

Face Recognition Access Controller

User's Manual








Foreword

General

This manual introduces the installation and basic operation of the face recognition access controller (hereinafter referred to as "access controller").

Safety Instructions

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

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

Revision History

Version	Revision Content	Release Time
V1.0.1	Updated the manual.	October 2022
V1.0.0	First release.	September 2020

About the Manual

- The manual is for reference only. If there is inconsistency between the manual and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the manual.
- The manual would be updated according to the latest laws and regulations of related jurisdictions. For detailed information, refer to the paper manual, CD-ROM, QR code or our official website. If there is inconsistency between paper manual and the electronic version, the electronic version shall prevail.
- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the manual. Please contact the customer service for the latest program and supplementary documentation.

- There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, 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 the company names in the manual are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurring when using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

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

Operation Requirement

- Do not expose the access controller to direct sunlight or heat source.
- Do not install the access controller in a humid or dusty area.
- Install the access controller horizontally at stable places to prevent it from falling.
- Do not drip or splash liquids onto the access controller; do not put on the access controller anything filled with liquids.
- Install the access controller at well-ventilated places and do not block its ventilation opening.
- Operate the access controller within rated input and output range.
- Do not disassemble the access controller by yourself.
- Transport, use and store the access controller under allowed humidity and temperature.

Electrical Safety

- Improper battery use might result in fire or explosion.
- When replacing battery, make sure that the same model is used.
- Use recommended power cables in the region under their rated specification.
- Use the power adapter provided with the access controller; otherwise, it might result in injury and device damage.
- The power supply should conform to the Safety Extra Low Voltage (SELV) requirements, and supply power with rated voltage that conforms to Limited Power Source in 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 earthing.
- The appliance coupler is a disconnection device. When using the coupler, keep the angle for easy operation.

Table of Contents

Foreword	I
Important Safeguards and Warnings	III
1 Overview	1
1.1 Introduction	1
1.2 Features	1
1.3 Dimension and Component	1
2 Installation	7
2.1 Cable Connection	7
2.2 Installation	9
3 System Operation	12
3.1 Initialization	12
3.2 Standby Interface	12
3.3 Unlocking Methods	13
3.3.1 Card	14
3.3.2 Face	14
3.3.3 Fingerprint	14
3.3.4 User Password	14
3.3.5 Administrator Password	14
3.4 Main Menu	14
3.5 User Management	16
3.5.1 Adding New Users	16
3.5.2 Viewing User information	18
3.6 Access Management	18
3.6.1 Period Management	19
3.6.2 Unlock	20
3.6.3 Alarm Configuration	23
3.6.4 Door Status	24
3.6.5 Lock Holding Time	24
3.7 Network Communication	24
3.7.1 IP Address	25
3.7.2 Serial Port Settings	26
3.7.3 Wiegand Configuration	27
3.8 System	27
3.8.1 Time	27
3.8.2 Face Parameter	28
3.8.3 Fill Light Mode Setting	28
3.8.4 Fill Light Brightness Setting	29
3.8.5 Volume Adjustment	29
3.8.6 IR Light Brightness Adjustment	29
3.8.7 FP Parameter	29
3.8.8 Restore to Factory Settings	29
3.8.9 Restart	29
3.9 USB	30
3.9.1 USB Export	30

3.9.2 USB Import	31
3.9.3 USB Update	31
3.9.4 Features	31
3.9.5 Privacy Setting	33
3.9.6 Result Feedback	34
3.10 Record	36
3.11 Auto Test	37
3.12 System Info	38
4 Web Operation	39
4.1 Initialization	39
4.2 Login	41
4.3 Resetting the Password	41
4.4 Alarm Linkage	43
4.4.1 Setting Alarm Linkage	43
4.4.2 Alarm Log	45
4.5 Call Configuration	45
4.5.1 Configuring the Access Controller	45
4.5.2 SIP Server	47
4.5.3 Door Station Management	48
4.5.4 Indoor Monitor Management	50
4.5.5 Configuring the Managing Device	52
4.5.6 Online Status	53
4.5.7 Call Logs	54
4.6 Data Capacity	54
4.7 Video Setting	55
4.7.1 Data Rate	55
4.7.2 Image	56
4.7.3 Exposure	57
4.7.4 Motion Detection	58
4.7.5 Volume Setting	59
4.7.6 Image Mode	60
4.7.7 Local Coding	60
4.8 Face Detect	61
4.9 Network Setting	62
4.9.1 TCP/IP	62
4.9.2 Port	64
4.9.3 Register	64
4.9.4 P2P	64
4.10 Date Setting	65
4.11 Safety Management	66
4.11.1 IP Authority	66
4.11.2 Systems	67
4.12 User Management	68
4.12.1 Adding Users	68
4.12.2 Modifying User Information	68
4.12.3 Onvif User	68
4.13 Maintenance	69

4.14 Configuration Management.....	69
4.14.1 Config Mgmt.	70
4.14.2 Wiegand Serial Port Setting.....	70
4.15 Upgrade	70
4.15.1 Version Information	71
4.15.2 Online User	71
4.16 System Log	71
4.16.1 Querying Logs	72
4.16.2 Backup Logs	72
4.17 Admin Log.....	72
4.18 Exit.....	73
5 Smart PSS Configuration	74
5.1 Login	74
5.2 Adding Devices.....	74
5.2.1 Auto Search.....	74
5.2.2 Manual Add.....	75
5.3 Adding Users.....	76
5.3.1 Card Type Selection.....	77
5.3.2 Adding One User.....	78
5.4 Adding Door Group.....	80
5.5 Access Permission Configuration.....	81
5.5.1 Giving Permission by Door Group	81
5.5.2 Giving Permission by User ID	83
Appendix 1 Cybersecurity Recommendations	85

1 Overview

1.1 Introduction

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

1.2 Features

- Supports face unlock, IC card unlock, fingerprint unlock, and password unlock; unlock by period.
- Face detection box is designed; when faces appear at the same time, the largest face is recognized first; the maximum face size can be configured on the web.
- 2MP wide-angle WDR lens; with auto/manual fill light.
- Face-camera distance: 0.3 m–2.0 m; human height: 0.9 m–2.4 m.
- With face recognition algorithm, the access controller can recognize more than 360 positions on human face.
- Face verification accuracy > 99.5%; low false recognition rate.
- Supports profile recognition; the profile angle is 0°–90°.
- Supports liveness detection.
- Supports duress alarm and tamper alarm.
- Supports general users, duress users, patrol users, blocklist users, VIP users, guest users, and special users.
- Various unlock status display modes protect user privacy.

1.3 Dimension and Component

The access controller has two types: 7-inch and 10-inch access controllers. See Figure 1-1 to Figure 1-6.

The 7-inch access controller has two models: Model A and model B. See Figure 1-1 to Figure 1-4.

7-Inch Access Controller

Figure 1-1 Dimensions and components of model A (1) (mm [inch])

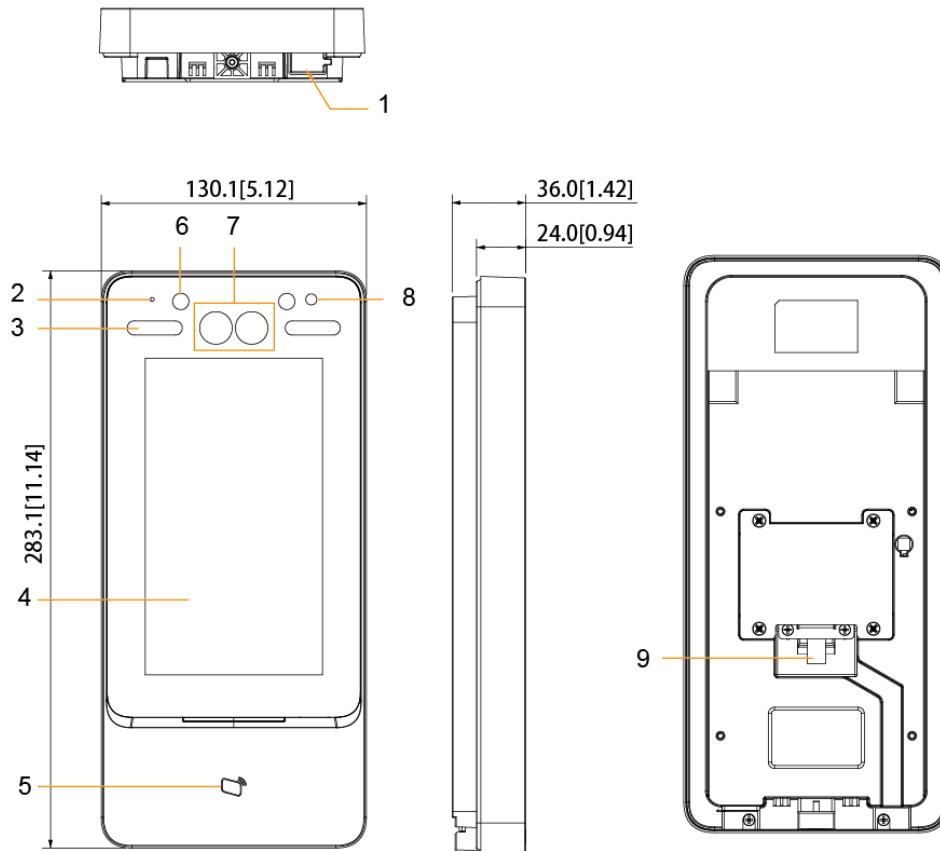


Table 1-1 Component description (1)

No.	Name	No.	Name
1	USB port	6	IR light
2	MIC	7	Dual camera
3	White light illuminator	8	Phototransistor
4	Display	9	Cable entry
5	Card swiping area	–	–

Figure 1-2 Dimensions and components of model A (2) (mm [inch])

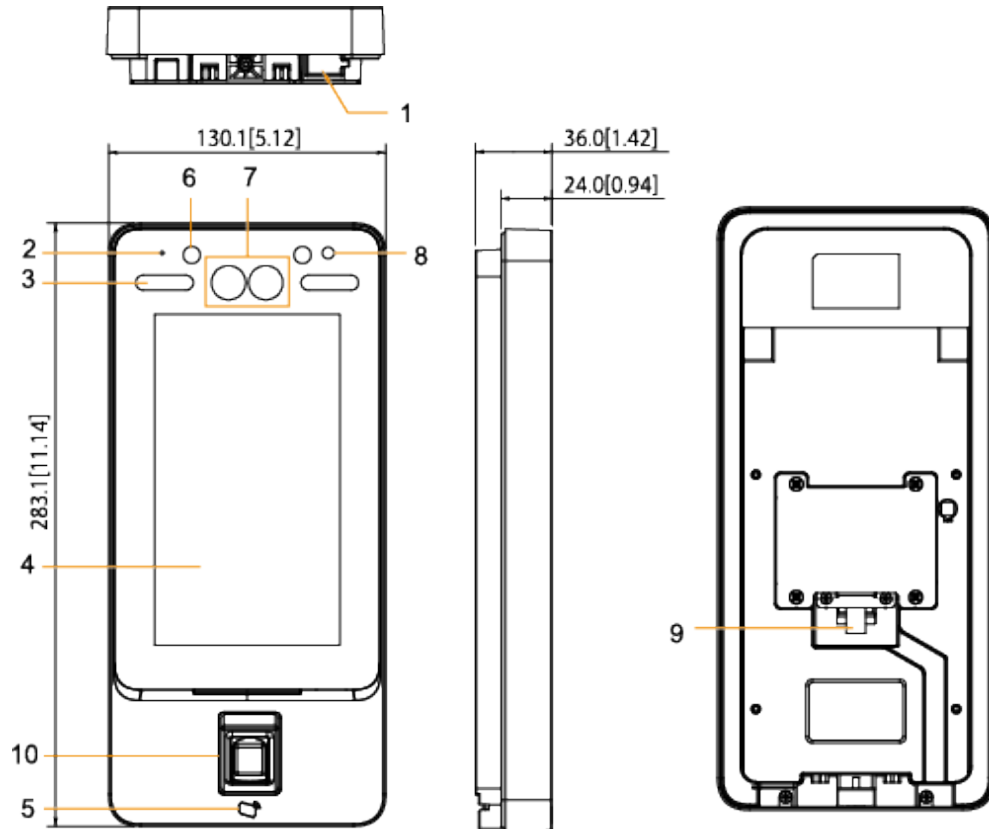


Table 1-2 Component description (2)

No.	Name	No.	Name
1	USB port	6	IR light
2	MIC	7	Dual camera
3	White fill light	8	Phototransistor
4	Display	9	Cable entry
5	Card swiping area	10	Fingerprint sensor

Figure 1-3 Dimensions and components of model B (1) (mm [inch])

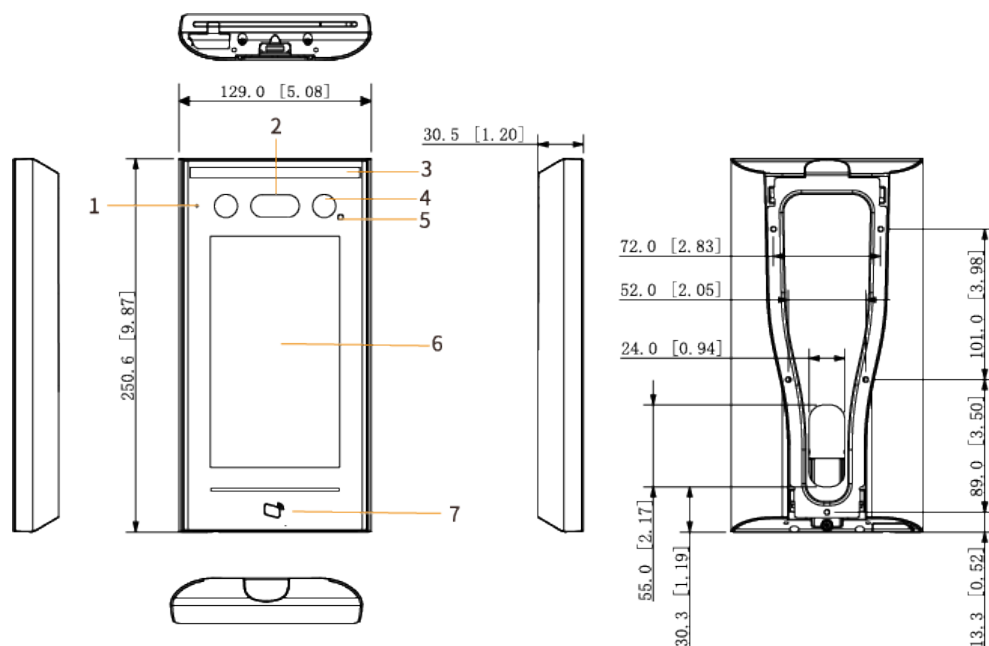


Table 1-3 Component description (3)

No.	Name	No.	Name
1	MIC	5	Phototransistor
2	Dual camera	6	Display
3	White fill light	7	Card swiping area
4	IR light	—	—

Figure 1-4 Dimensions and components of model B (2) (mm [inch])

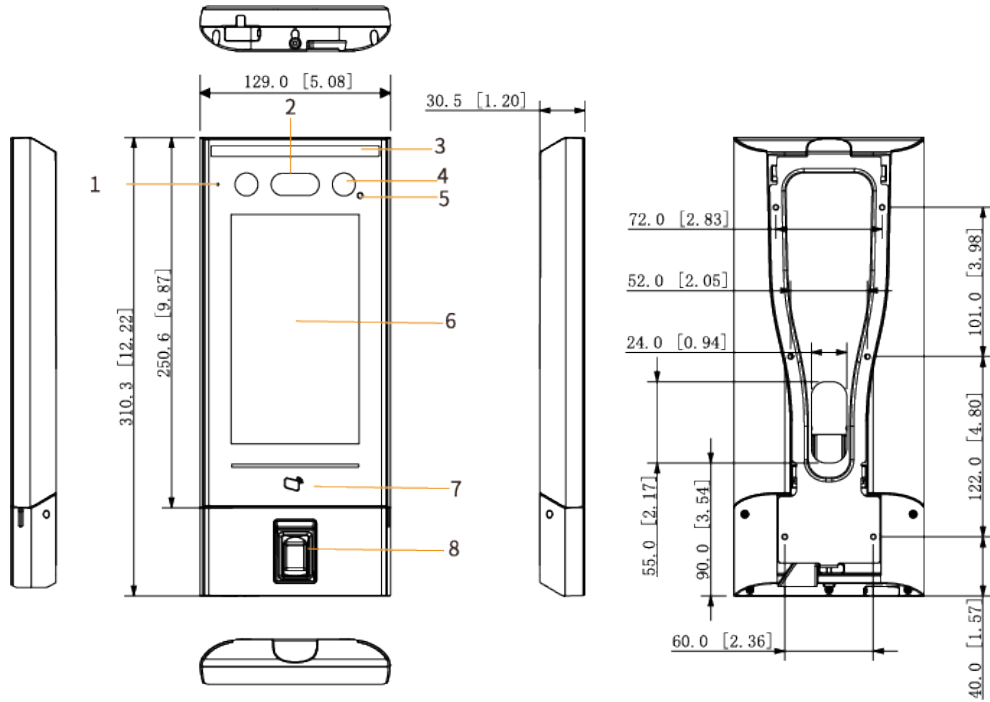


Table 1-4 Component description (4)

No.	Name	No.	Name
1	MIC	5	Phototransistor
2	Dual camera	6	Display
3	White fill light	7	Card swiping area
4	IR light	8	Fingerprint sensor

10-Inch Access Controller

Figure 1-5 Dimensions and components (1) (mm [inch])

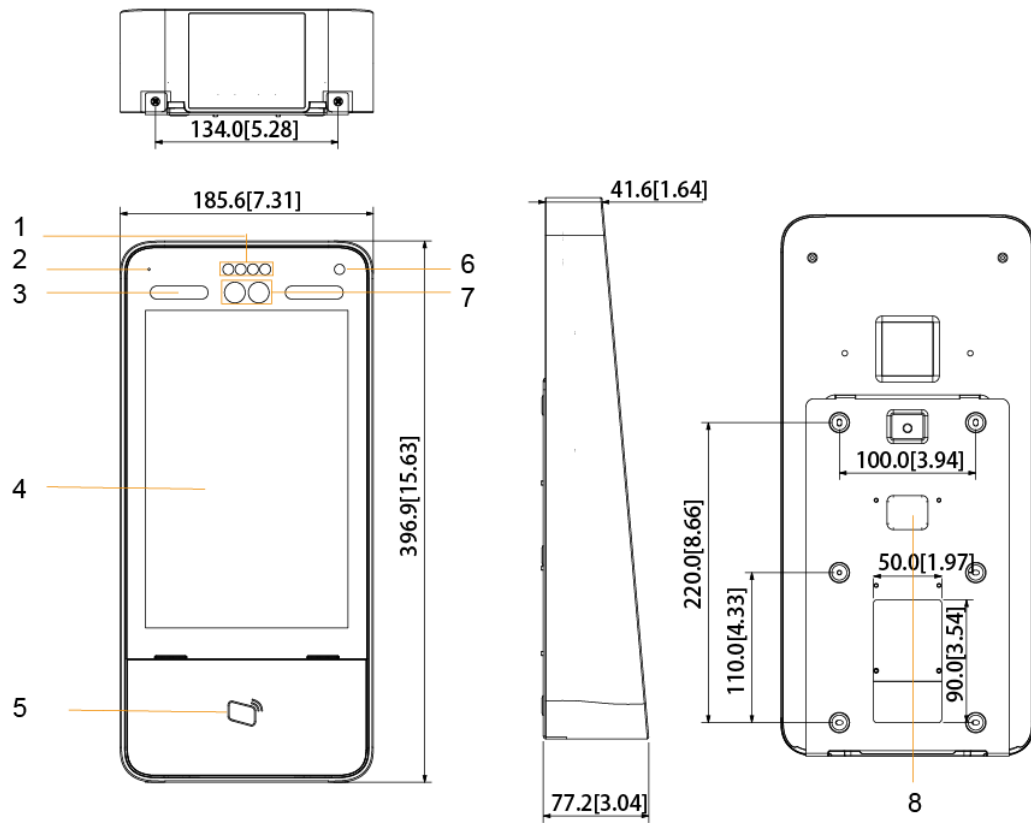


Table 1-5 Component description (1)

No.	Name	No.	Name
1	IR light	6	Phototransistor
2	MIC	7	Dual camera
3	White fill light	8	Cable entry
4	Display	–	–
5	Card swiping area	–	–

Figure 1-6 Dimensions and components (2) (mm [inch])

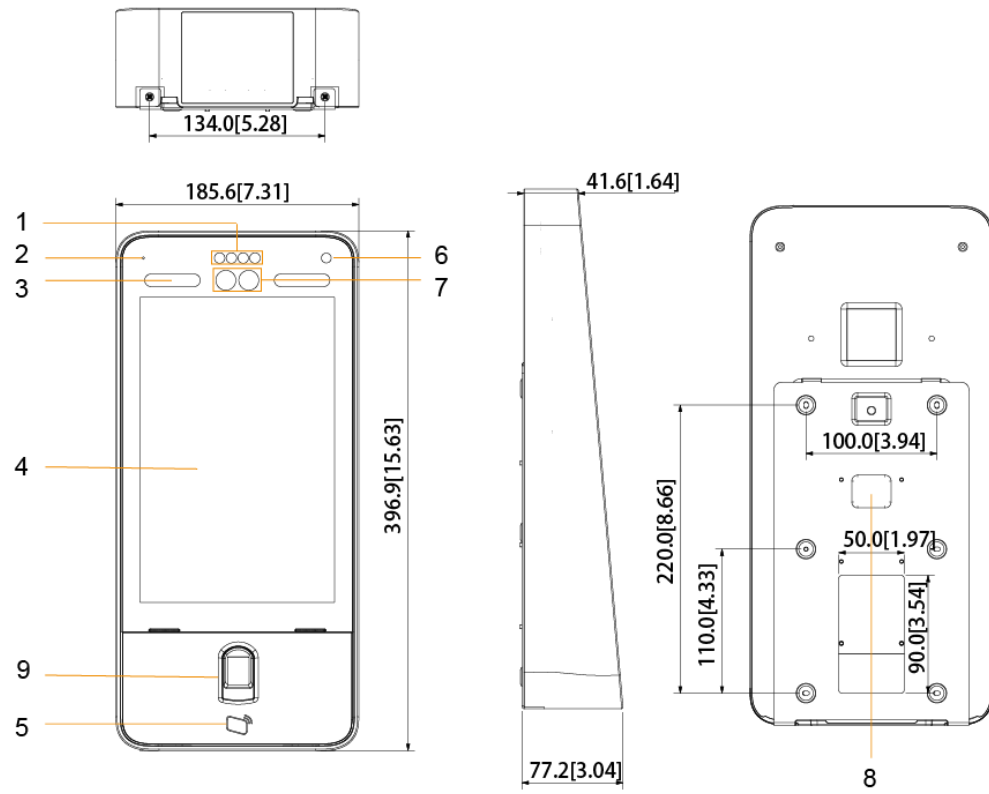


Table 1-6 Component description (2)

No.	Name	No.	Name
1	IR light	6	Phototransistor
2	MIC	7	Dual camera
3	White fill light	8	Cable entry
4	Display	9	Fingerprint sensor
5	Card swiping area	—	—

2 Installation

2.1 Cable Connection

The access controller needs to be connected to devices like sirens, readers, and door contacts.

Figure 2-1 Cable connections

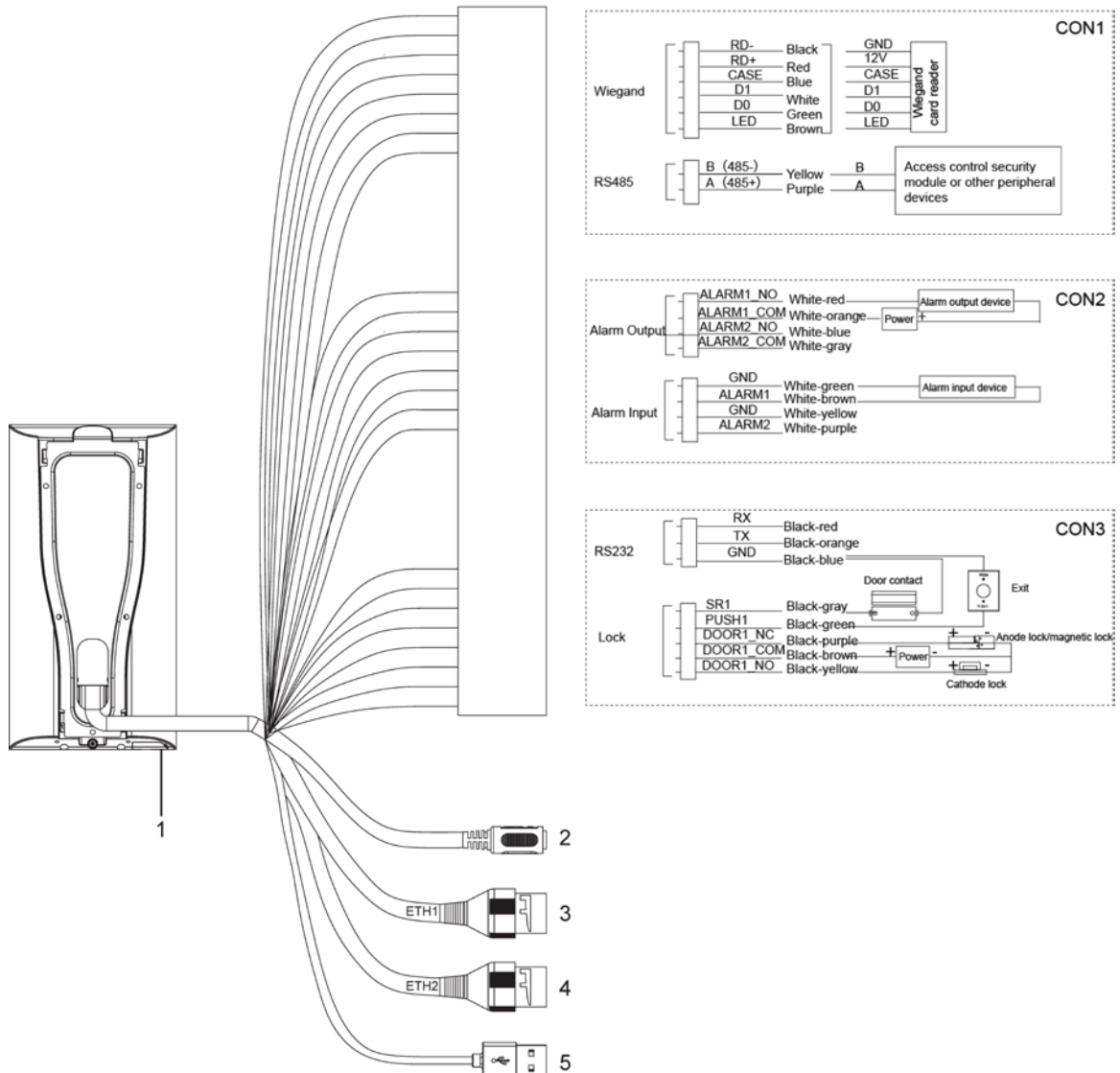




Table 2-1 Component description

No.	Name
1	USB port
2	Power port
3	Ethernet port
4	Ethernet port (only supported by 7-inch model B access controllers)
5	USB port (only supported by 7-inch model B access controllers)

For detail function of each port, see the table below.

Table 2-2 Port description

Port	Cable color	Cable name	Description
CON1	Black	RD-	Negative electrode of external card reader power supply.
	Red	RD+	Positive electrode of external card reader power supply.
	Blue	CASE	Tamper alarm input of the external card reader.
	White	D1	Wiegand D1 input (connected to external card reader)/output (connected to controller).
	Green	D0	Wiegand D0 input (connected to external card reader)/output (connected to controller).
	Brown	LED	Connected to external reader and verify card number.
	Yellow	B	<p>RS-485 negative electrode input (connected to external card reader)/output (connected to controller, or connected to door control security module).</p>  <ul style="list-style-type: none"> If the security module is enabled, you need to purchase access control security module separately. The security module needs separate power supply to provide power. Once the security module is enabled, the exit button, lock control and firefighting linkage will be invalid.
	Purple	A	<p>RS-485 positive electrode input (connected to external card reader)/output (connected to controller, or connected to door control security module).</p>  <ul style="list-style-type: none"> If the security module is enabled, you need to purchase access control security module separately. The security module needs separate power supply to provide power. Once the security module is enabled, the exit button, lock control and firefighting linkage will be invalid.
CON2	White and red	ALARM1_NO	Alarm 1 normally open output port.
	White and orange	ALARM1_CO M	Alarm 1 common output port.
	White and blue	ALARM2_NO	Alarm 2 normally open output port.
	White and gray	ALARM2_CO M	Alarm 2 common output port.
	White and green	GND	Connected to the common GND port.
	White Brown	ALARM1	Alarm 1 input port.

Port	Cable color	Cable name	Description
	White and yellow	GND	Connected to the common GND port.
	White and purple	ALARM2	Alarm 2 input port.
CON3	Black and red	RX	RS-232 receiving port.
	Black and orange	TX	RS-232 sending port.
	Black and blue	GND	Connected to the common GND port.
	Black and gray	SR1	Used for door contact detection.
	Black and green	PUSH1	Door open button of door No.1
	Black and brown	DOOR1_COM	Lock control common port.
	Black and yellow	DOOR1_NO	Lock control normally open port.
	Black and purple	DOOR1_NC	Lock control normally closed port.

2.2 Installation

Installation method of model A and model B are the same. Make sure that the distance between the lens and ground is 1.4 meters. The installation of 2-inch model B is an example.

Figure 2-2 Installation height

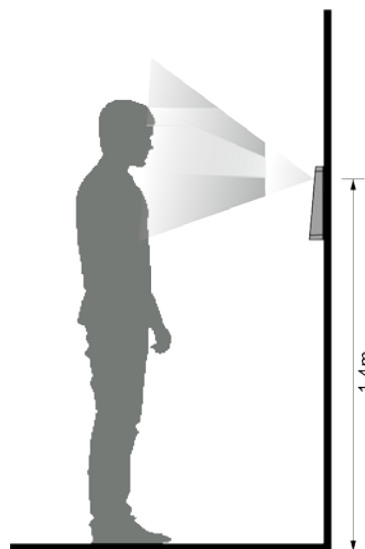


Figure 2-3 Installation diagram (1)

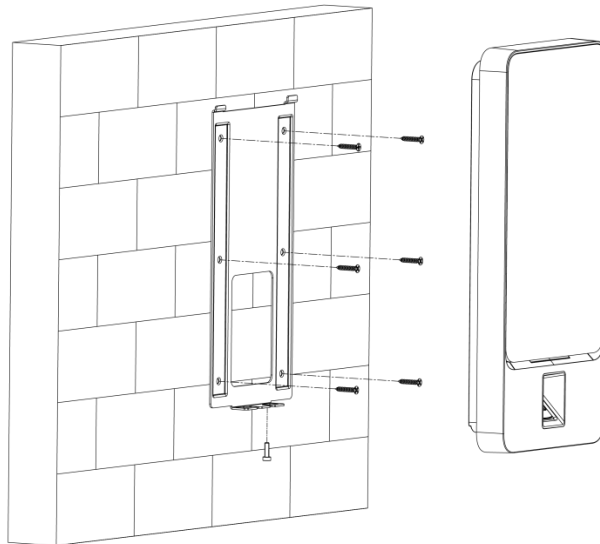
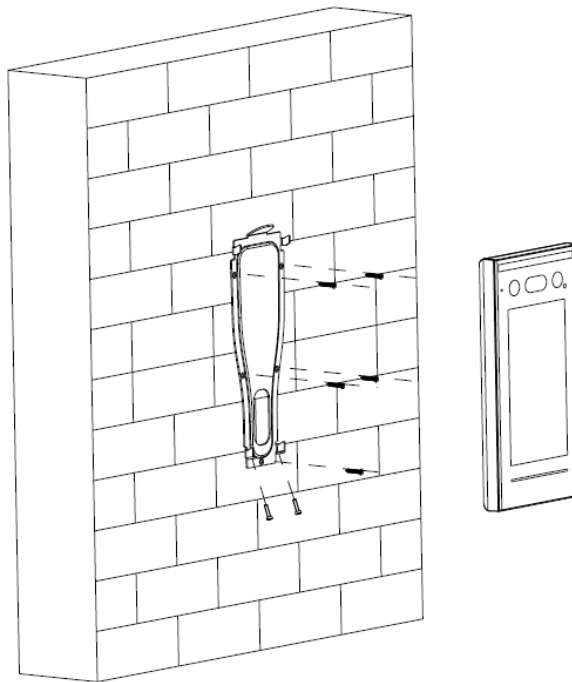


Figure 2-4 Installation diagram (2)



Installation Procedure

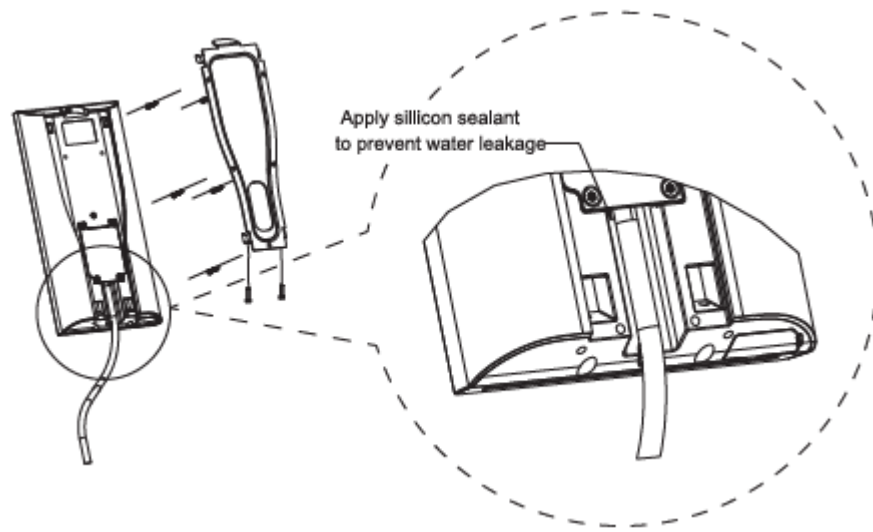
Here takes a 7-inch model A access controller as an example.

- 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 controller. See "2.1 Cable Connection."
- Step 4** Hang the access controller on the bracket hook.
- Step 5** Tighten the screws at the bottom of the access controller.
The installation is completed.



You need to apply silicon sealant to the cable outlet of 7-inch model B access controller.

Figure 2-5 Applying silicon sealant

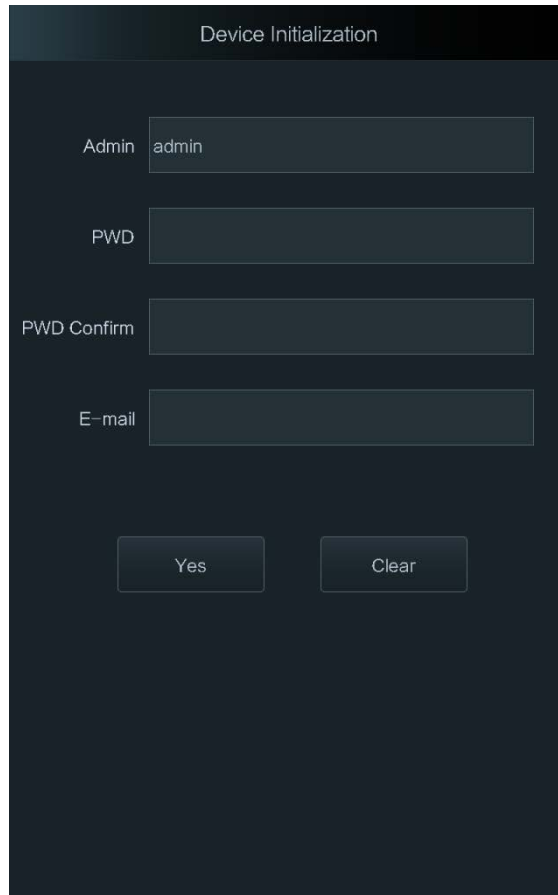


3 System Operation

3.1 Initialization

Set administrator password and email when the access controller is turned on for the first time; otherwise the access controller cannot be used.

Figure 3-1 Initialization



Device Initialization

Admin admin

PWD

PWD Confirm

E-mail

Yes Clear



- Administrator and password set on this interface are used to log in to the web management platform.
- The administrator password can be reset through the email address you entered if the administrator forgets the administrator password.
- The password must 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 ' " ; : &).

3.2 Standby Interface

You can unlock the door through faces, passwords, cards and fingerprints.



If there are no operations in 30 seconds, the access controller will go to the standby mode.

Figure 3-2 Homepage

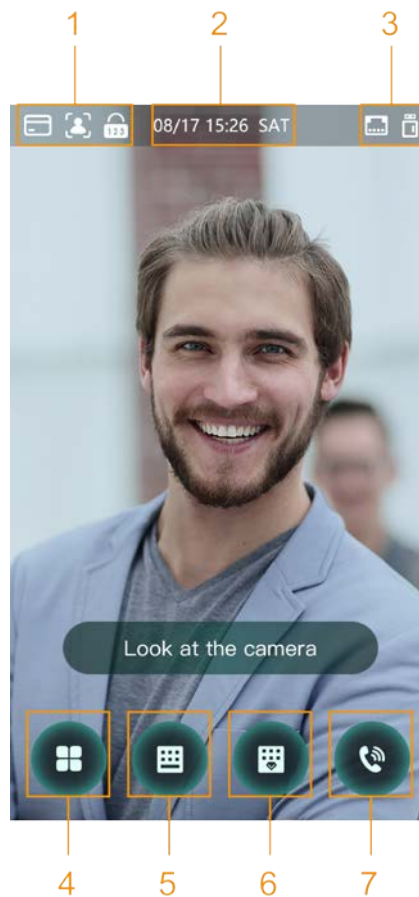




Table 3-1 Homepage description

No.	Description
1	<p>Unlock methods: Card, face, fingerprint, and password.</p> <p> When card, face, fingerprint, and password are all set as unlock mode, the password icon will not be displayed at the upper-left corner of the access controller.</p>
2	Date & Time: Current date and time.
3	Network status and USB status.
4	<p>Main menu icon.</p> <p> Only the administrator can enter the main menu.</p>
5	Password unlock icon.
6	Administrator password unlock icon.
7	Tap to call other devices.

3.3 Unlocking Methods

You can unlock the door through faces, passwords, fingerprints, and cards.

3.3.1 Card

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

3.3.2 Face




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

3.3.3 Fingerprint

Place your fingerprint at the fingerprint sensor to unlock the door.

3.3.4 User Password

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



- Step 1 Tap  on the homepage.
- Step 2 Enter the User ID, and then tap .
- Step 3 Enter the User password, and then tap .
- The door is unlocked.

3.3.5 Administrator Password

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




Administrator password cannot be used when NC is selected at "3.6.1.5 NC Period."

- Step 1 Tap  on the homepage.
- Step 2 Tap **Please Enter Administrator PWD.**
- Step 3 Enter the administrator password, and then tap .
- The door is unlocked.

3.4 Main Menu

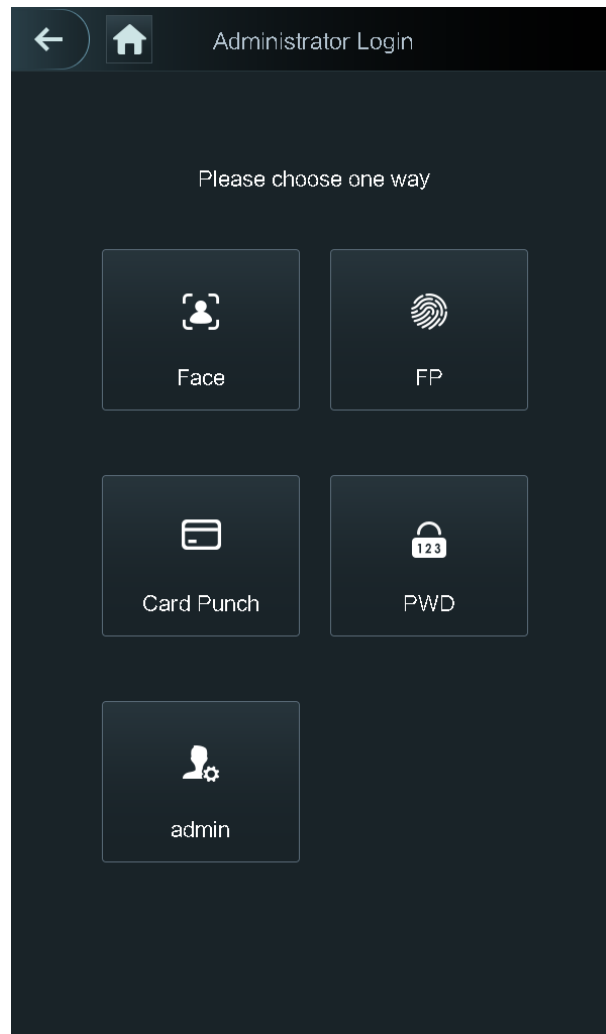
Administrators can add users of different levels, set access-related parameters, do network configuration, view access records and system information, and more in the main menu.

- Step 1 Tap  on the standby interface.



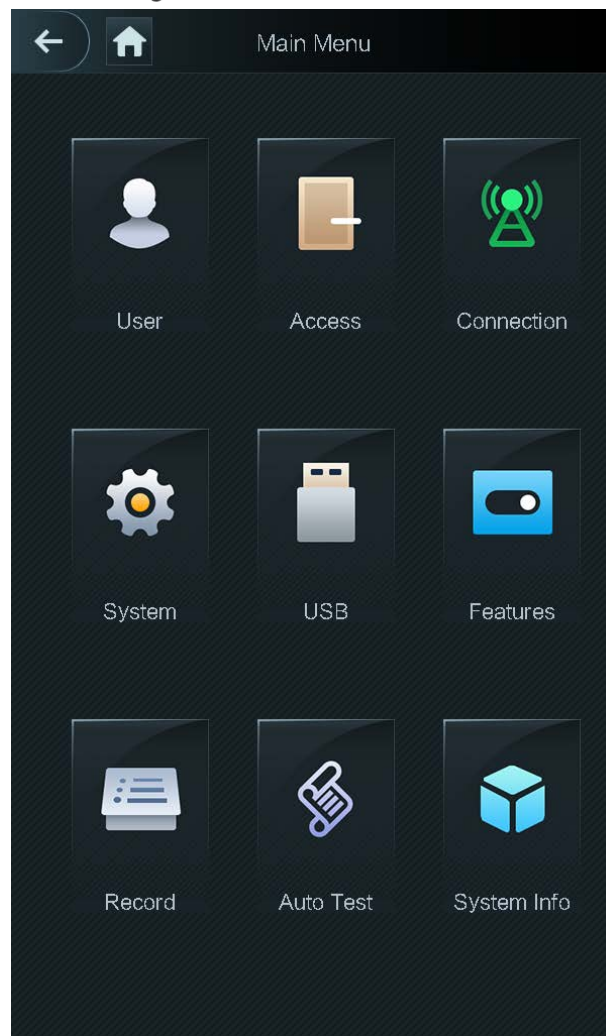
Different modes support different unlock methods, and the actual interface shall prevail.

Figure 3-3 Administrator login



Step 2 Select a main menu entering method.

Figure 3-4 Main Menu



3.5 User Management

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

3.5.1 Adding New Users


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



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

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


Figure 3-5 New User Info






Parameter	Value
User ID	1
Name	
FP	0
Face	0
Card	0
PWD	
User Level	User
Period	255-Default
Holiday Plan	255-Default
Valid Date	2037-12-31
User Level	General
Use Time	Unlimited

Step 2 Configure parameters on the interface.

Table 3-2 New user parameter description

Parameter	Description
User ID	ID that helps identify the user. The IDs can be numbers, letters, and their combinations, and the maximum length of the ID is 32 characters.
Name	You can enter names with at most 32 characters (including numbers, symbols, and letters).
FP	<p>At most three fingerprints of one user can be recorded, and one fingerprints need to be verified three times.</p> <p>You can enable the duress FP function under each fingerprint, and only one of the three fingerprints can be the duress fingerprint. After enabling the duress function, an alarm will be triggered if a duress fingerprint is used to unlock the door.</p>  <p>It is not recommended that you select the first fingerprint as the duress fingerprint.</p>
Face	Make sure that your face is centered on the picture capturing frame and the access controller will take a picture of the new user's face automatically. For details, see the Quick Start Guide .

Parameter	Description
Card	<p>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 controller.</p> <p>You can enable the Duress Card function on the card registration interface. After enabling the duress function, an alarm will be triggered if a duress card is used to unlock the door.</p>  <p>Card unlock is only supported by certain models.</p>
PWD	The door unlocking password. The maximum length of the is 8 digits.
User Level	<p>You can select a user level for new users. There are two options:</p> <ul style="list-style-type: none"> ● User: Users only have door unlock permission. ● Admin: Administrators can not only unlock the door but also configure parameters.  <p>Administrator identity authentication is needed whether there is an administrator in the access controller or not.</p>
Period	The period in which the user can unlock the door.
Holiday Plan	The holiday plan in which the user can unlock the door.
Valid Date	The period during which the unlocking information of the user is valid.
User Level	<p>There are six levels:</p> <ul style="list-style-type: none"> ● General: General users can unlock the door normally. ● Blocklist: When users in the blocklist unlock the door, service personnel will get a prompt. ● Guest: Guests are allowed to unlock the door certain times. ● Patrol: Patrolling users can get their attendance tracked, but they have no unlock authority. ● VIP: When VIP unlocks the door, service personnel will get a prompt. ● Special: When special people unlock the door, there will be a delay of 5 seconds before the door is closed.
Use Time	When the user level is Guest , you can set the maximum number of times that the user can unlock the door.

Step 3 Tap  to save the configuration.

3.5.2 Viewing User information

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

3.6 Access Management

You can do access management on period, unlock mode, alarm, door status, and lock holding time.

Tap **Access** to go to the access management interface.

3.6.1 Period Management

You can set periods, holiday periods, holiday plan periods, door normally open periods, door normally closed periods, and remote verification periods.


3.6.1.1 Period Config

You can configure 128 periods (weeks) whose number range is 0–127. You can set four periods on each day of a period (week). Users can only unlock the door in the defined periods.

3.6.1.2 Holiday Group

You can set group holidays, and then you can set plans for holiday groups. You can configure 128 groups whose number range is 0–127. You can add 16 holidays into a group. Configure the start time and end time of a holiday group, and then users can only unlock the door in the defined periods.



You can enter names with 32 characters (including numbers, symbols, and letters). Tap  to save the holiday group name.

3.6.1.3 Holiday Plan

You can add holiday groups into holiday plans. You can use holiday plans to manage user access authority in different holiday groups. Users can only unlock the door in the defined periods.

3.6.1.4 NO Period

If a period is added to the NO period, then the door is normally open in that period.



The NO/NC period permissions are higher than permissions in other periods.

3.6.1.5 NC Period



If a period is added to the NC period, then the door is normally closed in that period. Users can not unlock the door in this period.

3.6.1.6 Remote Verification Period

Configure a remote verification period, and then when unlock doors during the period you configured, remote verification is required. To unlock the door in this period, a door unlock instruction sent by the management platform is needed.



You need to enable the **Remote Verification Period**.

-  means enabled.
-  means not enabled.

3.6.2 Unlock

There are three unlock modes: Unlock mode, unlock by period, and group combination.



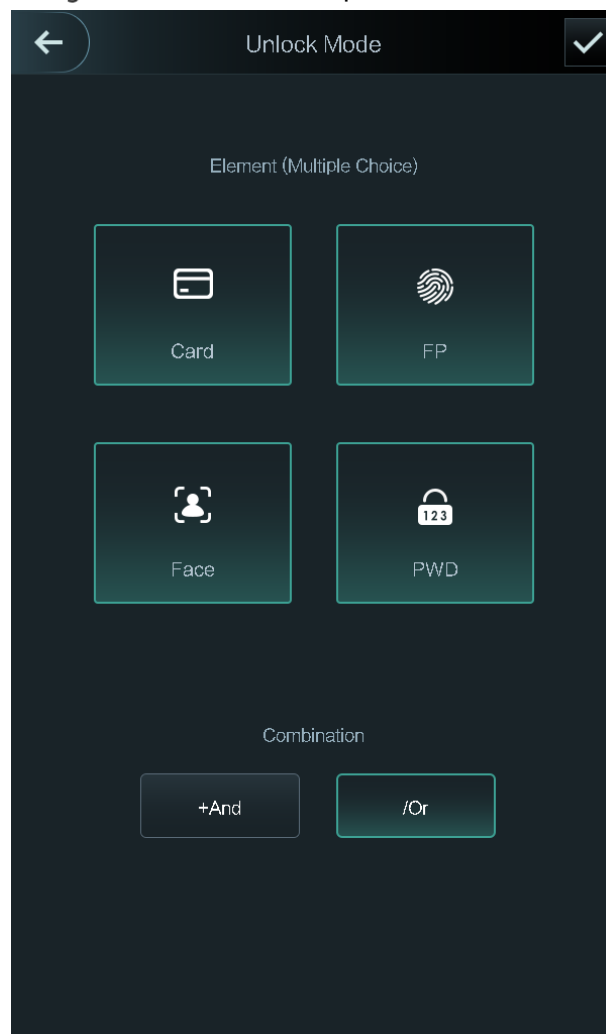
Unlock modes vary with controller access models, and the actual controller access shall prevail.

3.6.2.1 Unlock Mode

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

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

Figure 3-6 Element (multiple choice)



Step 2 Select unlock mode(s).





Tap a selected unlock mode again to cancel selecting the unlock mode.

Step 3 Select a combination mode.

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

Step 4 Tap  to save the settings.

Step 5 Enable the **Unlock Mode**.

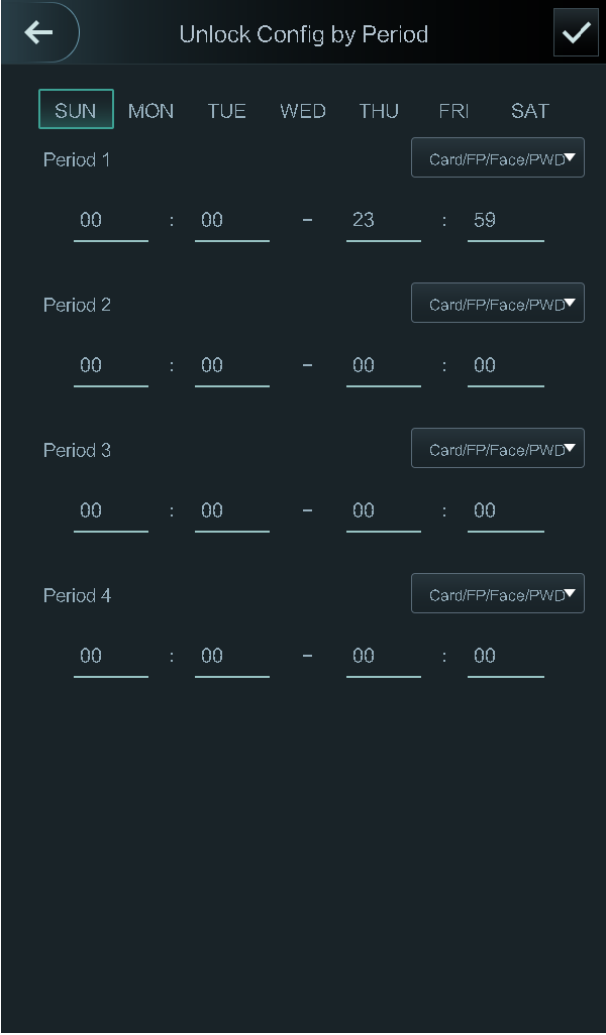
-  means enabled.
-  means not enabled.

3.6.2.2 Unlock by Period


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

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



Figure 3-7 Unlock by period



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

Step 3 Tap  to save the settings.

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

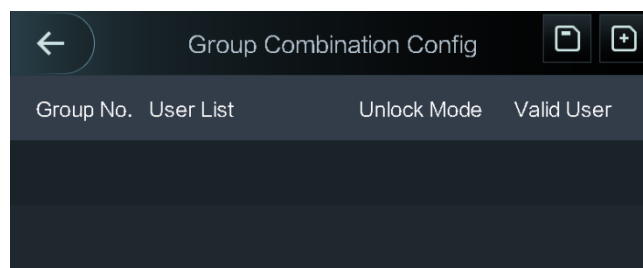
-  means enabled.
-  means not enabled.

3.6.2.3 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 **Access > Unlock Mode > Group Combination**.

Figure 3-8 Group Combination



Step 2 Tap  to create a group.

Figure 3-9 Add a group

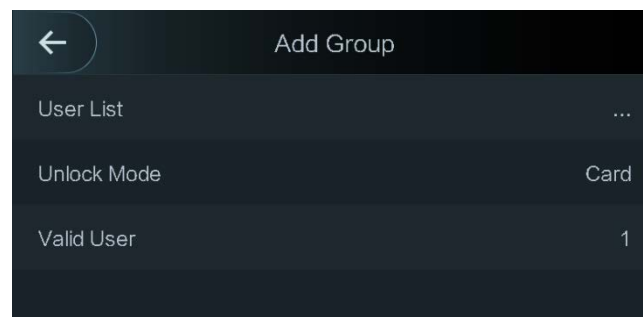




Table 3-3 Group parameter



Parameter	Description
User List	Add users to the newly created group. <ol style="list-style-type: none">1. Tap User List.2. Tap  then enter a user ID.3. Tap  to save the settings.
Unlock Mode	There are four options: Card , FP , PWD and Face .

Parameter	Description
Valid User	<p>Valid users are the ones that have unlock permission. Doors can be unlocked only when the number of users to unlock the doors equals the number valid users.</p> <ul style="list-style-type: none"> Valid users cannot exceed the total number of users in a group. If valid users equal total users 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 number of valid users.

Step 3 Tap  to go back to the previous interface.

Step 4 Tap  to save the settings.

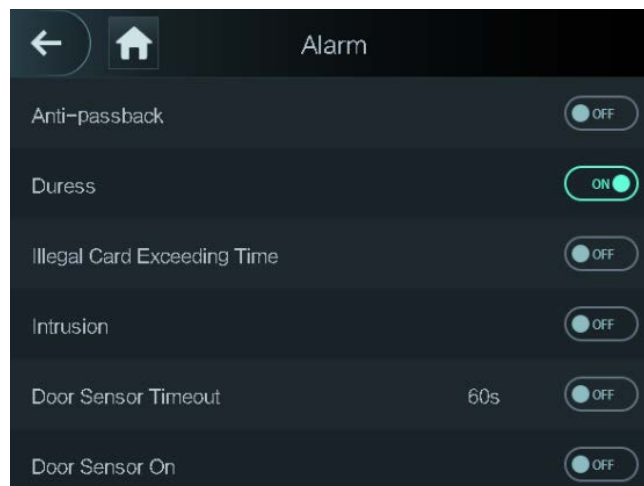
Step 5 Enable the **Group Combination**.

-  means enabled.
-  means not enabled.

3.6.3 Alarm Configuration

Select **Access > Alarm**, and then administrators can manage visitor unlock authority through alarm configuration.

Figure 3-10 Alarm





-  means enabled.
-  means not enabled.

Table 3-4 Parameters on the alarm interface

Parameter	Description
Anti-passback	<ul style="list-style-type: none"> If a person unlocks the door with the identity checked by the access controller, but when the person gets out without getting the identity checked by the access controller, an alarm will be triggered and the person will have no authority to unlock the door any more. If a person gets inside a building or a room without swiping the card, and the person swipes the card to get out, then the person will have no authority to unlock the door any more.
Duress	After enabling the duress function, 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	<p>A timeout alarm will be triggered if the time that a user takes to unlock the door exceeds the Door Sensor Timeout time.</p> <p>The Door Sensor Timeout time range is 1–9999 seconds.</p>
Door Sensor On	Only when the Door Sensor On is enabled can the intrusion alarm and door sensor timeout alarm be triggered.

3.6.4 Door Status

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

- **NO**: Select it and the door stays open.
- **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.

3.6.5 Lock Holding Time

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

3.7 Network Communication

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

3.7.1 IP Address

3.7.1.1 IP Configuration

Configure an IP address for the access controller and connect it to the network.

Figure 3-11 IP address configuration

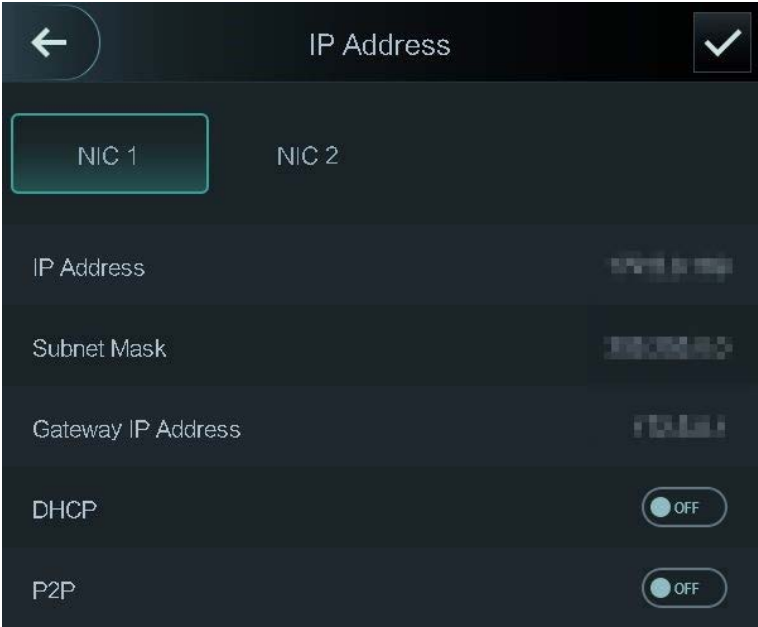


Table 3-5 IP configuration parameters

Parameter	Description
NIC 1/2	Tap to configure parameters for the Ethernet port.
IP Address/Subnet Mask/Gateway IP Address	The IP address, subnet mask, and gateway IP address must be on the same network segment.
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 (peer-to-peer) technology enables users to manage devices without requiring DDNS, port mapping or transit server.



- Make sure that the computer used to log in to the web is in the same LAN with the access controller.
- 7-inch model B access controllers of have dual NICs. The default IP address for ETH1 is 192.168.1.108, and for ETH2 is 192.168.2.108.

3.7.1.2 Active Register

Active register allows you to connect the access controller to the management platform, and then manage it through the management platform.



Because configurations can be cleared on the management platform, and the access controller can be initialized, you need to protect the platform access permission in case of data loss caused by improper operation.

For active register parameter, see the table below.

Table 3-6 Active register

Name	Parameter
Server IP Address	IP address of the managing platform.
Port	Port number of the managing platform.
Device ID	Subordinate device number on the managing platform.

3.7.1.3 Wi-Fi

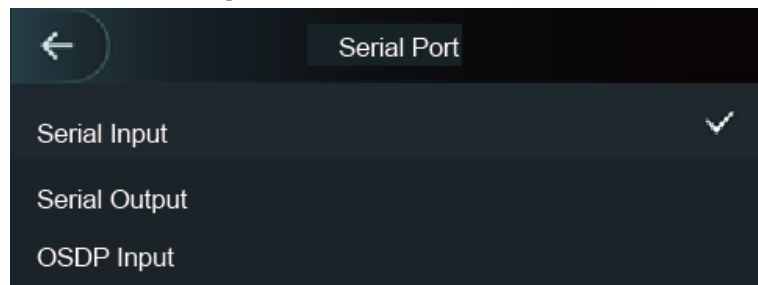
You can connect the access controller to the network through Wi-Fi if the access controller has Wi-Fi function.

3.7.2 Serial Port Settings

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

Select **Connection > Serial Port**.

Figure 3-12 Serial port



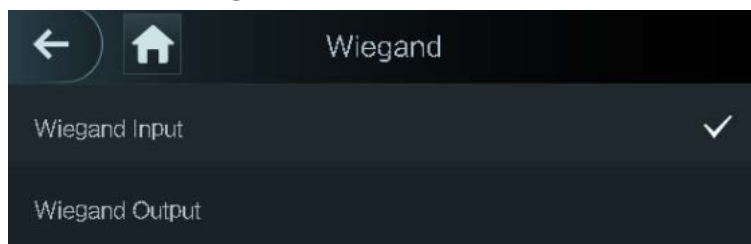
- Select **Serial Input** when external devices are with card reading and writing functions are connected to the access controller. **Serial Input** is selected to enable access card information to be sent to the access controller and the management platform.
- For access controllers with face recognition, fingerprint recognition, card reading and writing functions, if you select **Serial Output**, access controller will send lock/unlock information to the access controller. There are two types of lock/unlock information:
 - ◇ User ID
 - ◇ Card No.
- Select **OSDP Input** when card reader of OSDP protocol is connected to the access controller. The access controller can send card information to the management platform.

3.7.3 Wiegand Configuration

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

Select **Connection > Weigand**.

Figure 3-13 Weigand



- Select **Weigand Input** when an external card swipe mechanism is connected to the access controller.
- Select **Weigand Output** when the access controller works as a reader that can be connected to the controller.

Table 3-7 Weigand output

Parameter	Description
Weigand Output Type	The Weigand Output Type determines the card number or the digit of the number that can be recognized by the access controller. <ul style="list-style-type: none">• Weigand26, three bytes, six digits.• Weigand34, four bytes, eight digits.• Weigand66, 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. <ul style="list-style-type: none">• User ID: If User ID is selected, and then user ID will be output.• Card No.: If Card No. is selected, and then card number will be output.

3.8 System

3.8.1 Time

You can set up date format, date, time, DST, NTP check, and time zone.



- When you select **Network Time Protocol** (NTP), you need to enable the **NTP Check** function first.
- Server IP Address: enter the IP address of the time server, time of the access controller will be synchronized with the time server.
- Port: Enter the port number of the time server.
- Interval (min): NPT check interval. Tap the save icon to save.

3.8.2 Face Parameter

Figure 3-14 Face parameter




Tap a parameter and do configuration, and then tap .

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.
Max. Angle of Face Recognition	You can set the control panel shooting angle of profiles. The larger the value is, the wider range of the profiles will be recognized.
Pupillary Distance	Pupillary distance is the pixel value of the image between the centers of the pupils in each eye. You need to set an appropriate value so that the access controller can recognize faces as needed. The value changes according to the face sizes and the distance between faces and the lens. The closer the face is to the lens, the greater the value should be. If an adult is 1.5 meters away from the lens, the pupillary distance value can be within 50 to 70.
Recognition Timeout	When a person who does not have the access authority stands in front of the access controller and gets the face recognized, the controller will prompt that face recognition failed. The prompt interval is called recognition timeout.
Invalid Face Prompt Interval (S)	When a face has no access permission stands in front of the access controller, the controller will prompt that the face is invalid. The prompt interval is invalid face prompt interval.
Anti-fake Threshold	This function prevents people from unlocking by human face images or face models.

3.8.3 Fill Light Mode Setting

You can select fill light modes according to your needs. There are three modes:

- Auto: When the photo sensor detects that the ambient environment is bright, the fill light is

- normally off; otherwise, the fill light will be on.
- NO: The fill light is normally on.
- NC: The fill light is normally closed.

3.8.4 Fill Light Brightness Setting

You can select fill light brightness according to your needs.

3.8.5 Volume Adjustment

You can adjust the beeping and voice volume.

Step 1 Select **System > Volume**.

Step 2 Select **Beep Volume** or **Mic Volume** as needed.

Step 3 Tap  or  to adjust the volume.

3.8.6 IR Light Brightness Adjustment

The larger the value is, the clearer the images will be; otherwise the more unclear the images will be.

3.8.7 FP Parameter

Set the fingerprint accuracy level. The higher the level is, the lower the false recognition rate will be.

3.8.8 Restore to Factory Settings



- Data will be lost if you restore the access controller to the factory settings.
- After the access controller is restored to the factory settings, IP address will not be changed.
- You can select to restore the access controller to the factory settings with all user information and device information deleted or retained.

3.8.9 Restart

Select **Setting > Reboot**, tap **Reboot**, and the access controller will restart.

3.9 USB



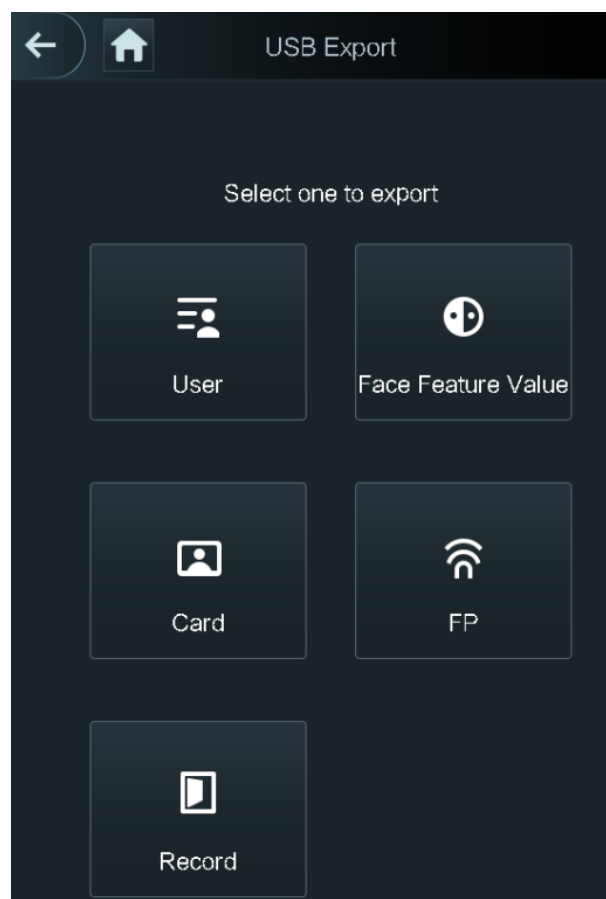
- Make sure that the USB is inserted before exporting user information and updating. During exporting or updating, do not pull out the USB or do other operations; otherwise the exporting or updating will fail.
- You need to import information from one access controller to the USB before using USB to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

3.9.1 USB Export

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

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

Figure 3-15 USB export



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

Step 3 Tap **OK**.

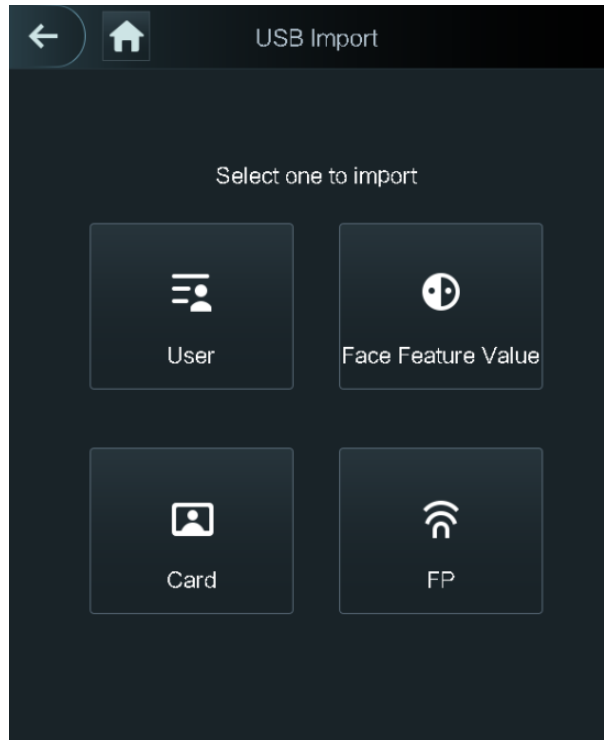
Data exported will be saved in the USB.

3.9.2 USB Import

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

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

Figure 3-16 USB Import



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

Step 3 Tap **OK**.

Data in the USB flash drive will be imported into the access controller.

3.9.3 USB Update

USB flash drive can be used to update the system.

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

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

Step 3 Tap **OK**.

The update starts, and the access controller reboots after the update is finished.

3.9.4 Features

Set privacy, card number reverse, security module, door sensor type, and result feedback.

Figure 3-17 Features

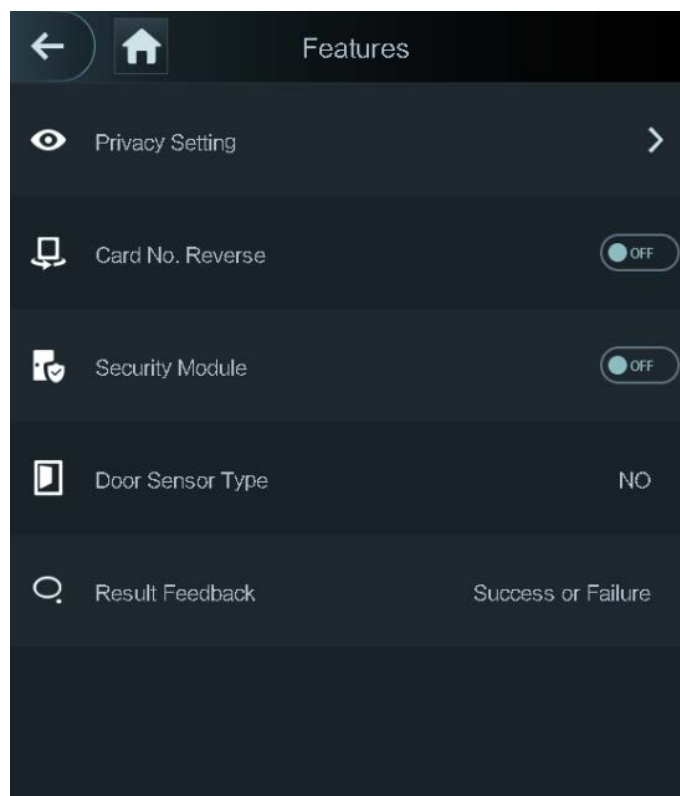


Table 3-9 Feature description

Parameter	Description
Privacy Setting	See "3.9.5 Privacy Setting" for details.
Card No. Reverse	If the third party card reader needs to be connected to the access controller through the wiegand output port, you need to enable the Card No. Reverse function; otherwise the communication between the access controller and the third party card reader might fail due to protocol discrepancy.
Security Module	<ul style="list-style-type: none"> • If the security module is enabled, you need to purchase access control security module separately. The security module needs separate power supply to provide power. • Once the security module is enabled, the exit button, lock control and firefighting linkage will be invalid.
Door Sensor Type	There are two options: NO and NC .
Result Feedback	Displays whether the unlock succeeded or failed.

3.9.5 Privacy Setting

Figure 3-18 Privacy setting

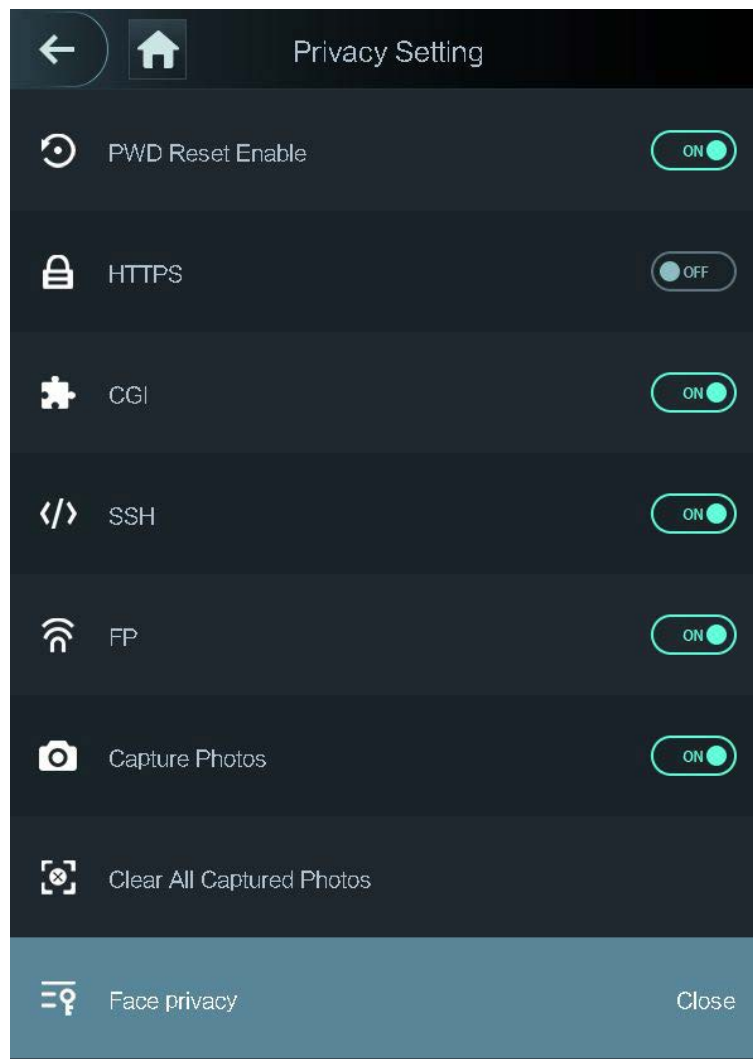



Table 3-10 Features

Parameter	Description
PWD Reset Enable	If the PWD Reset Enable function is enabled, you can reset the password. The PWD Reset function is enabled by default.
HTTPS	Hypertext Transfer Protocol Secure (HTTPS) is a protocol for secure communication over a computer network. When HTTPS is enabled, HTTPS will be used to access CGI commands; otherwise HTTP will be used.  When HTTPS is enabled, the access controller will restart automatically.
CGI	Common Gateway Interface (CGI) offers a standard protocol for web servers to execute programs that execute like console applications running on a server that generates web pages dynamically. When CGI is enabled, CGI commands can be used. The CGI is enabled by default.

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.
FP	If you select OFF for Fingerprint (FP), users' fingerprint information will not be displayed when they get fingerprints recorded or when they use fingerprints to unlock the door.
Capture Photo	If you select ON, when a user unlocks the door, the user's photo will be automatically taken. This function is ON by default.
Clear All Captured Photos	Tap the icon, and you can delete all captured photos.
Face Privacy	Set different levels to blur the standby interface.

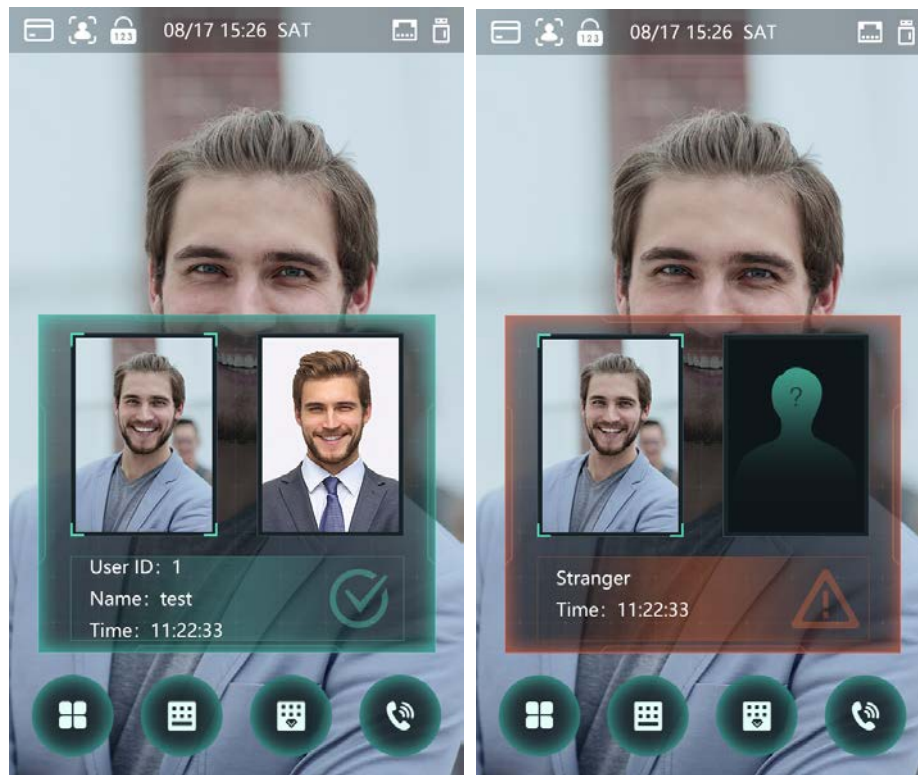
3.9.6 Result Feedback

You can select a result feedback mode as needed.

Select **Features > Result Feedback**.

Photo & Name

Figure 3-19 Photo & name



User Photo & Name

Figure 3-20 User photo & name



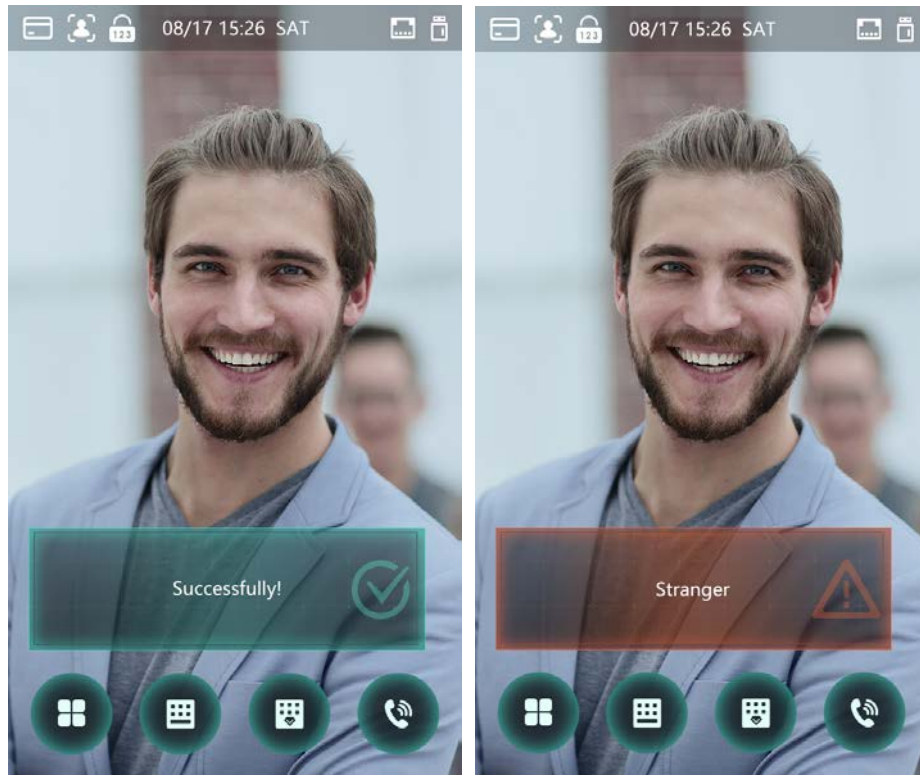
Only Name

Figure 3-21 Only name



Success or Failure

Figure 3-22 Success or failure



3.10 Record

You can search for all unlocking records.

Select **Record** > **Search Punch Records**.

Figure 3-23 Search punch records

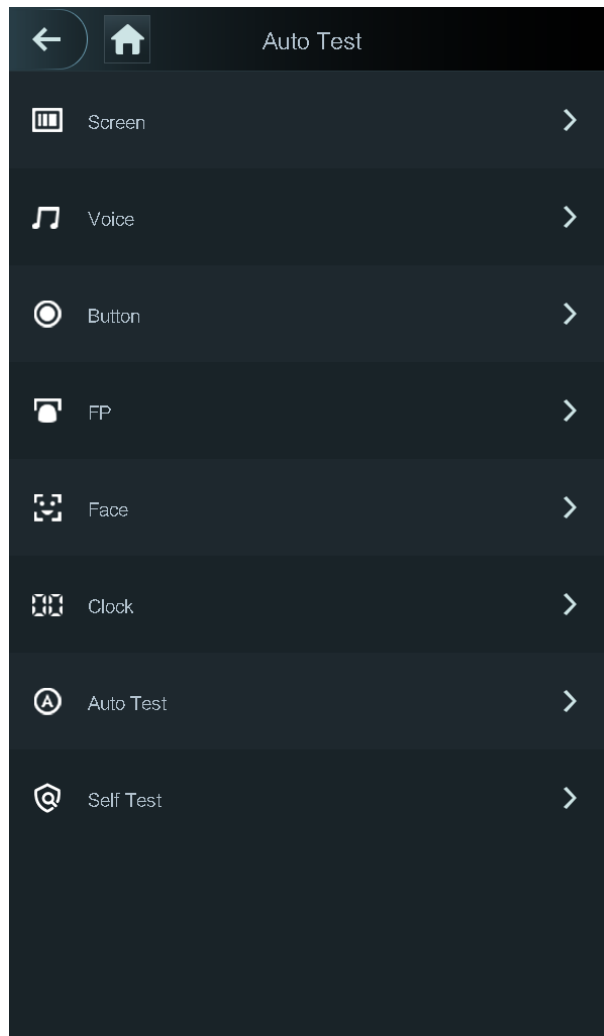


User ID.	Name	Time	Status	Verify Mode
		09-05 17:21	Failed	Face
1	zxl	09-05 17:19	OK	Face
1	zxl	09-05 17:19	OK	Face
1	zxl	09-05 17:19	OK	Face
1	zxl	09-05 17:19	OK	Face
		09-05 17:18	Failed	Face
		09-05 17:18	Failed	Face
		09-05 17:18	Failed	Face
		09-05 17:18	Failed	Face
		09-05 17:18	Failed	Face
		09-05 17:18	Failed	Face
		09-05 17:18	Failed	Face

3.11 Auto Test

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

Figure 3-24 Auto test



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

3.12 System Info

You can view data capacity, device version, and hardware version of the access controller on the **System Info** interface.

4 Web Operation

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

4.1 Initialization

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

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



- IE 8 and later are supported. Otherwise you might not log in to the web.
- Make sure that the computer used to log in to the web is in the same LAN with the device.
- 7-inch model B access controllers of have dual NICs. The default management address for ETH1 is 192.168.1.108, and for ETH2 is 192.168.2.108.

Figure 4-1 Initialization

Boot Wizard

① Device Initialization ② Auto Check

Username admin

New Password

Low Medium High

Confirm Password

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

☐ Bind Email

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

Next

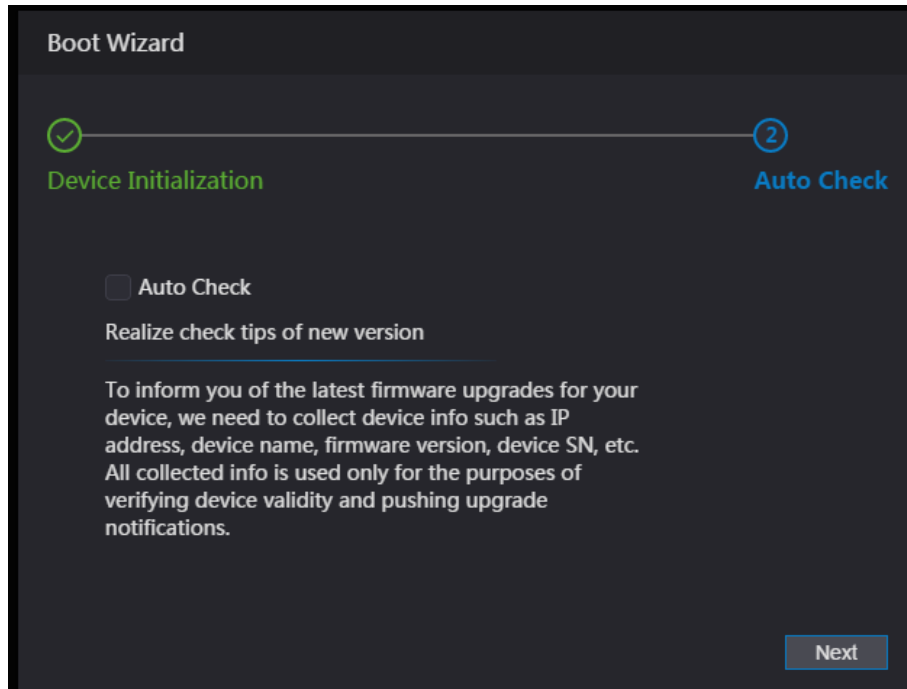
Step 2 Enter the new password, confirm password, enter an email address, and then tap **Next**.



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

Step 3 Click **Next**.

Figure 4-2 Auto check



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

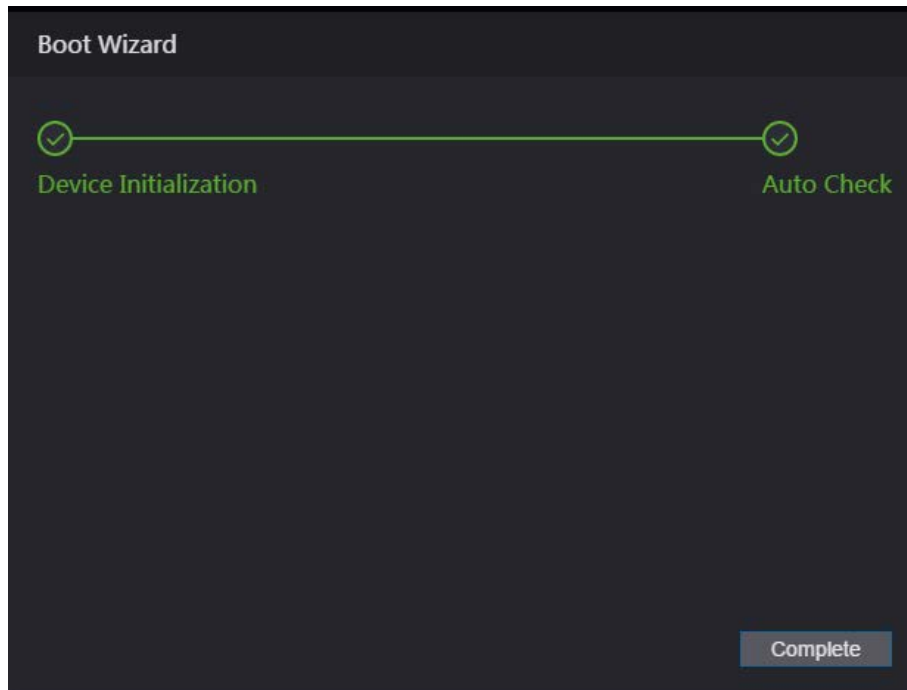


It is recommended that **Auto Check** be selected to get the latest program in time.

Step 5 Click **Next**.

The configuration is finished.

Figure 4-3 Finished configuration



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

4.2 Login

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



- IE 8 and later are supported. Otherwise you might not log in to the web.
- Make sure that the computer used to log in to the web is in the same LAN with the device.
- 7-inch model B access controllers of have dual NICs. The default management address for ETH1 is 192.168.1.108, and for ETH2 is 192.168.2.108.

Figure 4-4 Log in

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 controller. 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 Resetting the Password."

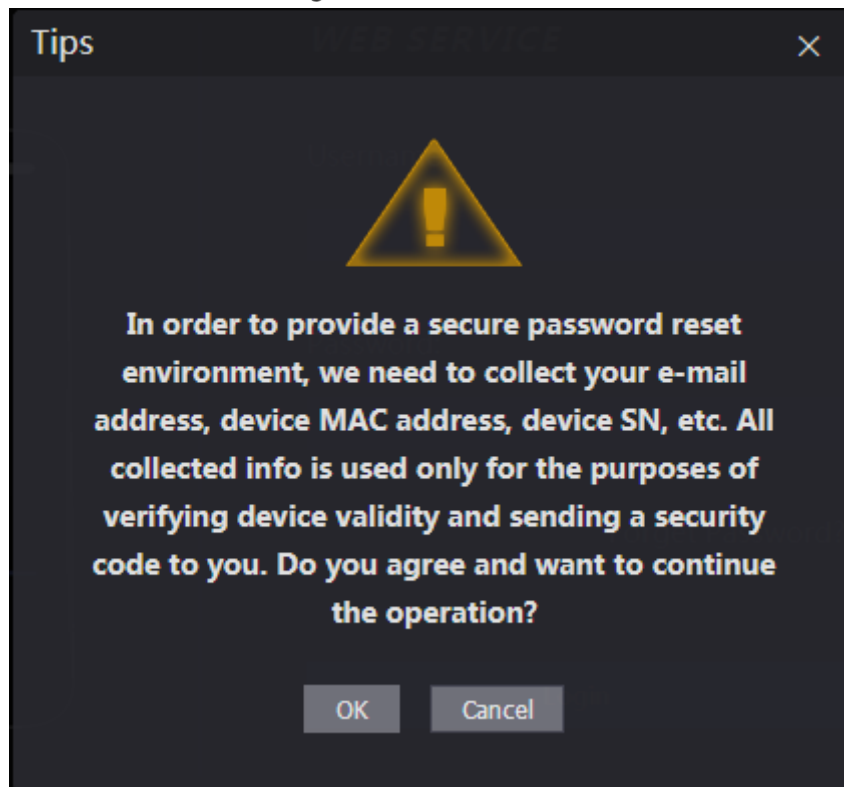
Step 3 Click **Login**.

4.3 Resetting the Password

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

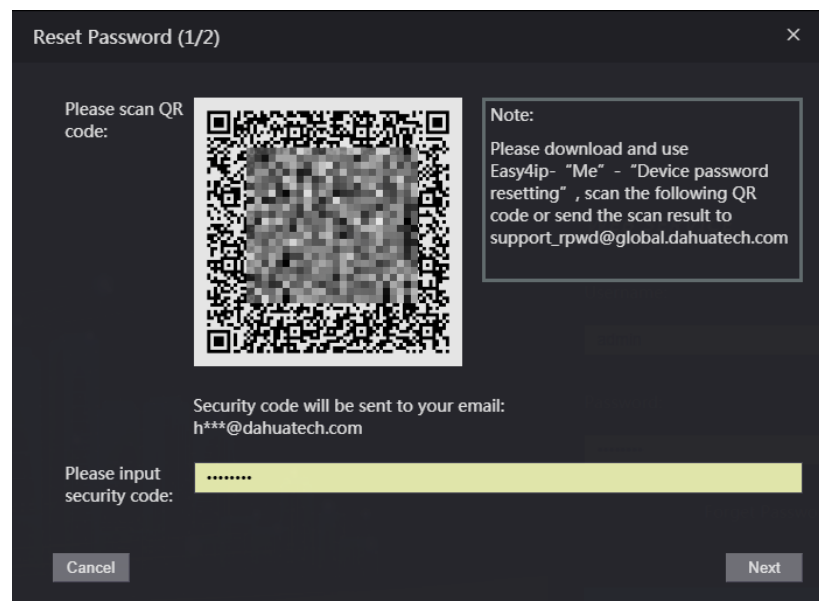
Step 1 On the login interface, click **Forgot password?**.

Figure 4-5 Tips



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

Figure 4-6 Reset Password



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



- At most two security codes will be generated by scanning the same QR code. If security codes become invalid, to get more security codes, refresh the QR code.
- You need to send the content you get after you scanned the QR code to the designated email address, and then you will get the security code.
- Please use the security code within 24 hours after you receive it. Otherwise, it will become invalid.
- If wrong security codes are entered for consecutive five times, the administrator will be

frozen for five minutes.

Step 4 Enter the security code you have received.

Step 5 Click **Next**.

Step 6 Reset and confirm the new password.



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

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

4.4 Alarm Linkage

4.4.1 Setting Alarm Linkage

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

Step 1 Select **Alarm Linkage**.

Figure 4-7 Alarm linkage

Alarm Input	Name	Alarm Input Type	Alarm Output Channel	Modify
1	Zone1	NO	1	
2	Zone2	NO	1	



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

Figure 4-8 Modify alarm linkage parameter

Table 4-1 Alarm linkage parameter description

Parameter	Description
Alarm Input	You cannot edit the value. Keep it default.
Name	Enter a zone name.
Alarm Input Type	There are two options: NO and NC. If alarm input type of the alarm device you purchased is NO, then you should select NO; otherwise you should select NC.
Fire Link Enable	If fire link is enabled the access controller will output alarms when fire alarms are triggered. The alarm details will be displayed in the alarm log.  Alarm output and access link are NO by default if fire link is enabled.
Alarm Output Enable	The relay can output alarm information (will be sent to the management platform) if the Alarm Output is enabled.
Duration (Sec.)	The alarm duration, and the range is 1–300 seconds.
Alarm Output Channel	You can select an alarm output channel according to the alarming device that you have installed. Each alarm device can be regarded as a channel.
Access Link Enable	After the Access Link is enabled, the access controller will be normally on or normally closed when there are input alarm signals.
Channel Type	There are two options: NO and NC.

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



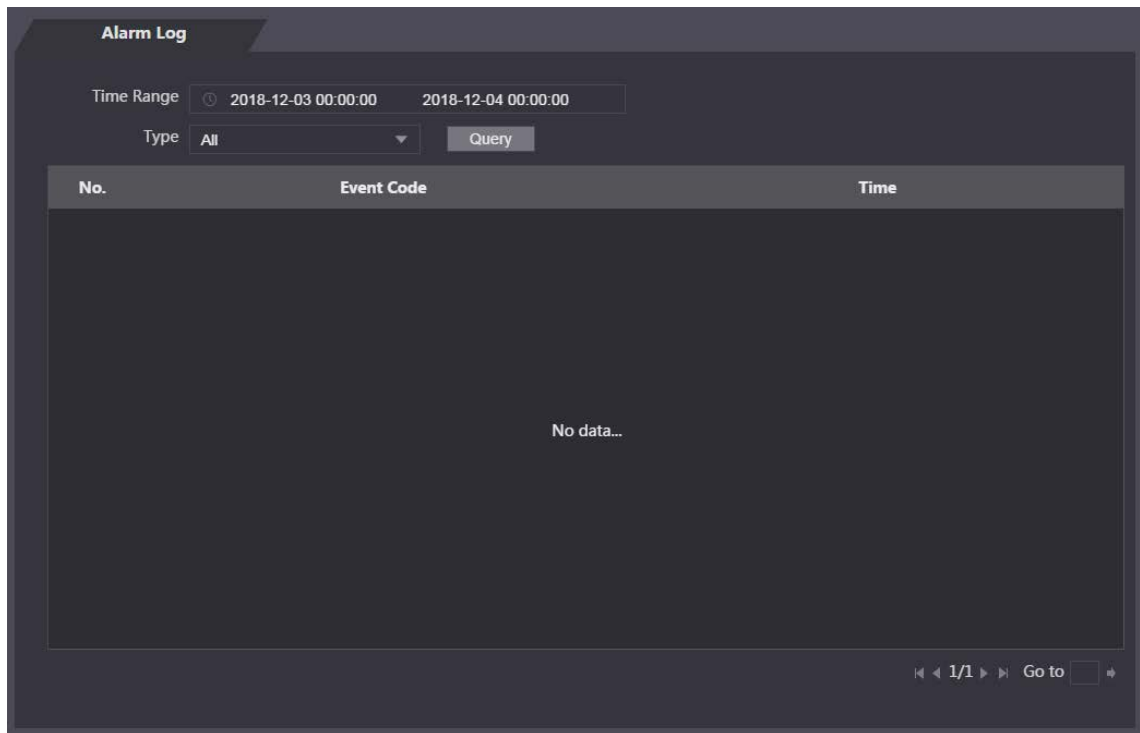
The configuration on the web will be synchronized with the configuration in the client if the access controller is added to a client.

4.4.2 Alarm Log

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

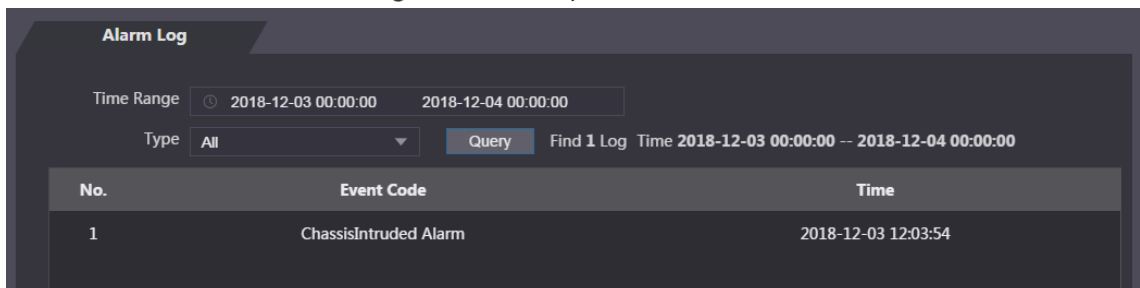
Step 1 Select **Alarm Linkage > Alarm Log**.

Figure 4-9 Alarm log



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

Figure 4-10 Query results



4.5 Call Configuration

The access controller can work as a door station and call other devices.

4.5.1 Configuring the Access Controller

Set the device type and number.

4.5.1.1 Access Controller as SIP Server

Step 1 Log in to the web.

Step 2 Select **Talkback Setting > Local**.

Step 3 Configure the parameters.

Figure 4-11 Local (1)

The screenshot shows a configuration interface titled 'Local'. It contains the following elements:

- Device Type:** A dropdown menu set to 'Unit Door Station'.
- Centre Call No.:** A text input field containing '888888'.
- VTO No.:** A text input field containing '8001'.
- Group Call:** A toggle switch that is currently disabled. A red warning message states: 'Warning: The device will be rebooted after modifying group call enable status.'
- Transmission Mode:** Two radio buttons, 'Mode1' (which is selected) and 'Mode2'.
- Buttons:** 'Confirm', 'Refresh', and 'Default' buttons at the bottom.

Table 4-2 Parameter description

Parameter	Description
Device Type	The access controller can only work as a unit door station.
Centre Call No.	Enter a number to be identified by the management center. It should be "888888" plus three numbers.
VTO No.	Cannot be configured.
Group Call	When enabled, a call from the access controller to a main indoor station will also be sent to all its extension indoor stations.
Transmission Mode	<ul style="list-style-type: none">● Mode1: Real-time call but the video and sound may be lagging with poor network.● Mode2: Not real-time call but ensures smooth video and sound.

Step 4 Click **Confirm**.

4.5.1.2 Other Device as SIP Server

Step 1 Log in to the web.

Step 2 Select **Talkback Setting > Local**.

Step 3 Configure the parameters.

Figure 4-12 Local (2)

This screenshot is identical to Figure 4-11, showing the 'Local' configuration page. The 'VTO No.' field now contains '8001'.

Table 4-3 Parameter description

Parameter	Description
Device Type	The access controller can work as a unit door station or fence station.
Centre Call No.	Enter a number to be identified by the management center. It should be "888888" plus three numbers.
VTO No.	<p>Enter a number for the access controller.</p> <p></p> <ul style="list-style-type: none">● It should be four digits. The first two should be 80 and the last two starts with 01, such as 8001.● If there are multiple door stations, VTO numbers cannot be the same.

Parameter	Description
Transmission Mode	<ul style="list-style-type: none"> Mode1: Real-time call but the video and sound may be lagging with poor network. Mode2: Not real-time call but ensures smooth video and sound.

4.5.2 SIP Server

On the web, you can add door stations and indoor stations to the SIP server so that they can talk to each other. The SIP server can be the access controller or other door stations.



When the access controller works as the SIP server, it can connect up to 50 other access controllers and indoor monitors combined.

4.5.2.1 Access Controller as SIP Server

Step 1 Log in to the web.

Step 2 Select **Talkback Setting > SIP Server**.

Step 3 Enable **SIP Server** and keep other parameters as default.

Figure 4-13 SIP server (1)

Step 4 Click **OK** and the access controller will restart.

4.5.2.2 Other Device as SIP Server

- Step 1** Log in to the web.
- Step 2** Select **Talkback Setting > SIP Server**.
- Step 3** Do not enable **SIP Server** and select **Server Type** as VTO.
- Step 4** Configure the parameters.

Figure 4-14 SIP server (2)

SIP Server

SIP Server ☐ Enable

Server Type **VTO**

IP Address **192.168.1.111**

Port **5060**

Username **8001**

Password

SIP Domain **VDP**

SIP Server Username

SIP Server Password

Warning: The device needs reboot after modifying the SIP server enable.

OK **Refresh** **Default**

Table 4-4 SIP server parameter description (1)

Parameter	Description
IP Address	The IP address of the door station working as the SIP server.
Port	5060 by default.
Username	Keep the default values.
Password	
SIP Domain	Must be VDP.
SIP Server Username	SIP server login username and password.
SIP Server Password	

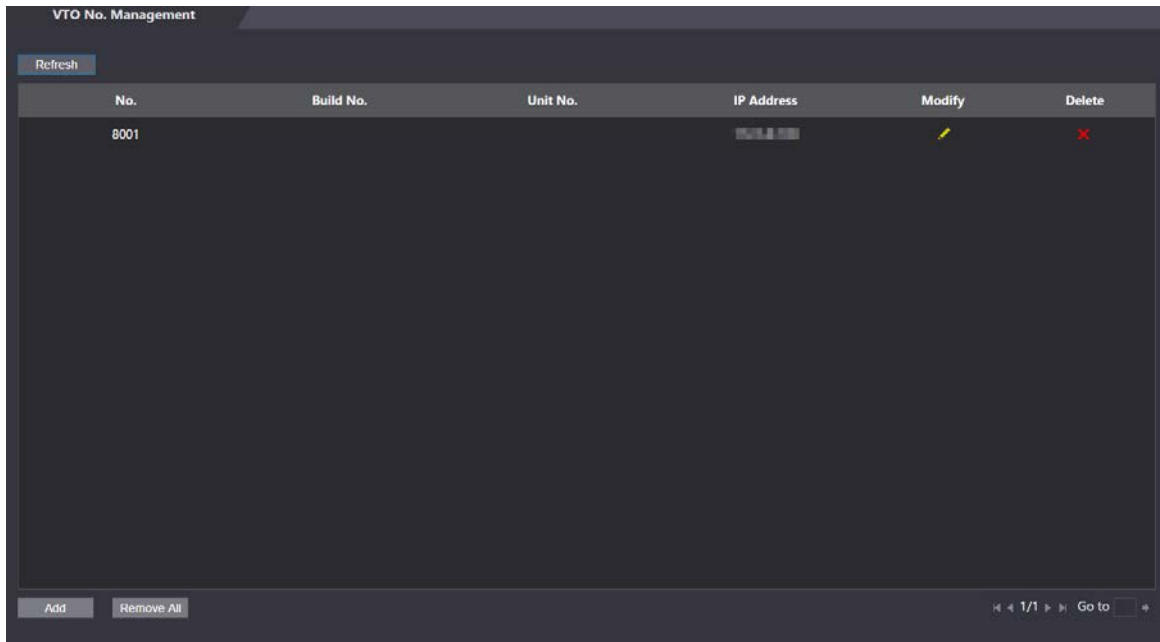
- Step 5** Click **OK**.

4.5.3 Door Station Management

When the access controller works as the SIP server, add other door stations to call them.

- Step 1** Log in to the web.
- Step 2** Select **Talkback Setting > VTO No. Management**.
- Step 3** Click **Add**.

Figure 4-15 VTO No. management



- Step 4** Configure the parameters.

Figure 4-16 Add a door station

The screenshot shows a dialog box titled "Add" with a close button (X) in the top right corner. It contains several input fields: "Rec No." with the value "8002", "Register Password" with a masked value "*****", "Build No." (empty), "Unit No." (empty), "IP Address" with a masked value "192.168.1.1", "Username" with the value "admin", and "Password" with a masked value "*****". At the bottom right are "OK" and "Cancel" buttons.

Table 4-5 Parameter description

Parameter	Description
Rec No.	Number of the door station.
Register Password	Keep the default value.

Parameter	Description
Build No.	Cannot be configured.
Unit No.	Cannot be configured.
IP Address	IP address of the door station.
Username	Web login username and password for the door station.
Password	

Step 5 Click **OK**.

4.5.4 Indoor Monitor Management

When the access controller works as the SIP server, add all relevant indoor monitors to call them.



When there are main and extension indoor monitors, you need to enable group call function first before adding them.

4.5.4.1 Add One Indoor Monitor

Step 1 Log in to the web.

Step 2 Select **Talkback Setting > Room No. Management**.

Step 3 Click **Add**.


Figure 4-17 Room No. Management

The screenshot displays the 'Room No. Management' web interface. At the top, there is a 'Refresh' button. Below it is a table with the following columns: Room No., First Name, Last Name, Nick Name, Register Type, and Modify. The table contains one row with the value '9901' in the Room No. column and 'public' in the Register Type column. Below the table, there are four buttons: Add, Remove All, Export, and Import. At the bottom of the interface, there are four input fields: Unit Layer Amount (with the value 5), First Floor Number (with the value 101), Room Amount in One Layer (with the value 4), and Second Floor Number (with the value 201). An Add button is located below these input fields.

Step 4 Enter the information.

Figure 4-18 Add one indoor monitor

Table 4-6 Parameter description

Parameter	Description
First Name	To differentiate each indoor monitor.
Last Name	
Nick Name	
Room No.	Room number of the indoor monitor.  <ul style="list-style-type: none"> It can contain up to five digits and must be the same as the one configured on the indoor monitor. When there are main and extension indoor monitors, the room number of main indoor monitor should end with "-0", and that of extension indoor monitors with "-1", "-2", "-3"...For example, the main indoor monitor is 101-0, extension monitors are 101-1, 101-2 and 101-3.
Register Type	Keep the default value.
Register Password	

Step 5 Click **OK**.



You can also click **Export** to export the room number and import to other devices.

4.5.4.2 Add Indoor Monitors in Batches

You can add up to 1024 indoor monitors.

Step 1 Log in to the web.

Step 2 Select **Talkback Setting > Room No. Management**.

Step 3 At the bottom, enter numbers for **Unit Layer Amount**, **Room Amount in One Layer**, **First Floor Number** and **Second Floor Number**.



- Unit layer amount can be 1–99, room amount in one layer 1–99, and floor number 1–99999.

Step 4 Click **Add**.

Figure 4-19 Add indoor monitors in batches

The screenshot shows a web interface titled "Room No. Management". At the top, there is a "Refresh" button. Below it is a table with the following columns: "Room No.", "First Name", "Last Name", "Nick Name", "Register Type", and "Modify". The table contains one row with "Room No." 9901 and "Register Type" public. Below the table are buttons for "Add", "Remove All", "Export", and "Import". At the bottom, there are input fields for "Unit Layer Amount" (5), "First Floor Number" (101), "Room Amount in One Layer" (4), and "Second Floor Number" (201). The "Add" button is highlighted with an orange box.

4.5.5 Configuring the Managing Device

When the access controller works as the SIP server, add other managing devices to call them.

Step 1 Log in to the web.

Step 2 Select **Talkback Setting > VTS Management**.

Step 3 Click **Add**.

Figure 4-20 Add managing devices

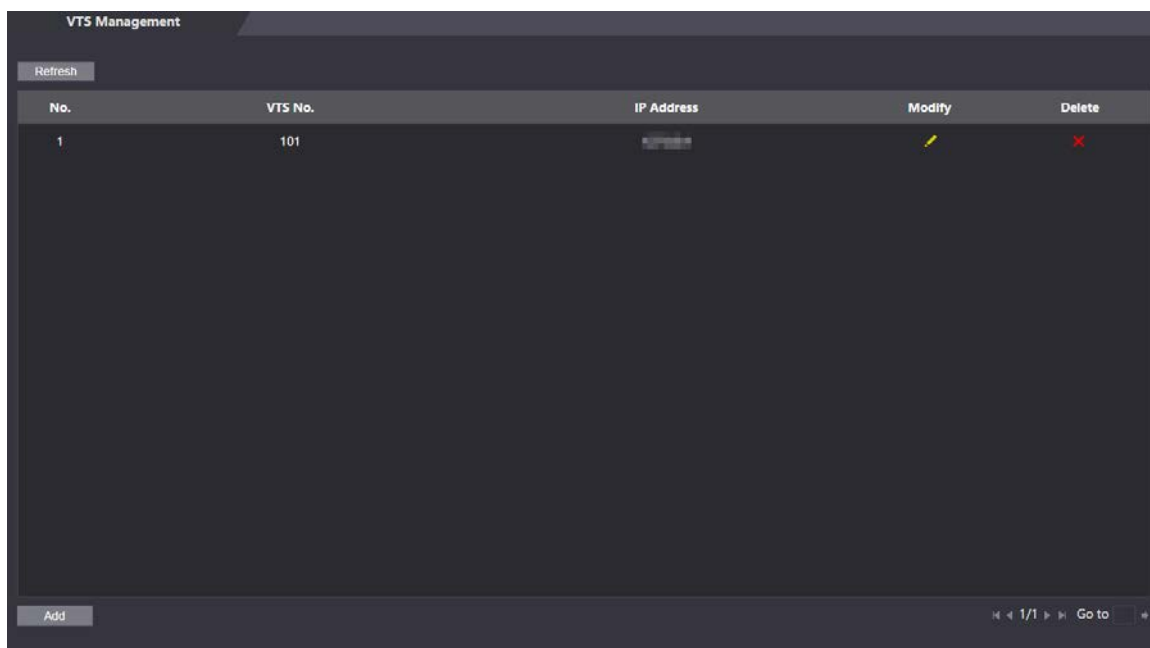
The screenshot shows a dialog box titled "Add" with a close button (X) in the top right corner. It contains three input fields: "VTS No." (a text box), "Register Password" (a password box with masked characters), and "IP Address" (a box with four segments for IP address entry). At the bottom right are "OK" and "Cancel" buttons.

Step 4 Enter the information.

- VTS No. can contain up to 9 digits.
- Login password for the managing device. Keep the default value.

Step 5 Click **OK**.

Figure 4-21 Added a managing device



The screenshot shows the 'VTS Management' interface. At the top, there is a 'Refresh' button. Below it is a table with the following columns: 'No.', 'VTS No.', 'IP Address', 'Modify', and 'Delete'. The table contains one row with the following data: '1' in the 'No.' column, '101' in the 'VTS No.' column, and an IP address in the 'IP Address' column. The 'Modify' column contains a yellow pencil icon, and the 'Delete' column contains a red 'X' icon. At the bottom left, there is an 'Add' button. At the bottom right, there is a pagination control showing '1/1' and a 'Go to' button.

No.	VTS No.	IP Address	Modify	Delete
1	101			

- Modify a managing device.
You need to update the information when the register password or IP address of the managing device changes. Click and enter the new password or IP address, and then click **OK**.
- Delete a managing device.
Click .

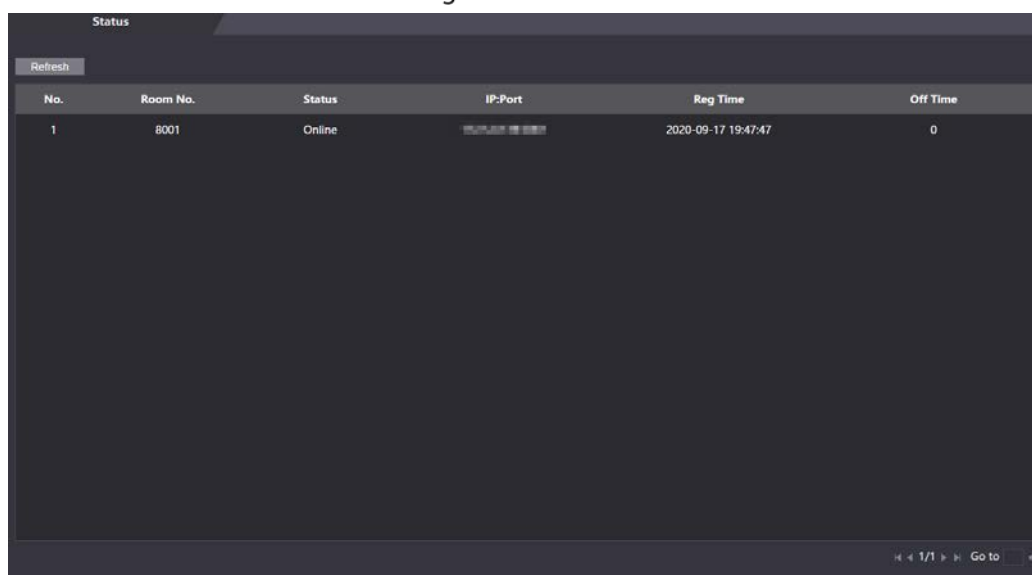
4.5.6 Online Status

When the access controller works as the SIP server, administrators can log in to the web and check the information of online devices.

Step 1 Log in to the web.

Step 2 Select **Talkback Setting > Status**.

Figure 4-22 Status



The screenshot shows the 'Status' interface. At the top, there is a 'Refresh' button. Below it is a table with the following columns: 'No.', 'Room No.', 'Status', 'IP-Port', 'Reg Time', and 'Off Time'. The table contains one row with the following data: '1' in the 'No.' column, '8001' in the 'Room No.' column, 'Online' in the 'Status' column, an IP-Port in the 'IP-Port' column, '2020-09-17 19:47:47' in the 'Reg Time' column, and '0' in the 'Off Time' column. At the bottom right, there is a pagination control showing '1/1' and a 'Go to' button.

No.	Room No.	Status	IP-Port	Reg Time	Off Time
1	8001	Online		2020-09-17 19:47:47	0

4.5.7 Call Logs

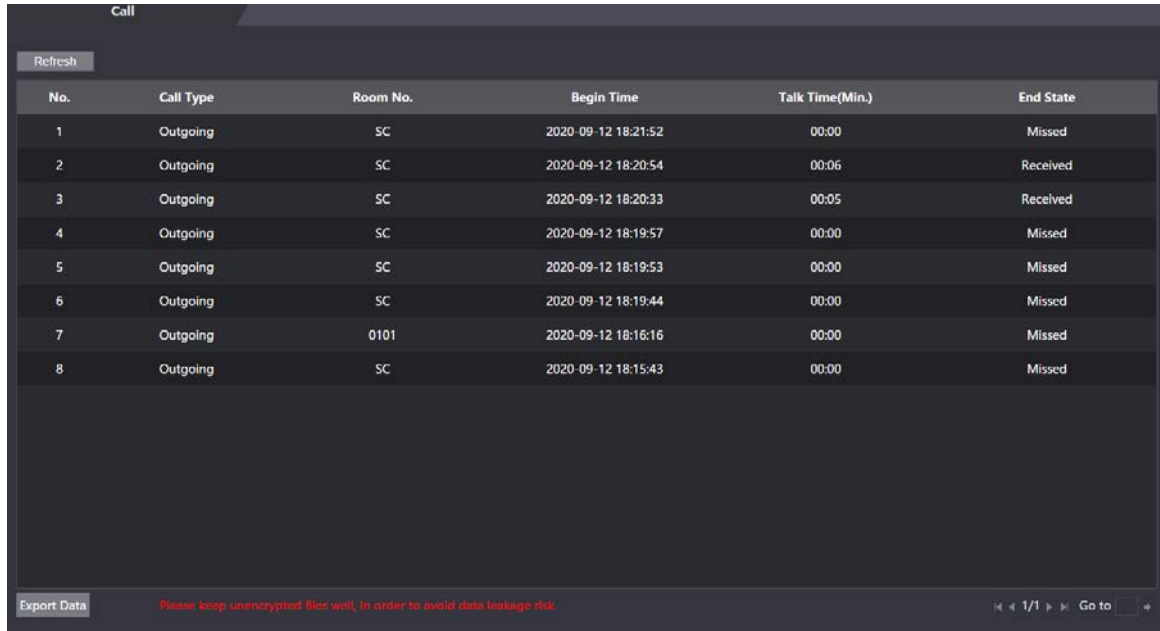
You can check up to 1024 call logs.

Step 1 Log in to the web.

Step 2 Select **Talkback Setting > Call**.

Step 3 (Optional) Click **Export Data** to export all the logs.

Figure 4-23 Call logs

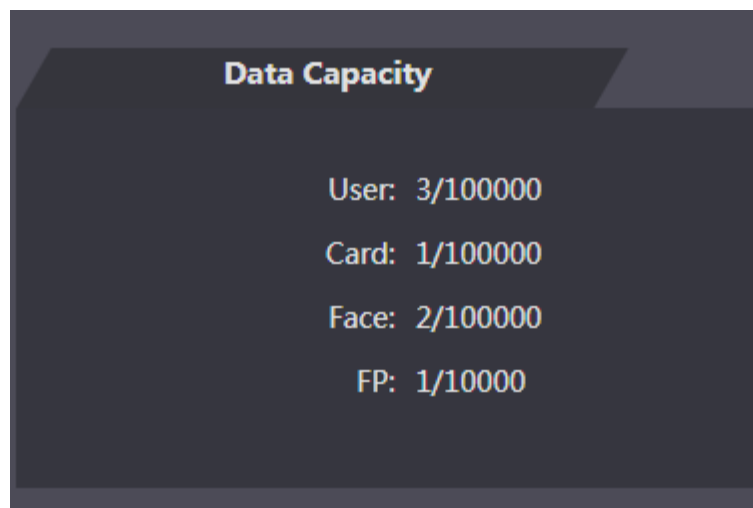


No.	Call Type	Room No.	Begin Time	Talk Time(Min.)	End State
1	Outgoing	SC	2020-09-12 18:21:52	00:00	Missed
2	Outgoing	SC	2020-09-12 18:20:54	00:06	Received
3	Outgoing	SC	2020-09-12 18:20:33	00:05	Received
4	Outgoing	SC	2020-09-12 18:19:57	00:00	Missed
5	Outgoing	SC	2020-09-12 18:19:53	00:00	Missed
6	Outgoing	SC	2020-09-12 18:19:44	00:00	Missed
7	Outgoing	0101	2020-09-12 18:16:16	00:00	Missed
8	Outgoing	SC	2020-09-12 18:15:43	00:00	Missed

4.6 Data Capacity

You can see how many users, cards, face images, and fingerprints the access controller can hold on the **Data Capacity** interface.

Figure 4-24 Data capacity



Data Capacity	
User:	3/100000
Card:	1/100000
Face:	2/100000
FP:	1/10000

4.7 Video Setting

You can set parameters including data rate, image parameters (brightness, contrast, hue, saturation, and more), and exposure on the **Video Setting** interface.

4.7.1 Data Rate

Figure 4-25 Data rate

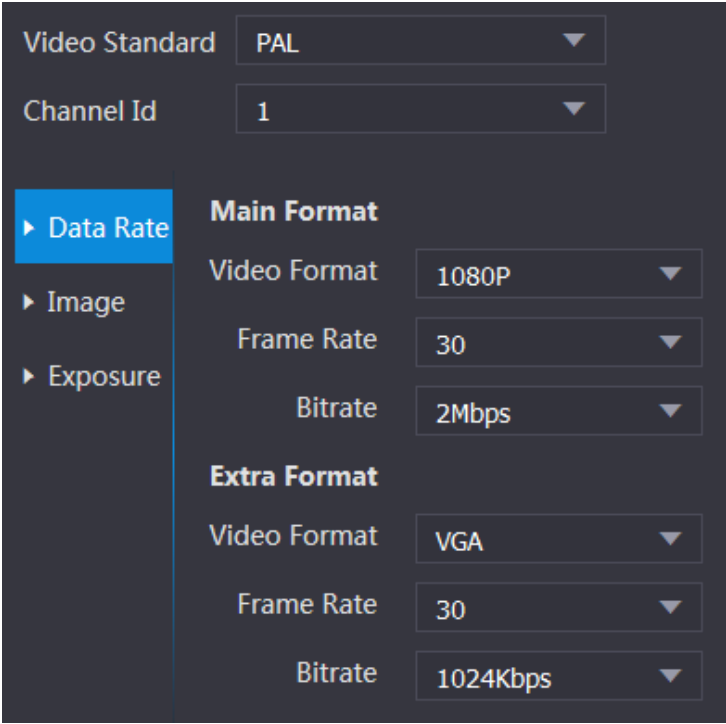



Table 4-7 Data rate parameter description

Parameter		Description
Video Standard		There are two options: NTSC and PAL. Select a standard according to the video standard of your region.
Channel		There are two options: 1 and 2. 1 is white light camera and 2 is IR light camera.
Main Format	Video Format	There are four options: D1, VGA, 720p and 1080p. Select an option according to the video quality you want.  720p is set by default. If you need the call function, do not set it to 1080p.
	Frame Rate	The rate at which consecutive frames appear on a display. The frame rate range is 1–30 fps.
	Bit Rate	The number of bits that are conveyed or processed per unit of time. There are five options: 2 Mbps, 4 Mbps, 6 Mbps, 8 Mbps, and 10 Mbps.
Extra Format	Video Format	There are three options: D1, VGA, and QVGA.
	Frame Rate	The rate at which consecutive frames appear on a display. The frame rate range is 1–30 fps.

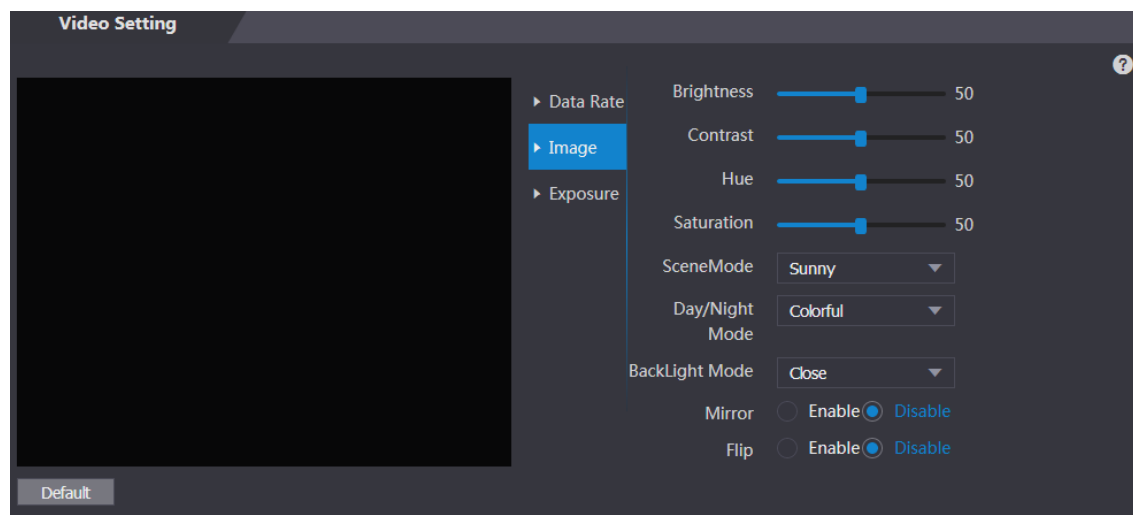
Parameter		Description
	Bit Rate	The number of bits that are conveyed or processed per unit of time. There are options: 512 Kbps, 640 Kbps, 768 Kbps, 896 Kbps, 1024 Kbps, 1.25 Mbps, 1.5 Mbps, 1.75 Mbps, and 2 Mbps.

4.7.2 Image

There are two channels, and you need to configure parameters for each channel.

Step 1 Select **Video Setting > Video Setting > Image**.


Figure 4-26 Image



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

Table 4-8 Image parameter description


Parameter	Description
Brightness	The larger the value is, the brighter the images will be.
Contrast	Contrast is the difference in luminance or color that makes an object distinguishable. The larger the contrast value is, the greater the brightness and color contrast will be.
Hue	The larger the value is, the deeper the color will be.
Saturation	The larger the value is, the brighter the colors will be. The value does not change image brightness.
Scene Mode	<ul style="list-style-type: none"> ● Close: Without modes. ● Auto: The system automatically adjusts scene modes. ● Sunny: In this mode, image hue will be reduced. ● Night: In this mode, image hue will be increased. Sunny is selected by default.
Day/Night Mode	Day/Night mode decides the working status of the fill light. <ul style="list-style-type: none"> ● Auto: The system automatically adjusts the day/night modes. ● Colorful: In this mode, images are with colors. ● Black and white: In this mode. Images are in black and white.

Parameter	Description
Back Light Mode	<ul style="list-style-type: none"> ● Close: Without back light. ● BLC: Backlight compensation corrects regions with extremely high or low levels of light to maintain a normal and usable level of light for the object in focus. ● WDR: In the wide dynamic range mode, the system dims bright areas and compensates dark areas to ensure the definition of objects in the bright areas and dark areas.  <p>When human faces are in the backlight, you need to enable the Wide Dynamic.</p> <ul style="list-style-type: none"> ● HLC: Highlight compensation is needed to compensate for overexposure of highlights or strong light sources like spotlights, headlights, porch lights, etc. to create an image that is usable and not overtaken by a bright light.
Mirror	When the function is enabled, images will be displayed with left and right side reversed.
Flip	When this function is enabled, videos can be flipped over.

4.7.3 Exposure

Table 4-9 Exposure parameter description

Parameter	Description
Anti-flicker	<ul style="list-style-type: none"> ● 50Hz: When the utility frequency of alternating current is 50Hz, the exposure is automatically adjusted to make sure that there are no stripes on images. ● 60Hz: When the utility frequency of alternating current is 60Hz, the exposure is automatically adjusted to make sure that there are no stripes on images. ● Outdoor: When Outdoor is selected, the exposure mode can be switched.

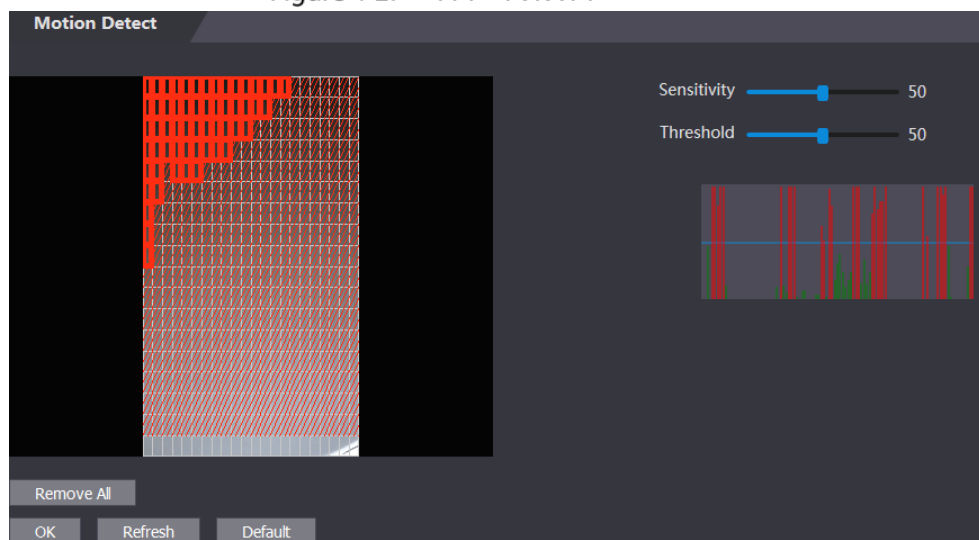
Parameter	Description
Exposure Mode	 <ul style="list-style-type: none"> When you select Outdoor in the Anti-flicker drop-down list, you can select Shutter Priority as the exposure mode. Exposure modes of different devices might vary, and the actual product shall prevail. <p>You can select from:</p> <ul style="list-style-type: none"> Auto: The access controller will automatically adjust brightness of images. Shutter Priority: The access controller will adjust image brightness according to shutter exposure value range. If the image brightness is not enough and the shutter value has reached upper or lower limit, the access controller will adjust gain value automatically to get ideal brightness. Manual: You can configure gain and shutter value manually to adjust image brightness.
Shutter	The larger the shutter value is and the shorter the exposure time is, the darker the images will be.
Shutter Value Range	If you select Customized Range , you can customize the shutter value range.
Gain Value Range	When the gain value range is set, video quality will be improved.
Exposure Compensation	You can increase video brightness by adjusting exposure compensation value.
3D NR	When 3D Noise Reduction (RD) is enabled, video noise can be reduced, and high definition videos will be produced.
Grade	<p>You can adjust the value of the 3D NR when 3D NR is enabled.</p> <p>The larger the value is, the less the noise there will be.</p>

4.7.4 Motion Detection

Set a range in which moving objects can be detected.

Step 1 Select **Video Setting > Video Setting > Motion Detection**.

Figure 4-27 Motion detection

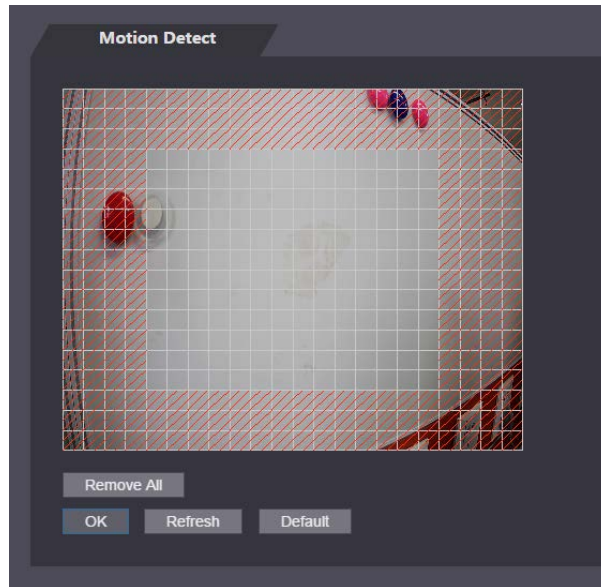


Step 2 Press and hold the left mouse button, and then drag the mouse in the red area. The motion detection area is displayed.



- 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 4-28 Motion detection area



Step 3 Set sensitivity and threshold.



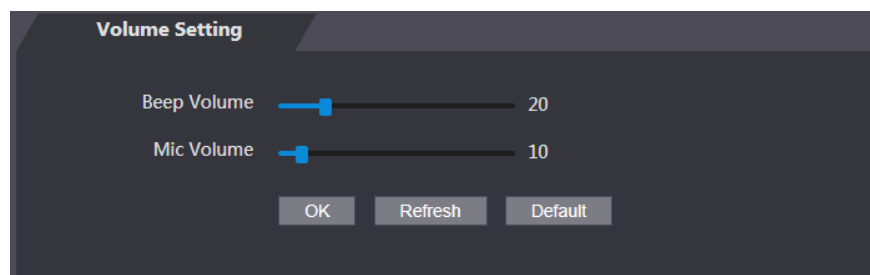
- Sensitivity represents the ability of each grid to sense motion. The larger the value is, the higher the sensitivity is.
- Threshold is the condition of motion detection. When grid number reaches the threshold, motion detection will be triggered. The smaller the value is, the more likely the motion detection will be triggered.
- When grid number is smaller than the threshold, green line will appear; when grid number is more than the threshold, red line will appear.

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

4.7.5 Volume Setting

You can adjust volume of the access controller speaker.

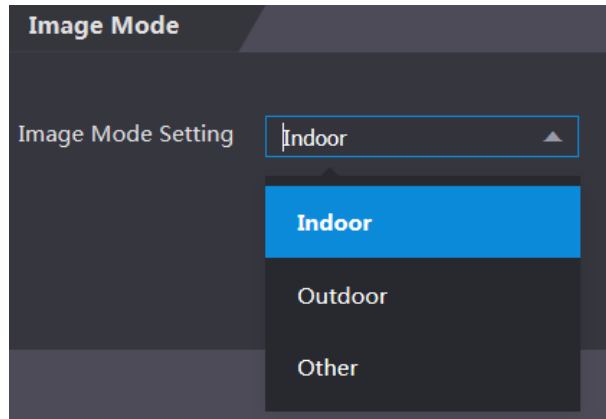
Figure 4-29 Volume setting



4.7.6 Image Mode

There are three options: indoor, outdoor and other. Select **Indoor** when the access controller is installed indoors; select **Outdoor** when the access controller is installed outdoors; and select **Other** when the access controller is installed at places with backlights like corridors and hallways.

Figure 4-30 Image mode



4.7.7 Local Coding

Set up the area to be displayed on the indoor monitors.

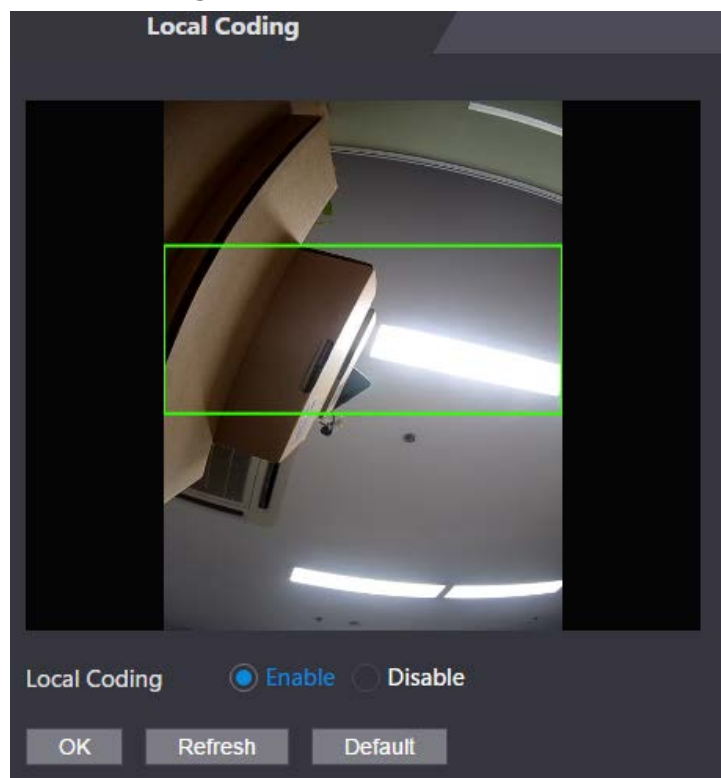
Step 1 Log in to the web.

Step 2 Select **Video Setting > Local Coding**.

Step 3 Enable the function.

Step 4 Drag the box as needed.

Figure 4-31 Local coding



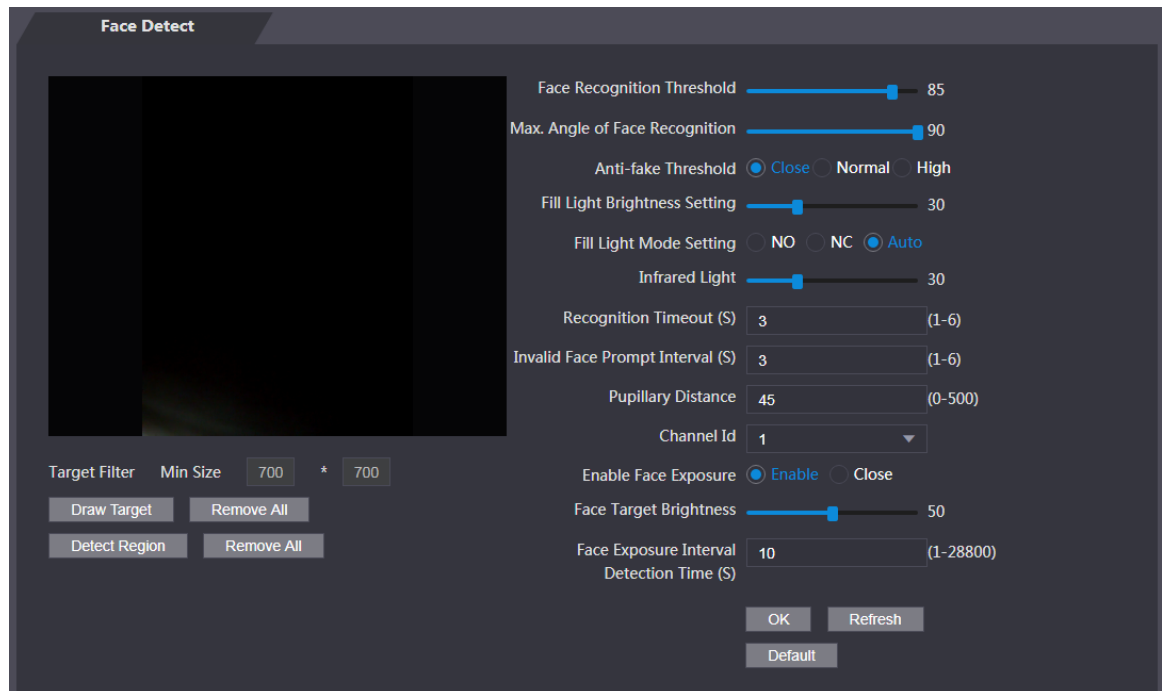
Step 5 Click **OK**.

4.8 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**.

Figure 4-32 Face detect



Step 2 Configure the parameters.

Table 4-10 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	There are two options: Enable and Close .
Fill Light Brightness Setting	You can set fill light brightness.
Fill Light Mode Setting	<p>There are three fill light modes.</p> <ul style="list-style-type: none">● NO: Fill light is normally on.● NC: Fill light is normally closed.● Auto: Fill light will be automatically on when a motion detection event is triggered. <p> When Auto is selected, the fill light will not be on even if Infrared Light value is greater than 19.</p>
Infrared Light	Adjust IR brightnees by dragging the scroll bar.
Recognition Timeout	When a person who does not have the access authority stands in front of

Parameter	Description
	the access controller and gets the face recognized, the controller will prompt that face recognition failed. The prompt interval is called recognition timeout.
Invalid Face Prompt Interval	When a face has no access authority stands in front of the access controller, the controller will prompt that the face is invalid. The prompt interval is invalid face prompt interval.
Pupillary Distance	Pupillary distance is the pixel value of the image between the centers of the pupils in each eye. You need to set an appropriate value so that the access controller can recognize faces as needed. The value changes according to the face sizes and the distance between faces and the lens. The closer the face is to the lens, the greater the value should be. If an adult is 1.5 meters away from the lens, the pupillary distance value can be within 50 to 70.
Enable Face Exposure	After face exposure is enabled, human face will be clearer when the access controller is installed outdoors.
Channel Id	There are two options: 1 and 2. 1 is white light camera and 2 is IR light camera.
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 detection region. Click Remove All , and you can remove all the detection regions.
Face Target Brightness	The default value is 50. Adjust the brightness as needed.
Face Exposure Interval	After a face is detected, the access controller will give out light to illuminate the face, and the access controller will not give out light again until the interval you set has passed.

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

4.9 Network Setting

4.9.1 TCP/IP

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


Make sure that the access controller is connected to the network correctly.

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

Figure 4-33 TCP/IP

Step 2 Configure parameters.

Table 4-11 TCP/IP

Parameter	Description
IP Version	There is one option: IPv4.
Ethernet Card	Select to configure parameters of the card.
MAC Address	MAC address of the access controller.
Mode	<ul style="list-style-type: none"> Static Set IP address, subnet mask, and gateway address manually. DHCP <ul style="list-style-type: none"> ◇ After DHCP is enabled, IP address, subnet mask, and gateway address cannot be configured. ◇ If DHCP is effective, IP address, subnet mask, and gateway address will be displayed automatically; if DHCP is not effective, IP address, subnet mask, and gateway address will all be zero. ◇ If you want to see the default IP when DHCP is effective, you need to disable DHCP.
Link-local address	Link-local address is only available when IPv6 is selected in the IP version. Unique link-local addresses will be assigned to network interface controller in each local area network to enable communications. The link-local address cannot be modified.
Subnet Mask	Enter IP address, and then configure subnet mask and gateway address.
Default Gateway	 IP address and gateway address must be in the same network segment.
Preferred DNS Server	Set IP address of the preferred DNS server.
Alternate DNS Server	Set IP address of the alternate DNS server.

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

4.9.2 Port

Set the maximum connections clients that the access controller can be connected to and port numbers.


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

Step 2 Configure port numbers. See the following table.



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

Table 4-12 Port description

Parameter	Description
Max Connection	You can set the maximum connections of clients that the access controller can be connected to.  Platform clients like Smartpss are not counted.
TCP Port	Default value is 37777.
HTTP Port	Default value is 80. If other value is used as port number, you need to add this value behind the address when logging in through browsers.
HTTPS Port	Default value is 443.
RTSP Port	Default value is 554.

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

4.9.3 Register

When connected to external network, the access controller will report its address to the server that is designated by the user so that clients can get access to the access controller.

Step 1 Select **Network Setting > Auto Register**.

Step 2 Select **Enable**, and enter host IP, port, and sub device ID.

Table 4-13 Auto register description

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

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

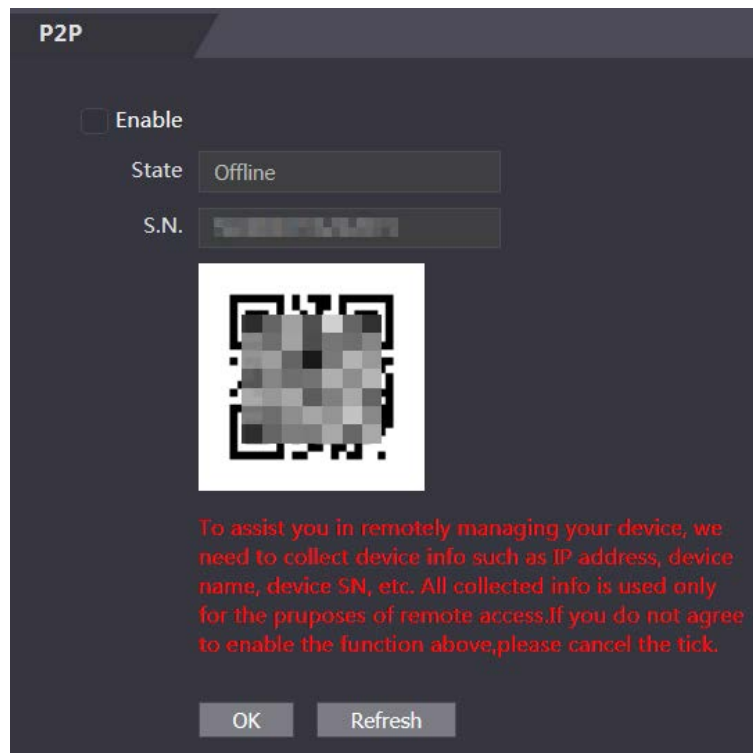
4.9.4 P2P

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



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

Figure 4-34 P2P



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

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

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



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

4.10 Date Setting

You need to set time zone, time, DST, and NTP for the access controller.



Only access controllers of certain models have this function.

Step 1 Select **Date Setting**.

Figure 4-35 Date Setting

Date Setting

Time Zone: GMT+08:00

System Time: 2019-12-07 15 : 15 : 39 Sync with PC

DST: ☐ Enable ☒ Close

Date Setting: ☒ Date ☐ Week

Starting Time: January 1 00 : 00

Ending Time: January 2 00 : 00

☐ NTP Setting

Server: clock.isc.org

Port: 123

Update Cycle: 60 Min.

OK Refresh Default

Step 2 Set parameters.

Table 4-14 Date setting

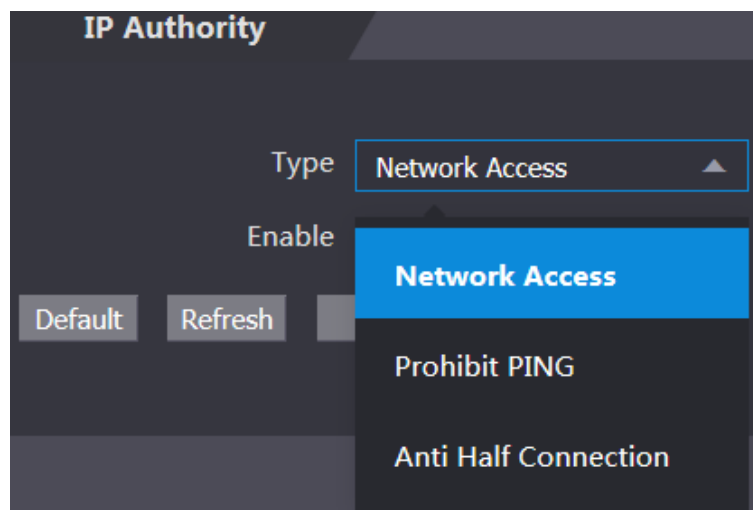
Parameter	Description
Time Zone	Select time zone as needed.
System Time	You can set system time manually, or you can click Sync with PC , to synchronize access controller time with the computer time.
DST	1. Enable DST. 2. Select Date or Week in Date Setting . 3. Set Starting Time and Ending Time .
NTP Setting	1. Enable NTP Setting . 2. Configure parameters. <ul style="list-style-type: none"> ◇ Server: Enter domain name of the NTP server. The access controller time will be synchronized with the NTP server. ◇ Port: Enter port number of the NTP server. ◇ Update Cycle: Set an update cycle, and then access controller time will be updated accordingly. 3. Click OK .

4.11 Safety Management

4.11.1 IP Authority

Select a cybersecurity mode as needed.

Figure 4-36 IP authority



4.11.2 Systems

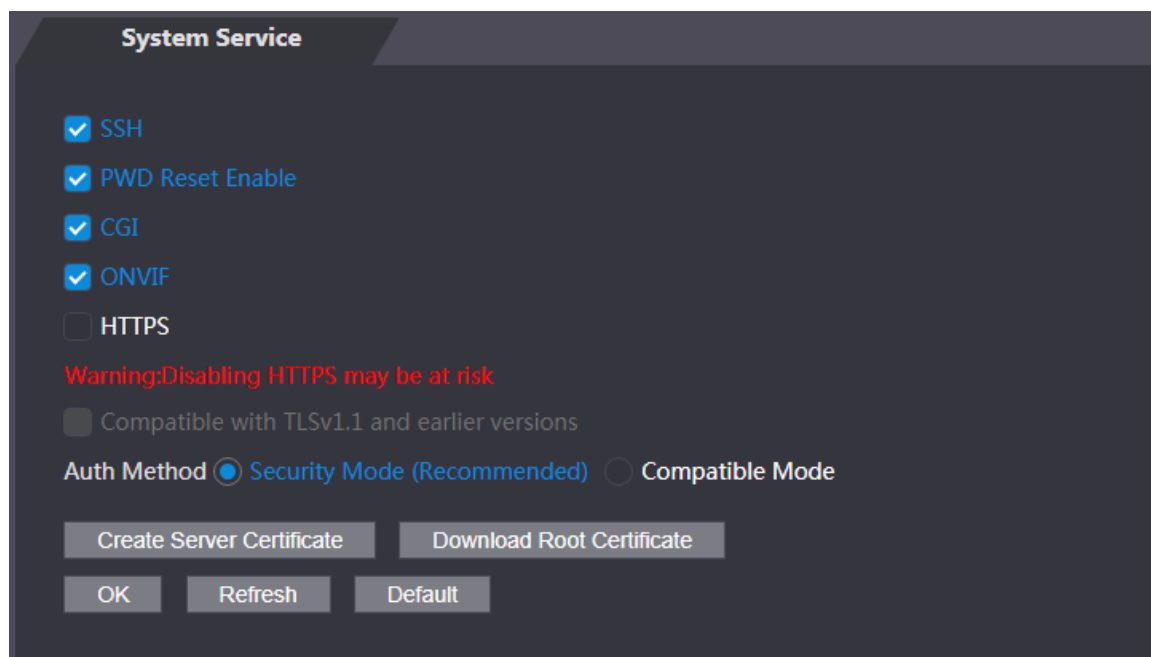
4.11.2.1 System Service

There are four options: SSH, PWD Reset Enable, CGI, and HTTPS. Refer to "3.9.4 Features" to select one or more than one of them.



The system service configuration done on the web page and the configuration on the **Features** interface of the access controller will be synchronized.

Figure 4-37 System service



4.11.2.2 Creating Server Certificate

Click **Create Server Certificate**, enter needed information, click **Save**, and then the access controller will reboot.

4.11.2.3 Downloading Root Certificate

Step 1 Click Download Root Certificate.

Select a path to save the certificate on the **Save File** dialog box.

Step 2 Double-click on the **Root Certificate** that you have downloaded to install the certificate. Install the certificate by following the onscreen instructions.

4.12 User Management

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

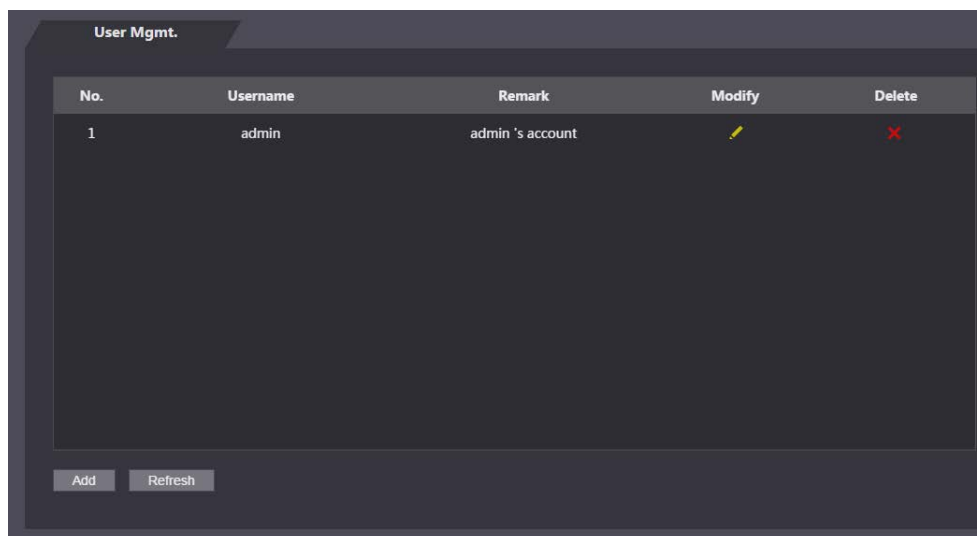
4.12.1 Adding Users

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

4.12.2 Modifying User Information

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

Figure 4-38 User management



4.12.3 Onvif User

Open Network Video Interface Forum (ONVIF), a global and open industry forum with the goal of

facilitating the development and use of a global open standard for the interface of physical IP-based security products. When ONVIF is used, administrator, operator, and user have different permission of ONVIF server. Create onvif users as needed.

Figure 4-39 Onvif user

Onvif User				
No.	Username	Group	Modify	Delete
1	admin	admin		
Add Refresh				

4.13 Maintenance

You can make the access controller reboot itself in idle time to improve the running speed of the access controller. You need to set the auto reboot date and time.

The default reboot time is at 2 O'clock in the morning on Tuesday. Click **Reboot Device**, the access controller will reboot immediately. Click **OK**, the access controller will reboot at 2 O'clock in the morning every Tuesday.

Figure 4-40 Maintenance

Maintenance

Auto Reboot

Tuesday

02:00

Reboot Device

OK

Refresh

Self Test

Test

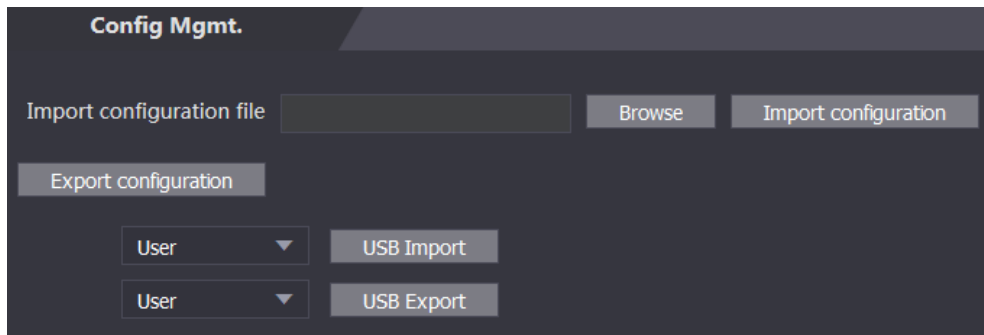
4.14 Configuration Management

You need to do configuration management, select unlock result feedback, Wiegand and serial settings for the access controller.

4.14.1 Config Mgmt.

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

Figure 4-41 Configuration management

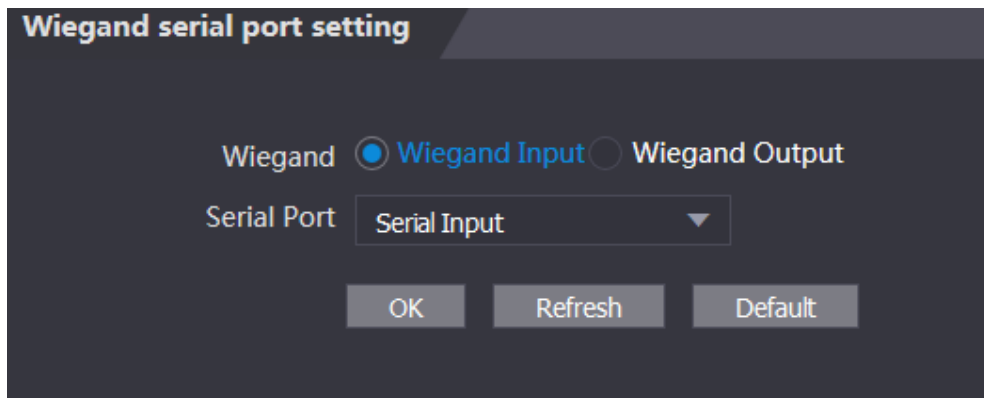


The screenshot shows a dark-themed window titled "Config Mgmt.". It contains a text input field labeled "Import configuration file" with a "Browse" button to its right and an "Import configuration" button further right. Below this is an "Export configuration" button. At the bottom, there are two rows, each with a "User" dropdown menu and a corresponding "USB Import" or "USB Export" button.

4.14.2 Wiegand Serial Port Setting

Select Wiegand/serial port setting as needed. For details, see "3.7.2 Serial Port Settings" and "3.7.3 Wiegand Configuration."

Figure 4-42 Wiegand serial port setting

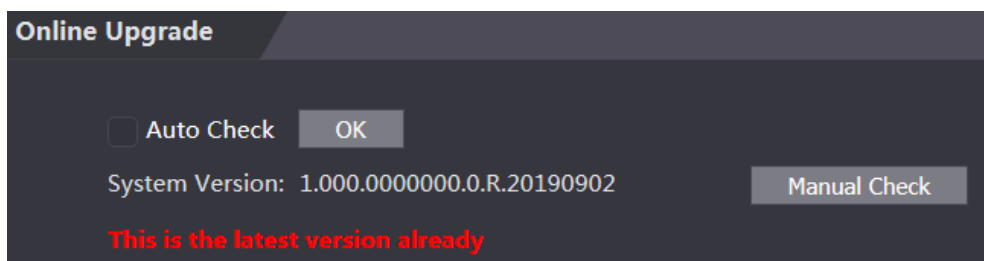


The screenshot shows a dark-themed window titled "Wiegand serial port setting". It features two radio buttons under the "Wiegand" label: "Wiegand Input" (which is selected) and "Wiegand Output". Below this is a "Serial Port" dropdown menu currently set to "Serial Input". At the bottom, there are three buttons: "OK", "Refresh", and "Default".

4.15 Upgrade

You can select **Auto Check** to upgrade the system automatically. You can also select **Manual Check** to upgrade the system manually.

Figure 4-43



The screenshot shows a dark-themed window titled "Online Upgrade". It has an "Auto Check" checkbox which is unchecked, followed by an "OK" button. Below this, the "System Version" is displayed as "1.000.0000000.0.R.20190902". To the right of the version is a "Manual Check" button. At the bottom, a red text message states "This is the latest version already".

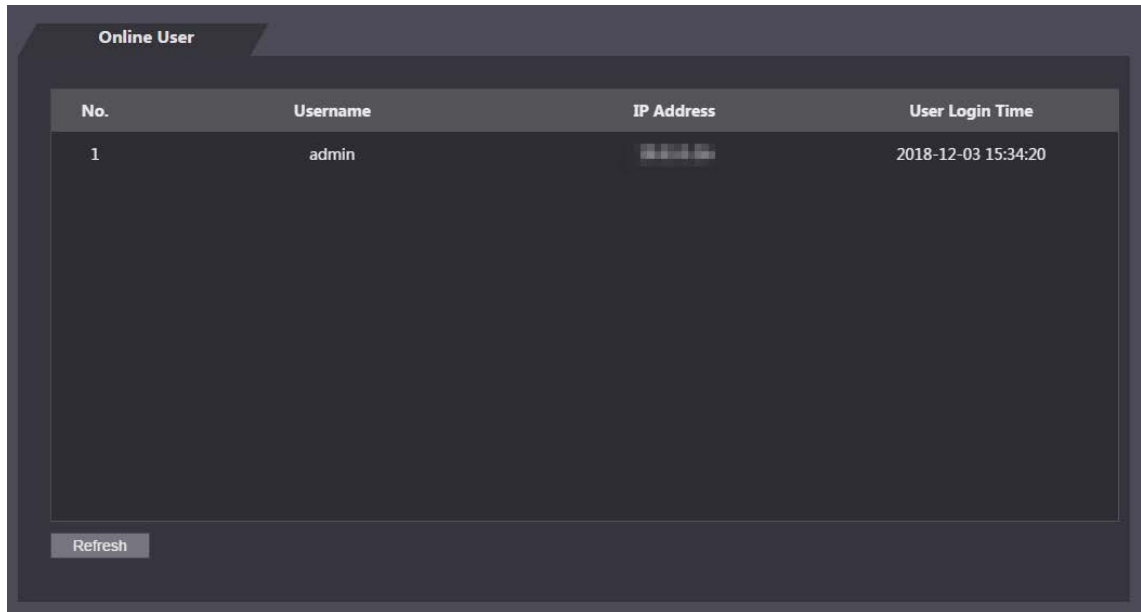
4.15.1 Version Information

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

4.15.2 Online User

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

Figure 4-44 Online user



The screenshot shows a web interface titled "Online User". It contains a table with the following data:

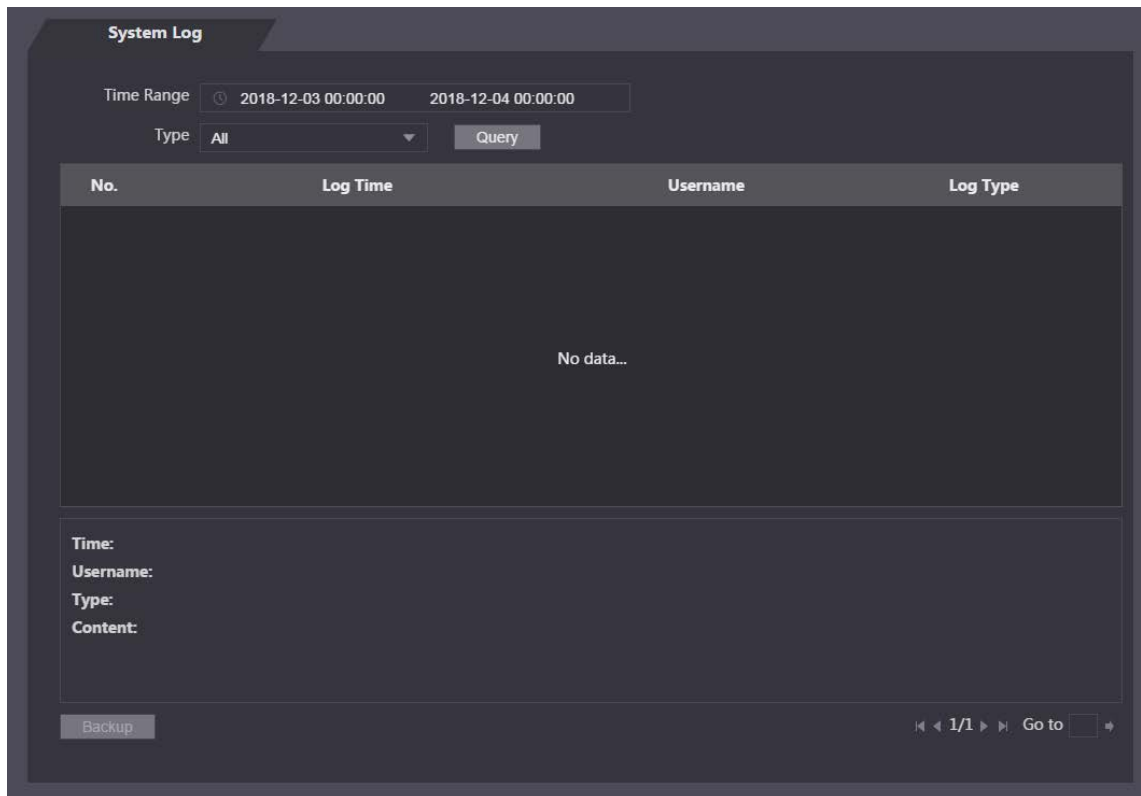
No.	Username	IP Address	User Login Time
1	admin	[REDACTED]	2018-12-03 15:34:20

Below the table, there is a "Refresh" button.

4.16 System Log

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

Figure 4-45 System log



System Log

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

Type: All

No.	Log Time	Username	Log Type
No data...			

Time:
Username:
Type:
Content:

1/1 Go to

4.16.1 Querying Logs

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

4.16.2 Backup Logs

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

4.17 Admin Log

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

Figure 4-46 Admin log


Admin Log

Admin ID Query


No.	Name	Time	Admin ID
No data...			

« 1/1 » Go to



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

4.18 Exit

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

5 Smart PSS Configuration

You can do access permission configuration to a single door or door groups through the Smart PSS client. For detailed configurations, see the Smart PSS user manual.



Smart PSS interfaces might vary with versions, and the actual interface shall prevail.

5.1 Login

Install the Smart PSS (the default username is admin, and the default password is admin123), double-

click  to operate it. Follow the instructions to finish the initialization and log in.

5.2 Adding Devices

You need to add access controllers to the Smart PSS. You can click **Auto Search** to add and click **Add** to manually add devices.

5.2.1 Auto Search

You can search and add access controllers at the same network segment to the Smart PSS.

Figure 5-1 Devices

Auto Search

+ Add

Delete

Import

Export

All Devices: 1

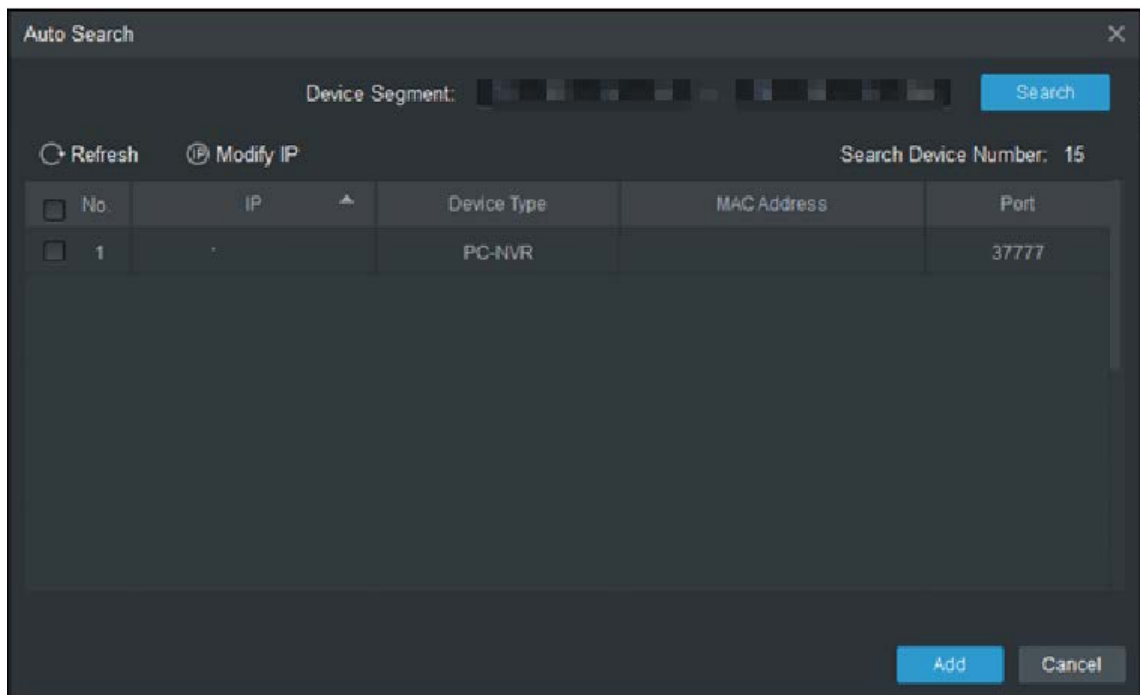
Online Devices: 1

All Device

Access Controller

No.	Name	IP/Domain Name	Device Type	Device Model	Port	annel Num	Online Status	SN	Operation
1	172.5.0.100		Access Cont...	ASi8215Y	37...	0/0/2/2	Online	4H05EE598766	<div><div></div><div></div><div></div></div>

Figure 5-2 Auto search



Step 1 Click **Auto Search**, enter the network segment, and then click Search. A list will be displayed.

Step 2 Select access controllers that you want to add to the Smart PSS, and then click Add, the Login information dialog box will be displayed.

Step 3 Enter the username and the login password to login.

You can see the added access controller on the **Devices** interface.



Select an access controller, click **Modify IP**, and you can modify the access controller's IP address. For details about IP address modification, see Smart PSS user manual.

5.2.2 Manual Add

You need to know IP addresses and domain names of access controllers that you want to add.

Figure 5-3 Devices

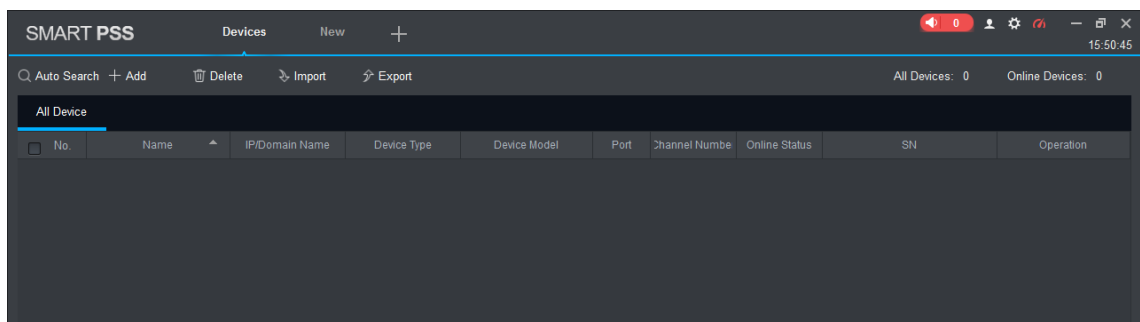
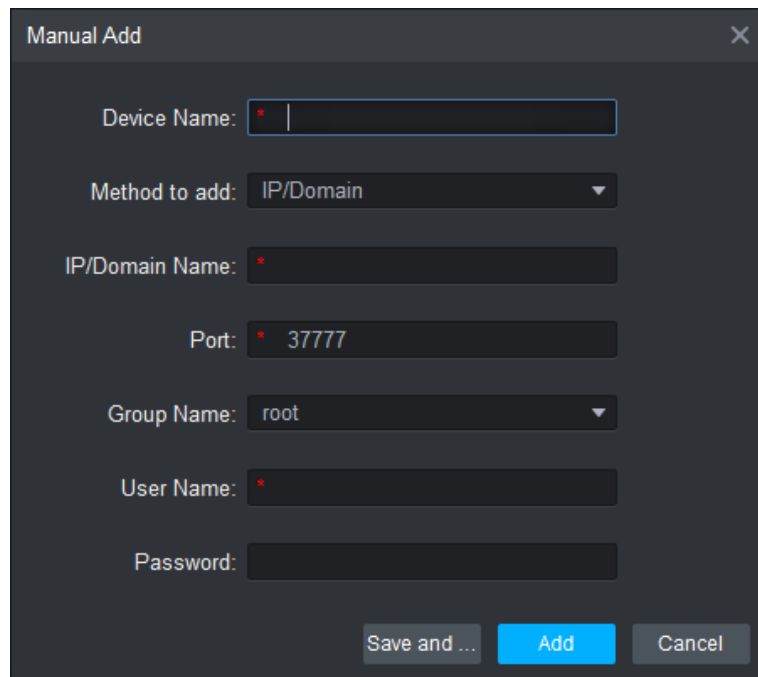


Figure 5-4 Manual add

A dark-themed dialog box titled "Manual Add" with a close button (X) in the top right corner. It contains several input fields and buttons. The fields are: "Device Name:" with a red asterisk and a text input field; "Method to add:" with a dropdown menu showing "IP/Domain"; "IP/Domain Name:" with a red asterisk and a text input field; "Port:" with a red asterisk and a text input field containing "37777"; "Group Name:" with a dropdown menu showing "root"; "User Name:" with a red asterisk and a text input field; and "Password:" with a text input field. At the bottom right, there are three buttons: "Save and ..." (disabled), "Add" (highlighted in blue), and "Cancel" (disabled).

Manual Add

Device Name: * |

Method to add: IP/Domain ▼

IP/Domain Name: *

Port: * 37777

Group Name: root ▼

User Name: *

Password:

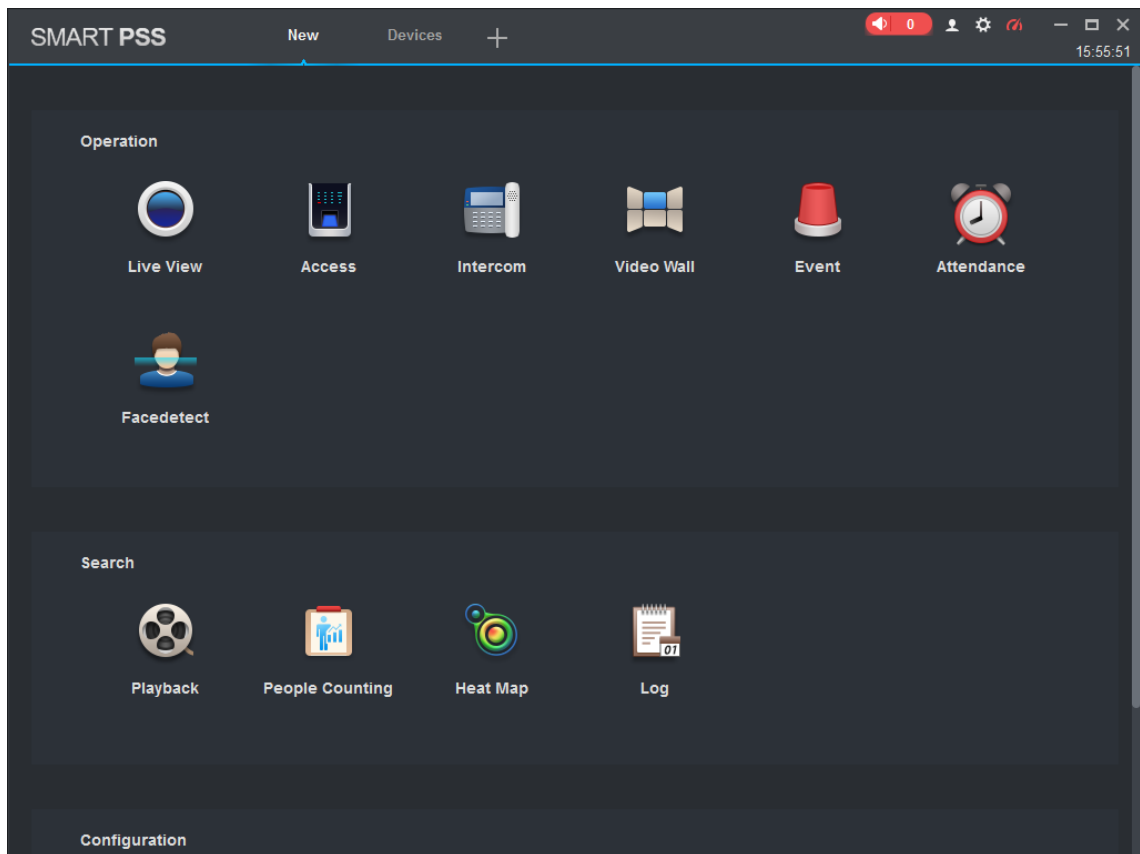
Save and ... Add Cancel

- Step 1 Click **Add** on the Devices interface, and the Manual Add interface will be displayed.
- Step 2 Enter the Device Name, select a method to add, enter the IP/Domain Name, Port number (37777 by default), Group Name, User Name, and Password.
- Step 3 Click **Add**, and then you can see the added access controller on the Devices interface.

5.3 Adding Users

Users are bound with cards. After you have added users to the Smart PSS, you can configure users access permissions on the **New > Access**.

Figure 5-5 New



5.3.1 Card Type Selection



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



On the **Access** interface, click , then click the IC or ID card icon, and then select a card type. There are two options: ID Card and IC Card.

Figure 5-6 Access

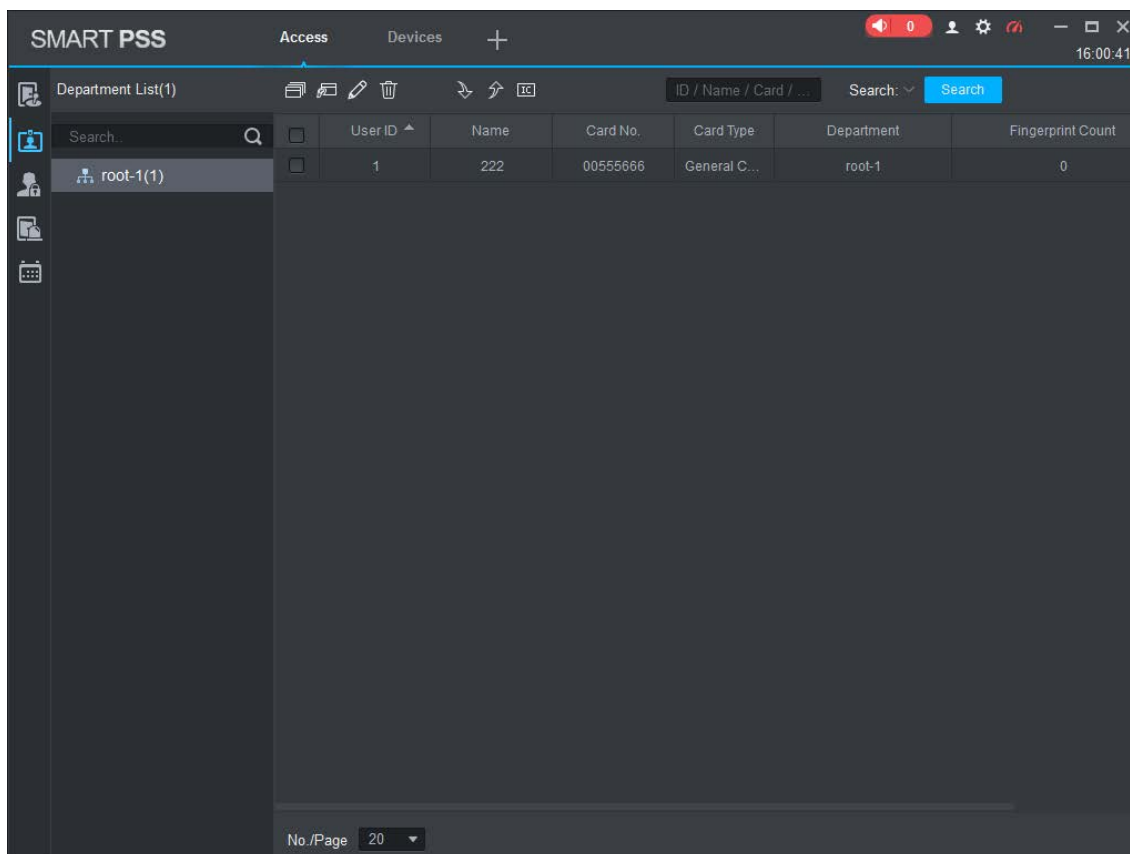
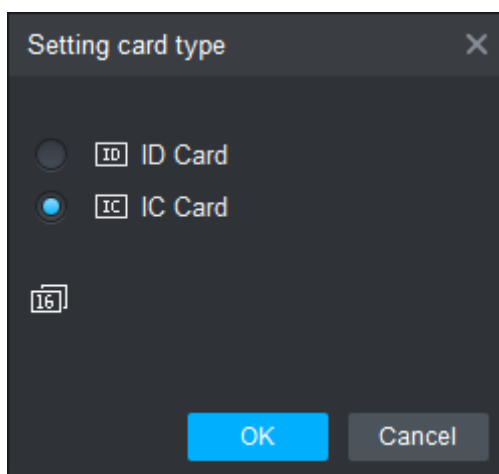


Figure 5-7 Setting card type



5.3.2 Adding One User

You can add users one by one.



On the **Access** interface, click , then click , and then enter user's information. Click **Finish** to complete the user adding.

Figure 5-8 Access

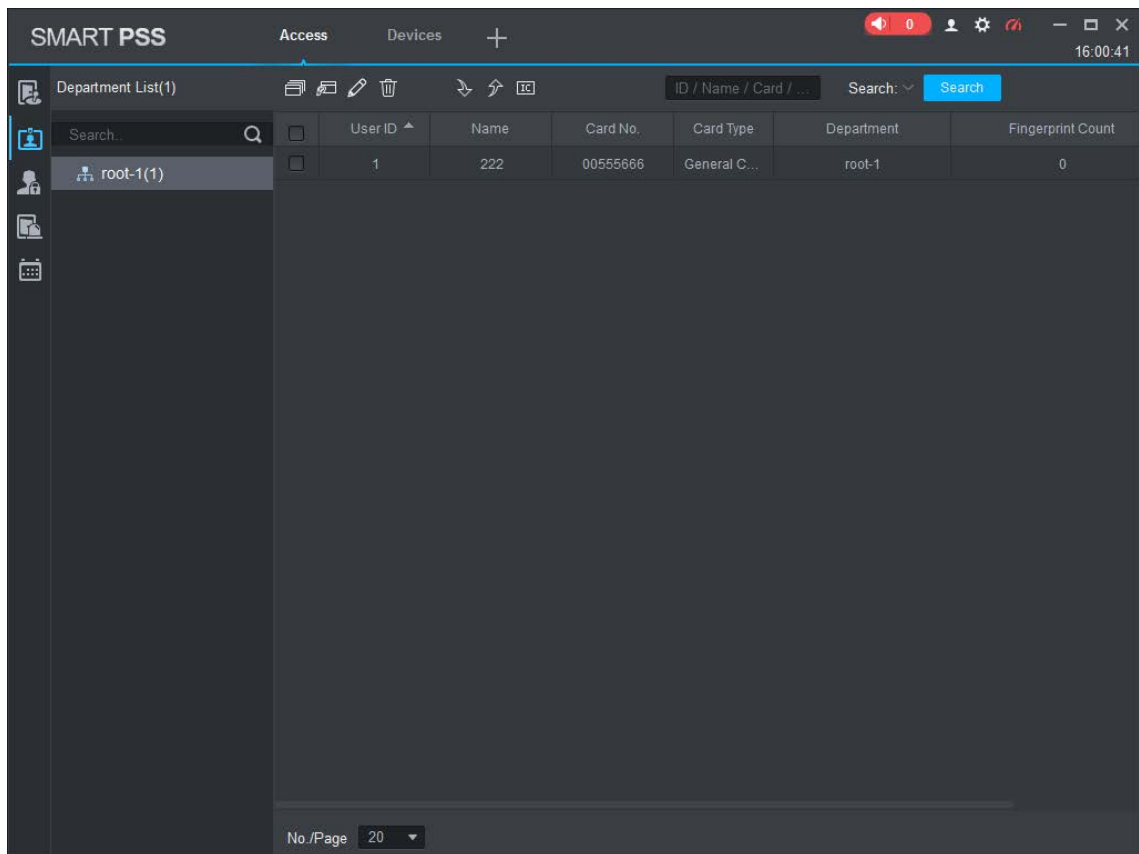


Figure 5-9 Add user

The screenshot shows the 'Add User' dialog box with three tabs: 'Basic Info', 'Fingerprint Info', and 'Details'. The 'Basic Info' tab is active. It contains the following fields:

- User ID: 2
- Name: (empty)
- Department: root-1
- Card No.: Card Reader not ready! Card issuer: (dropdown)
- Card Type: General Card
- Card Password: (empty)
- Unlock Password: (empty)
- Number of Use: 200
- Face Template...: 0 Select Device
- Valid Time: 2018/12/3 0:00:00 to 2028/12/3 23:59:59 (3654 Days)

At the bottom right, there are three buttons: 'Continue t...', 'Finish', and 'Cancel'.

5.4 Adding Door Group

You can manage doors by grouping doors.


On the **Access** interface, click , click **Add**, enter door group name, and then select a time zone. Click **Finish** to complete the user adding.

Figure 5-10 Access

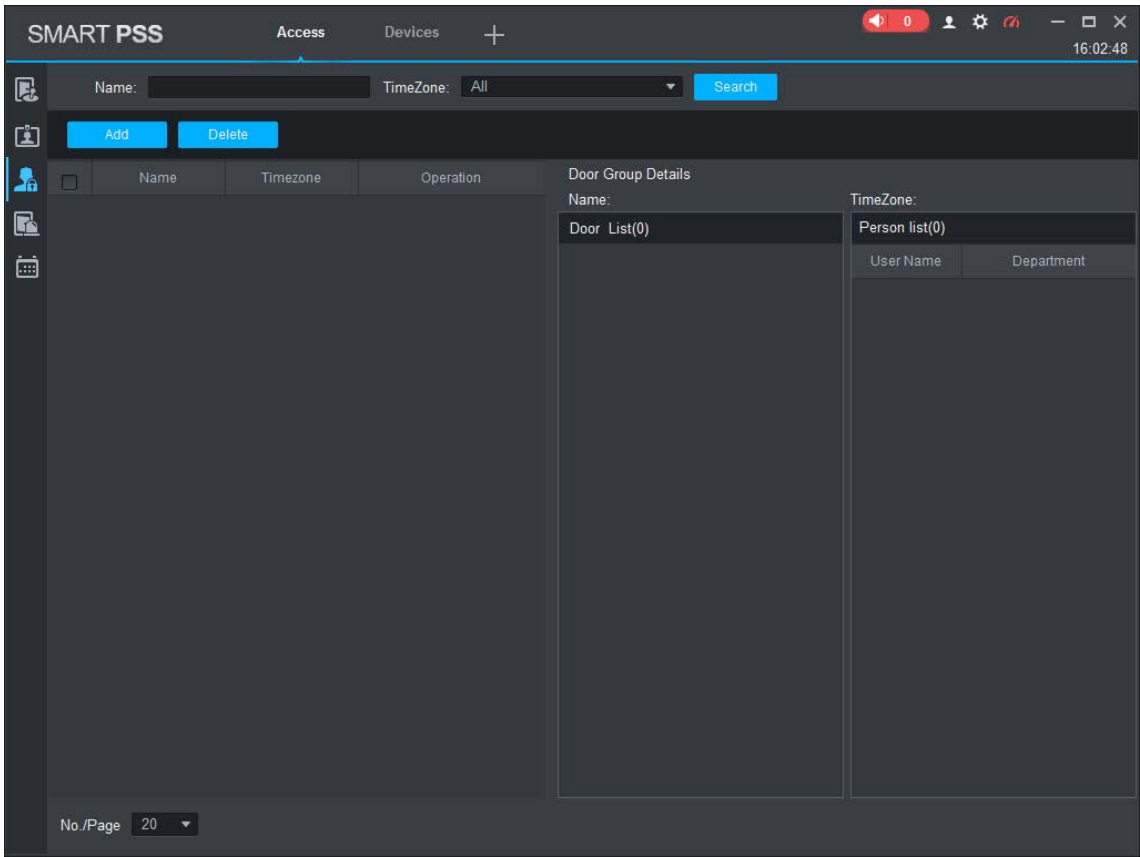
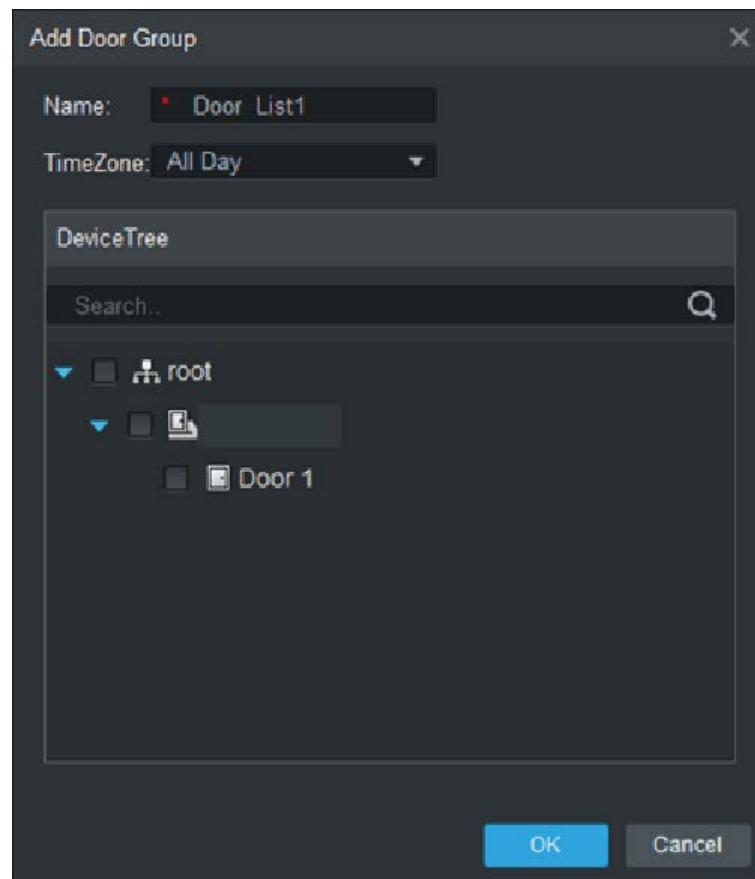


Figure 5-11 Add door group



5.5 Access Permission Configuration

You can do access permission configuration. There are two options: door group access permission and user access permission. Information of users who are given access permission in the Smart PSS and access controllers will be synchronized.

5.5.1 Giving Permission by Door Group

Select a door group, add users to the door list, and then users on the door list get access permissions of all doors on the door list.

Figure 5-12 Access

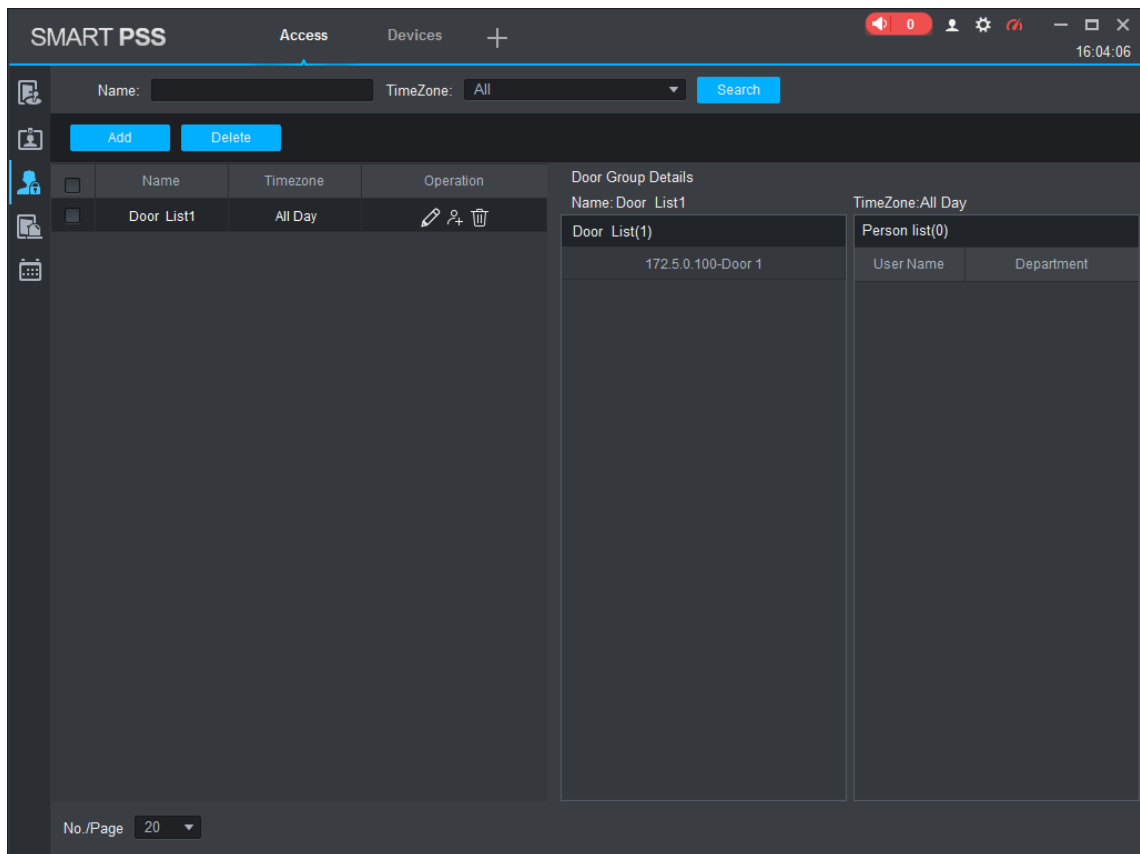
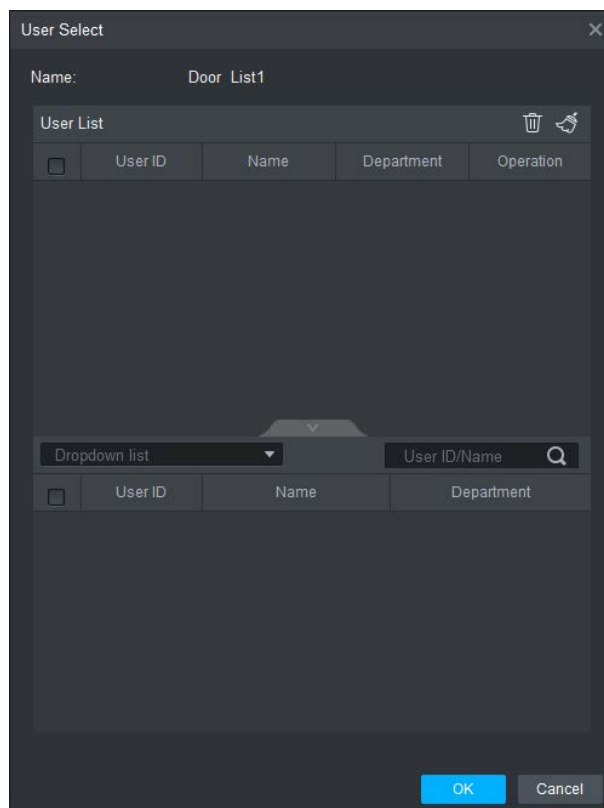



Figure 5-13 User select



Step 1 On the **Access** interface, click , click **Add**, and click **Door Group Permission**.

Step 2 Click . Select user department in the dropdown list, or enter user **ID/Name**, and then

search users. Select users from the users you found.

Step 3 Click **Finish** to complete the configuration.



Users without user ID cannot be found.

5.5.2 Giving Permission by User ID

You can give access permission to a user by selecting a user, and then select door groups for the user.

Figure 5-14 Access

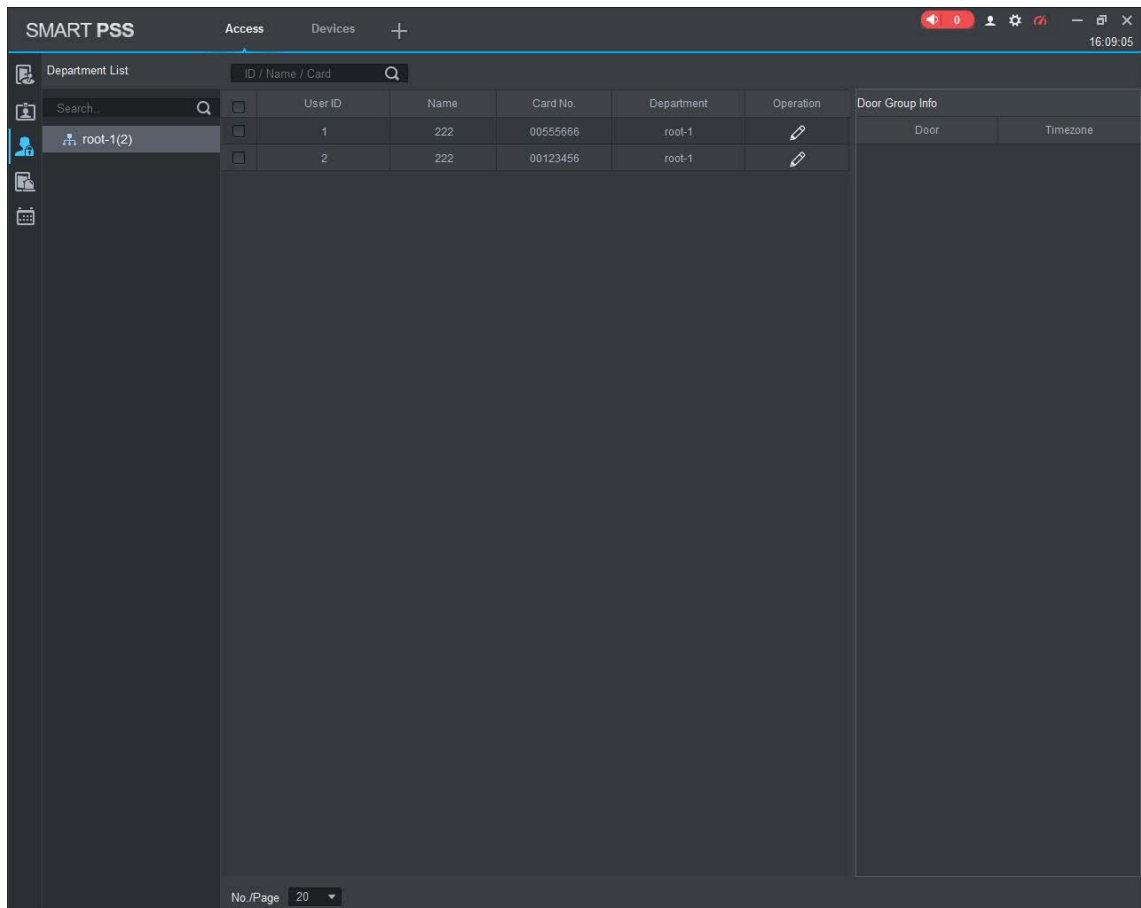
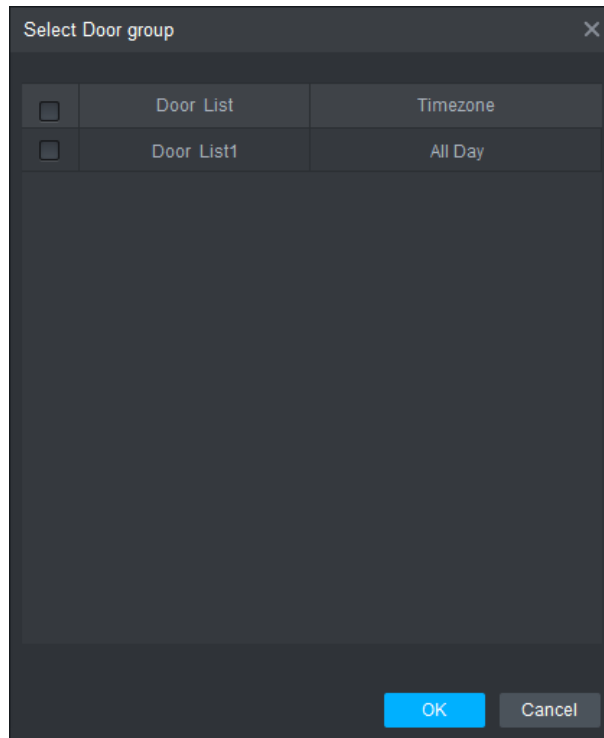




Figure 5-15 Select door group



- Step 1 On the **Access** interface, click .
- Step 2 Click . The Select Door Group interface is displayed.
- Step 3 Select user department in the dropdown list, or enter user ID/Name, and then select a door list.
- Step 4 Click **Finish**.

Appendix 1 Cybersecurity Recommendations

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

Mandatory actions to be taken for basic device network security:

1. Use Strong Passwords

Please refer to the following suggestions to set passwords:

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

2. Update Firmware and Client Software in Time

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

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

1. Physical Protection

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

2. Change Passwords Regularly

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

3. Set and Update Passwords Reset Information Timely

The device supports password reset function. Please set up related information for password reset in time, including the end user's mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

4. Enable Account Lock

The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

5. Change Default HTTP and Other Service Ports

We suggest you to change default HTTP and other service ports into any set of numbers between 1024~65535, reducing the risk of outsiders being able to guess which ports you are using.

6. Enable HTTPS

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

7. MAC Address Binding

We recommend you to bind the IP and MAC address of the gateway to the device, thus reducing the risk of ARP spoofing.

8. Assign Accounts and Privileges Reasonably

According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

9. Disable Unnecessary Services and Choose Secure Modes

If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.

If necessary, it is highly recommended that you use safe modes, including but not limited to the following services:

- SNMP: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
- SMTP: Choose TLS to access mailbox server.
- FTP: Choose SFTP, and set up strong passwords.
- AP hotspot: Choose WPA2-PSK encryption mode, and set up strong passwords.

10. Audio and Video Encrypted Transmission

If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

Reminder: encrypted transmission will cause some loss in transmission efficiency.

11. Secure Auditing

- Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
- Check device log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

12. Network Log

Due to the limited storage capacity of the device, the stored log is limited. If you need to save the log for a long time, it is recommended that you enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

13. Construct a Safe Network Environment

In order to better ensure the safety of device and reduce potential cyber risks, we recommend:

- Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
- The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
- Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
- Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.