.

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

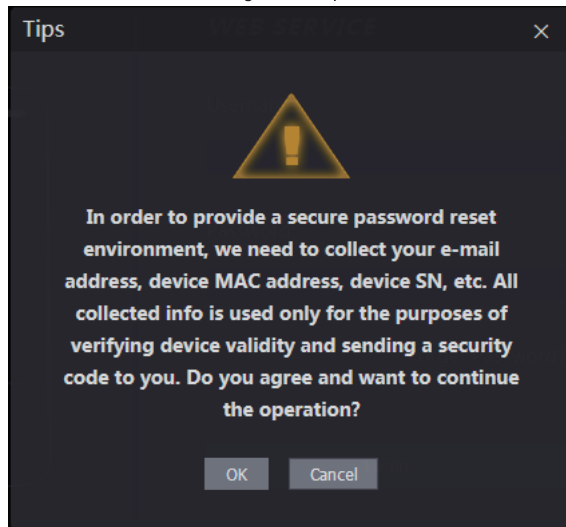Step 3 Click **Login**.

4.3 Reset the Password

When you need to reset the password of the admin account, your e-mail address will be needed.

Step 1 Click **Forgot password?** on the login interface.
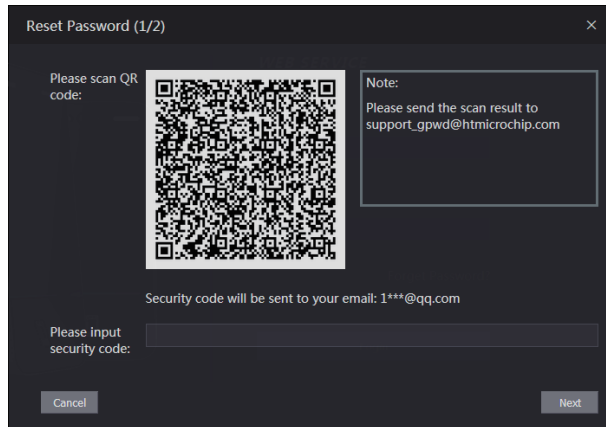
See Figure 4-5.

Figure 4-5 Tips

Step 2 Click **OK**.

The **Reset Password** interface is displayed. See Figure 4-6.

Figure 4-6 Reset Password

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

⚠

- At most two security codes will be generated by scanning the same QR code. To get more security code, refresh the QR code.
- Please use the security code within 24 hours after you receive it. Otherwise, it will become invalid.

- If wrong security codes are entered for consecutive five times, the administrator will be frozen for five minutes.

Step 4 Enter the security code you have received.

Step 5 Click **Next**.

The Reset Password interface is displayed.

Step 6 Reset and confirm the new password.

📖

The password should consist of 8 to 32 non-blank characters and contain at least two types of characters among upper case, lower case, number, and special character (excluding ' " ; : & and &).

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

4.4 Alarm Linkage

Enter alarm input type, when an alarm occurs, alarm output and access status will be linked.
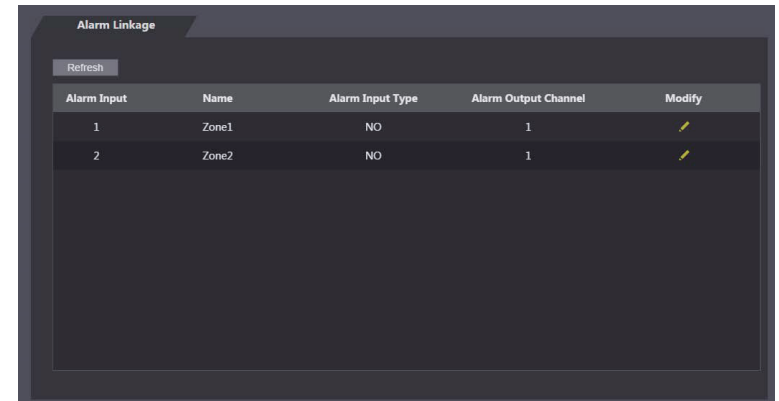
4.4.1 Setting Alarm Linkage

Alarm input devices can be connected to the access standalone, and you can modify the alarm linkage parameter according to your requirements.

Step 1 Select **Alarm Linkage**.

The **Alarm Linkage** interface is displayed. See Figure 4-7.

Figure 4-7 Alarm Linkage

Step 2 Click [icon], and then you can modify Alarm Linkage parameters. See Figure 4-8 and Table 4-1.

Figure 4-8 Modifying Alarm Linkage parameter

Table 4-1 Alarm Linkage Parameter description

Parameter	Description
Alarm Input	Enter an Alarm input number
Name	Enter a zone name.
Alarm Input Type	There are two options: NO and NC. If alarm input type of the alarm device you purchased is NO, then you should select NO; otherwise you should select NC.
Fire Link Enable	The access standalone will output alarms when fire alarms are triggered if the Fire Link is enabled. The alarm details will be displayed in the alarming record. Alarm Output and Access Link are NO by default if Fire Link is enabled.
Alarm Output Enable	The relay can output alarm information (will be sent to the management platform) if the Alarm Output is enabled.
Duration (second)	The alarm duration, and the range is 1–300 seconds.
Alarm Output Channel	You can select an alarm output channel according to the alarming device that you have installed.
Access Link Enable	After the Access Link is enabled, the access standalone will be normally on or normally closed when there are input alarm signals.

Parameter	Description
Channel Type	There are two options: NO and NC. If alarm input type of the alarm device you purchased is NO, then you should select NO; otherwise you should select NC.

Step 3 Click OK, and then the configuration is completed.

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

4.4.2 Alarm Log

You can view the alarm type and time range in the Alarm Log.

Step 1 Select **Alarm Linkage > Alarm Log**.
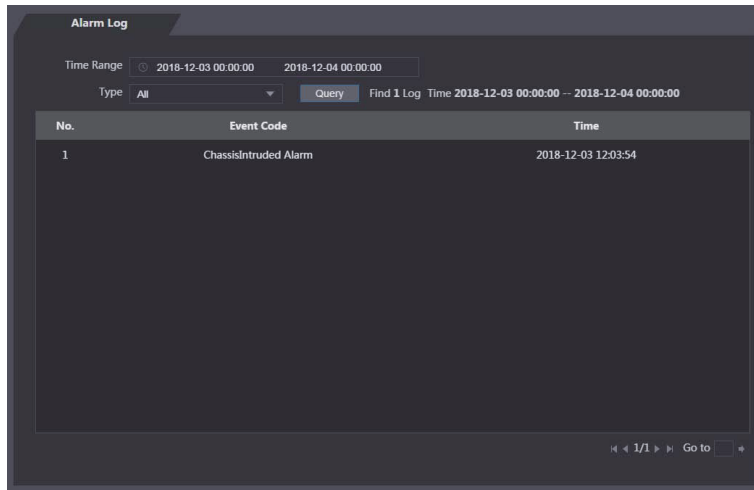
The **Alarm Log** interface is displayed, see Figure 4-9.

Figure 4-9 Alarm Log

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

The query results are displayed. See Figure 4-10.

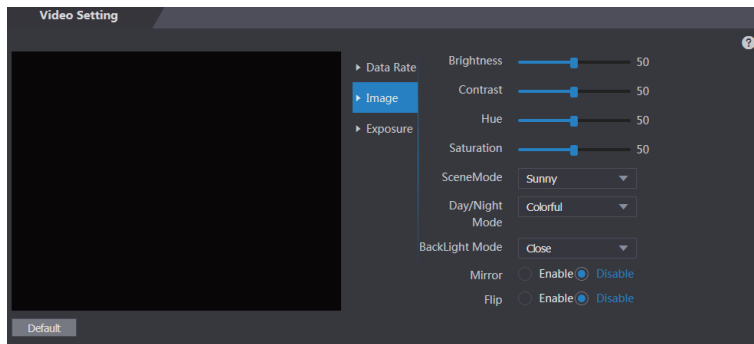Figure 4-10 Query results

4.5 Image Management

When human faces are in the backlight, you need to enable the Wide Dynamic.

The system dims bright areas and compensates dark areas to ensure the definition of objects in the bright areas and dark areas.

Step 1   Select **Video Setting > Video Setting > Image**.
　　　　See Figure 4-11.

Figure 4-11 Image

Step 2   Select **Wide Dynamic** in the Backlight Mode.

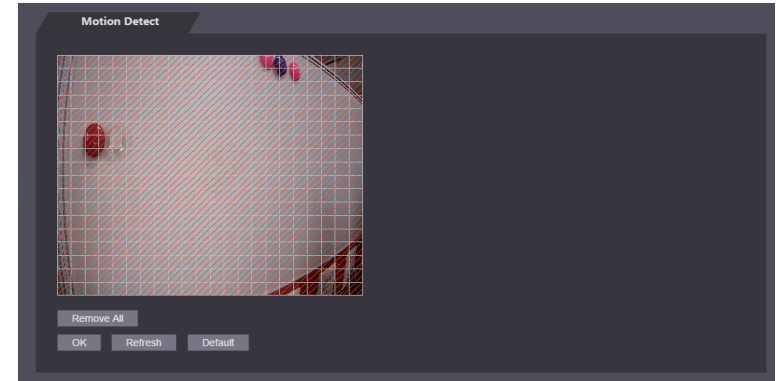For other parameter configuration, see the User's Manual.

4.6 Motion Detection

Set a range in which moving objects can be detected.

Step 1   Select **Video Setting > Video Setting > Motion Detection**.
　　　　The **Motion Detection** interface is displayed. See Figure 4-12.

Figure 4-12 Motion Detection

Step 2   Press and hold the left mouse button, and then drag the mouse in the red area. The **Motion Detection** area is displayed. See Figure 4-13.

- The red rectangles are motion detection area. The default motion detection range is all the rectangles.
- To draw a motion detection area, you need to click Remove All first.
- The motion detection area you draw will be a non-motion detection area if you draw in the default motion detection area.

Figure 4-13 Motion Detection area
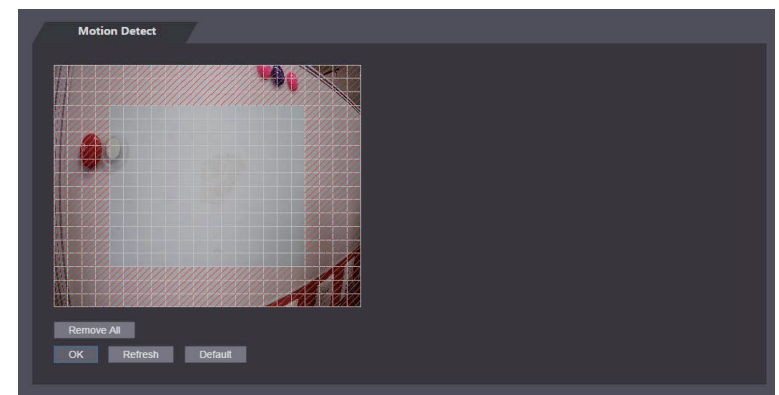
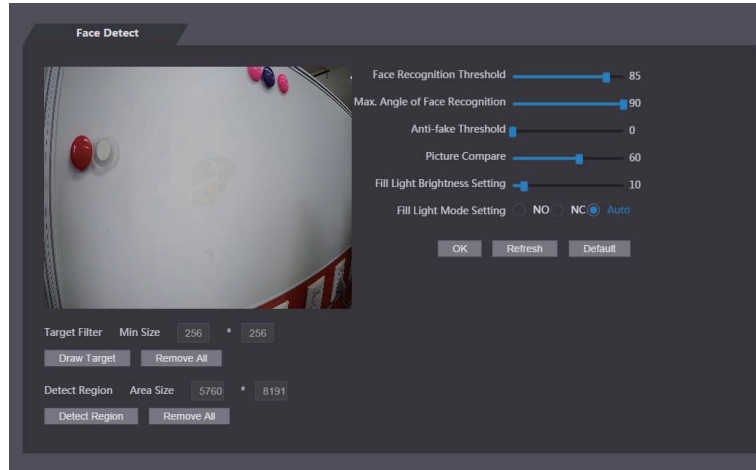Step 3   Click **OK** to finish the setting.

4.7 Face Detect

You can configure human face related parameters on this interface to increase the accuracy of the face recognition.

Step 1 Select **Face Detect**.

The **Face Detect** interface is displayed, see Figure 4-14.

Figure 4-14 Face detect

Step 2 See Table 4-2.

Table 4-2 Face detect parameter description

Parameter	Description
Face Recognition Threshold	The larger the value is, the higher the accuracy will be.
Max. Angle of Face Recognition	The larger the angle is, the wider range of the profiles will be recognized.
Anti-fake Threshold	This function prevents people from unlocking by human face images or human face models. The larger the value is, the more difficult face images or human face models can unlock the door.
Fill Light Brightness Setting	You can set fill light brightness.
Fill Light Mode Setting	There are three fill light modes. ● NO: NO means that the fill light is normally on. ● NC: NC means that the fill light is normally closed. ● Auto: Auto means the fill light will be automatically on when a motion detection event is triggered.
Draw Target	Click Draw Target, and then you can draw the minimum face detection frame. Click Remove All, and you can remove all the frames you drew.
Detect Region	Click Detect Region, move your mouse, and you can adjust the face

| Parameter	Description
	detection region. Click Remove All, and you can remove all the detection regions.

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

4.8 Upgrade

⚠️

● During upgrade, do not disconnect the power supply, network, and do not reboot or shut down the access standalone.
● Select correct upgrade files; otherwise the access standalone might be out of order.

Click **Upgrade**, and then the **Upgrade** interface is displayed. See Figure 4-15.

Figure 4-15 Upgrade
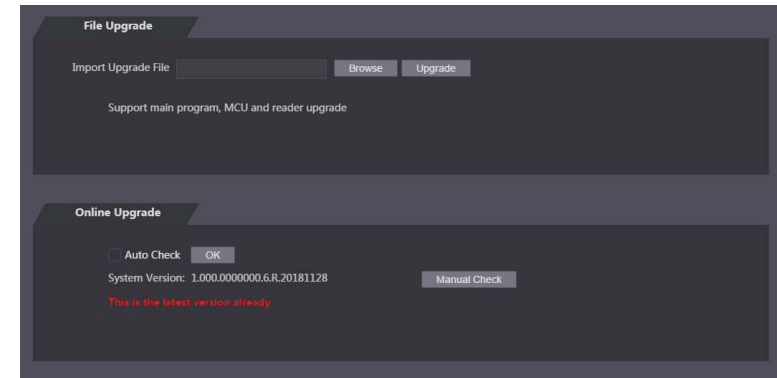
4.8.1 File Upgrade

The upgrade file should be a .bin file.

Step 1 Click **Browse**, and select the upgrade file.

Step 2 Click **Upgrade**, and then the upgrade will start.

After the upgrade, the access standalone will reboot itself automatically.

4.8.2 Online Upgrade

The Web can be upgraded online once the latest version is detected.

Step 1 Version detection

● Select **Auto Check**, click **OK**, and then the Web checks automatically to see whether there is a latest version. If there is a latest version, "A new version discovered" will be displayed at the top right corner of the Web.
● Select **Manual Check**, and then you can view the latest version of the access standalone system in the cloud.
  ◇ "This is the latest version already" will be displayed if the current version has already been the latest one.

◇ If a new version is detected, information about the new version including release date and modified content will be displayed.

Step 2 Click **Upgrade Now** after a new version is detected, and then the upgrade will start. After the upgrade, the access standalone will reboot itself automatically.

3 FAQ

1 **The access standalone cannot boot after power supply is connected.**

Check whether the 12V power supply is correctly connected, and whether the power button is pressed.

2 **Faces cannot be recognized after the access standalone is booted.**

◇ Make sure that Face is selected in the unlock mode. See "3.5.3 Unlock Mode".

◇ Make sure that Face is selected as unlock mode in Access > Unlock Mode > Group Combination. See "3.5.3.1 Unlock Mode".

3 **There is no output signal when the access standalone and the external controller is connected to the Wiegand port.**

Check whether the GND cables of access standalone and the external controller are connected.

4 **Configurations cannot be made after the administrator and password are forgotten.**

Delete administrators through the platform, or contact technical support to unlock the access standalone remotely.

5 **User information, fingerprints, and face images cannot be imported into the access standalone.**

Check whether titles of XML files and the title of the first row in the Excel spreadsheet were modified because the system will identify the files through their titles.

6 **When a user's face is recognized, but information of other users is displayed.**

Make sure that when importing human faces, there are no other people around. Delete the original face, and import it again.

Appendix 1 Notes of Face Recording

Notice

- Wearing glasses, hats or beards can all influence face registration.
- Do not let your hats cover your eyebrows.
- Do not change you beard style greatly and frequently before and after face registration; otherwise the recognition results might be influenced.
- Keep your face clean when doing face registration and verification.

Registration Description

You can register faces through the access standalone or through the platform. For registration through the platform, see the platform user manual.

📖

Do not shake your head or body, or the registration might fail.

Make your head be centered on the photo capture frame, tap 📷 . After the countdown stops, the face registration ends.

Appendix 2 Fingerprint Record Description

Notice

- Make sure that your fingers are clean and dry before recording your fingerprints.
- Press you finger to the fingerprint recording area, and make your fingerprint is centered on the recording area.

Fingers recommended

Forefingers, middle fingers, and ring fingers are recommended. Thumbs and little fingers cannot be put at the recording center easily.
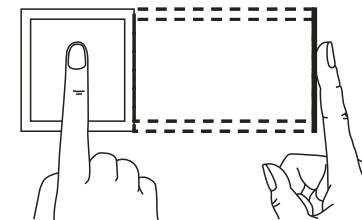
Appendix figure 2-1 Recommended fingers
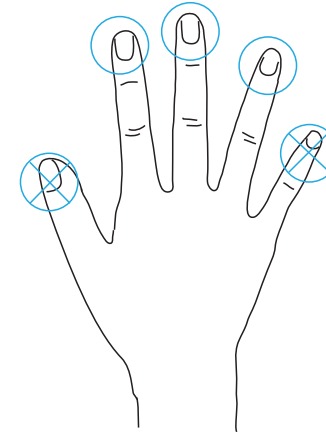
Finger pressing method

- Correct method

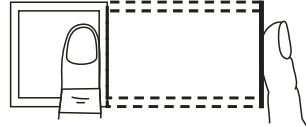Appendix figure 2-2 Correct finger pressing

- Incorrect method
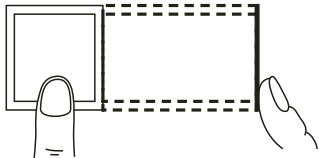
Appendix figure 2-3 Wrong finger pressing

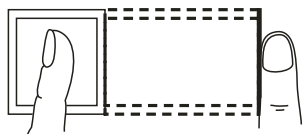Fingertip perpendicular to the record area

Fingertip not at the center of the record area

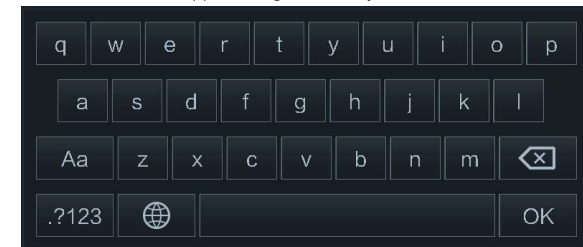Fingertip not at the center of the record area


Fingertip inclination

Appendix 3 Input Method Description

Input method of the access standalone supports Chinese characters, letters, numbers, and symbols.

Appendix figure 3-1 keyboards

- Tap [.?123], and then numbers and symbols can be typed.

- Tap [ABC], and then letters can be typed.

- Tap [🌐], and then Chinese characters can be typed.