Face Recognition Access Controller with Temperature Monitoring Unit

User's Manual

V1.0.0

Foreword

General

This manual introduces the installation and detailed operations of the face recognition access controller with temperature monitoring unit (hereinafter referred to as "access controller").

This manual applies to model G and model J access controllers. Figures of model G access controllers are demonstrated in the manual for example.

Safety Instructions

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

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

Revision History

Version	Revision Content	Release Date
V1.0.0	First Release.	May 2021

About the Manual

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

contact the customer service for the latest program and supplementary documentation.

- There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, please refer to our final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and the company names in the manual are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurred when using the device.
- If there is any uncertainty or controversy, please refer to our final explanation.

Important Safeguards and Warnings

This chapter describes the contents covering proper handling of the 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 place or install the access controller in a place exposed to sunlight or near the heat source.
- Keep the access controller away from dampness, dust or soot.
- Keep the access controller installed horizontally on the stable place to prevent it from falling.
- Do not drop or splash liquid onto the access controller, and make sure there is no object filled with liquid on the access controller to prevent liquid from flowing into the access controller.
- Install the access controller in a well-ventilated place, and do not block the ventilation of the access controller.
- Operate the access controller within the rated range of power input and output.
- Do not dissemble the access controller randomly.
- Transport, use and store the access controller under the allowed humidity and temperature conditions.
- When used in outdoors with high temperature, do not directly touch the surface of the access controller, such as the screen, metal back shell, and fingerprint sensor.

Electrical Safety

- Improper battery use might result in fire, explosion, or inflammation.
- When replacing battery, make sure the same model is used.
- Use the recommended power cables in the region and conform to the rated power specification.
- Use the power adapter provided with the access controller; otherwise, it might result in people injury and damage of the access controller.
- Use a power supply that meets ES1 but does not exceed PS2 limits defined in IEC 62368-1. For specific power supply requirements, refer to labels on the access controller.
- Connect the access controller (I-type structure) to the power socket with protective earthing.
- The appliance coupler is a disconnection device. When using the coupler, keep the angle for easy operation.

Table of Contents

1 Overview

1.1 Introduction

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

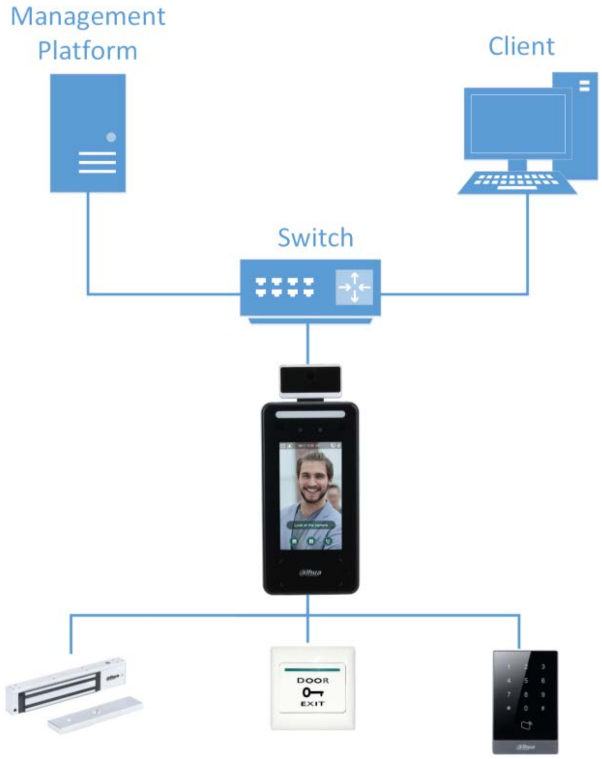
1.2 Features

- LCD display, the resolution of 4.3-inch access controller is 480 × 272.
- Supports face unlock, IC card unlock, fingerprint unlock, and password unlock; unlock by period.
- With a face detection box, the largest face among faces that appear at the same time is recognized first; the maximum face size can be configured on the web interface.
- 2MP wide-angle WDR lens; with auto/manual illuminator.
- Face recognition distance is 0.3 m–1.5 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, tamper alarm, intrusion alarm, door contact timeout alarm, illegal card exceeding threshold alarm, illegal password exceeding threshold alarm and external alarm.
- Supports general users, patrol users, blocklist users, VIP users, guest users, other users, and custom users.
- Various unlock status display modes to protect user privacy.
- Supports body temperature monitoring.

1.3 Application

The access controller is applicable for parks, office buildings, schools, factories, residential areas and other places. The identity is verified through face recognition to achieve passage without perception.

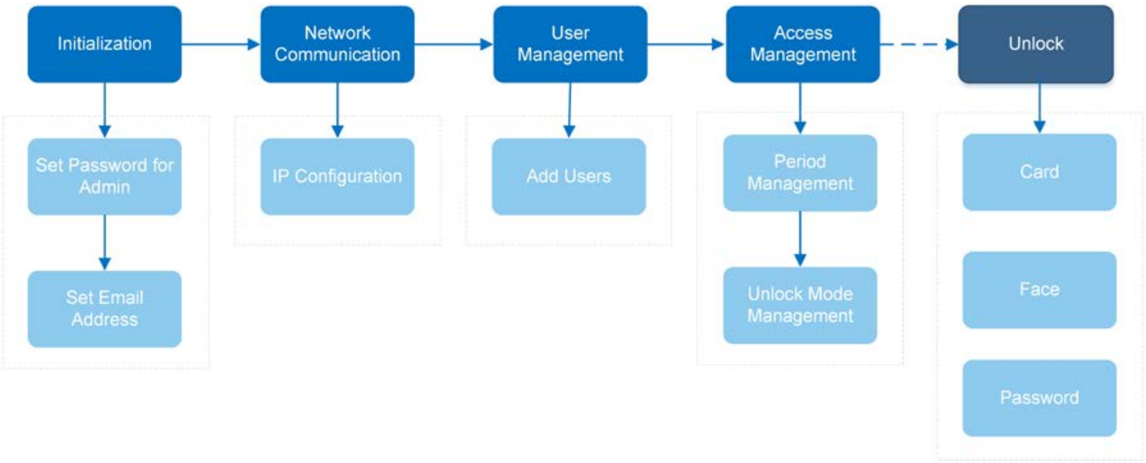
Figure 1-1 Networking



2 System Operations

2.1 Basic Configuration Procedure

Figure 2-1 Basic configuration procedure



2.2 Common Icons

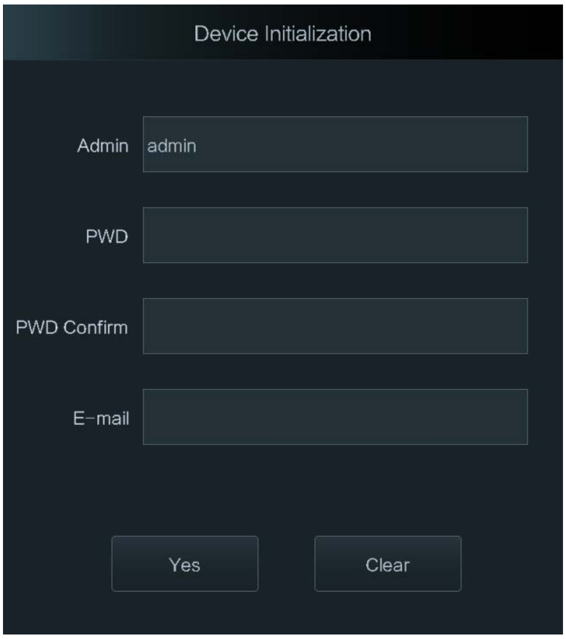
Table 2-1 Icon description

Icon	Description
✓	Confirm icon.
|<	Turn to the first page of the list.
>|	Turn to the last page of the list.
<	Turn to the previous page of the list.
>	Turn to the next page of the list.
←	Return to the previous menu.
ON	Enable.
OFF	Disable.
∧	Turn to previous page.
∨	Turn to next page.

2.3 Initialization

Administrator password and an email should be set the first time the access controller is turned on or after reset; otherwise the access controller cannot be used.

Figure 2-2 Initialization



Device Initialization

Admin admin

PWD

PWD Confirm

E-mail

- 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 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 ' " ; : &).

2.4 Standby Interface

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

- The unlock methods might vary with different models.
- If there are no operations in 30 seconds, the access controller will go to the standby mode.
- The standby interfaces shown in this section are for reference only, and might differ from the actual ones.

Figure 2-3 Standby interface of model J

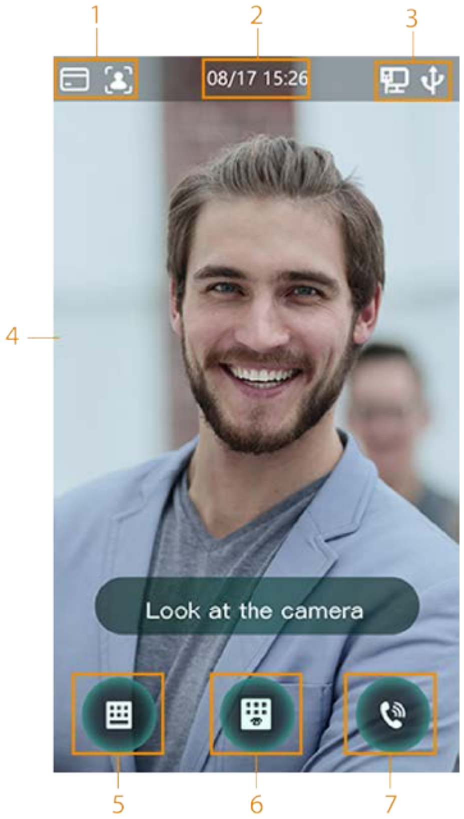


Figure 2-4 Standby interface of model G

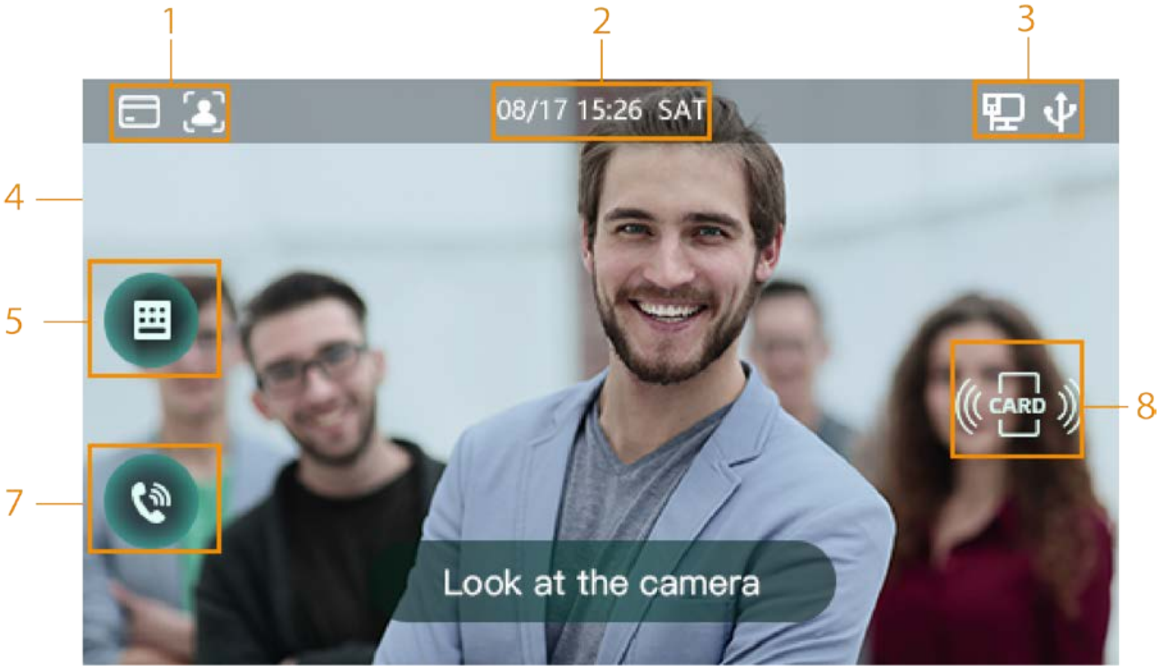


Table 2-2 Homepage description

No.	Description
1	Unlock methods: Card, face, fingerprint and password. 📖 When card, face, fingerprint and password are all set as unlock mode, the password icon will not be displayed at the top left corner of the access controller.
2	Date & Time. Displays the current date and time.

No.	Description
3	Display the network status and USB status.
4	Face recognition area.
5	Password unlock icon.
6	Administrator password unlock icon.
7	Tap to call other devices.
8	Card swiping area.

2.5 Main Menu

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

Step 1 On the standby interface, long press 3 s to go to the **Administrator Login** interface.

Step 2 Select a main menu entering method.

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

Figure 2-5 Administrator login

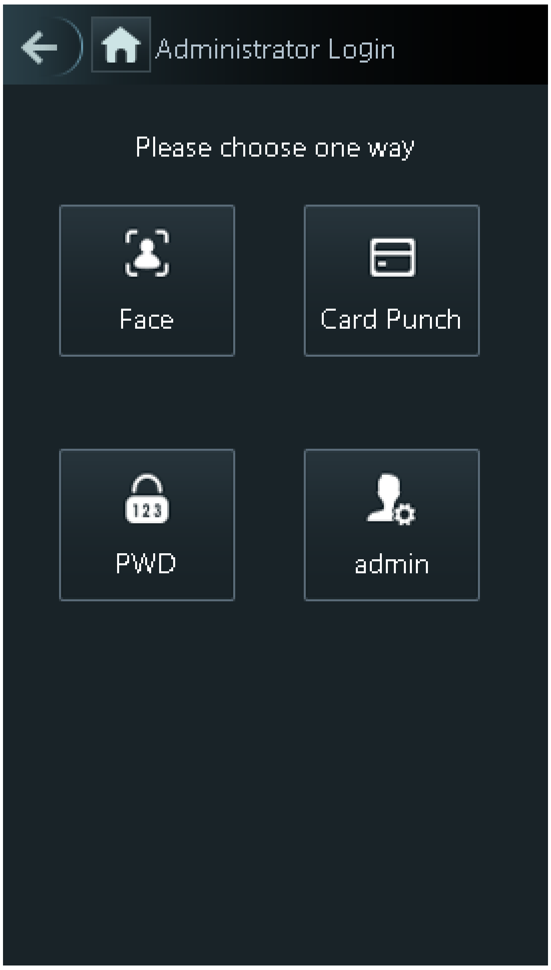
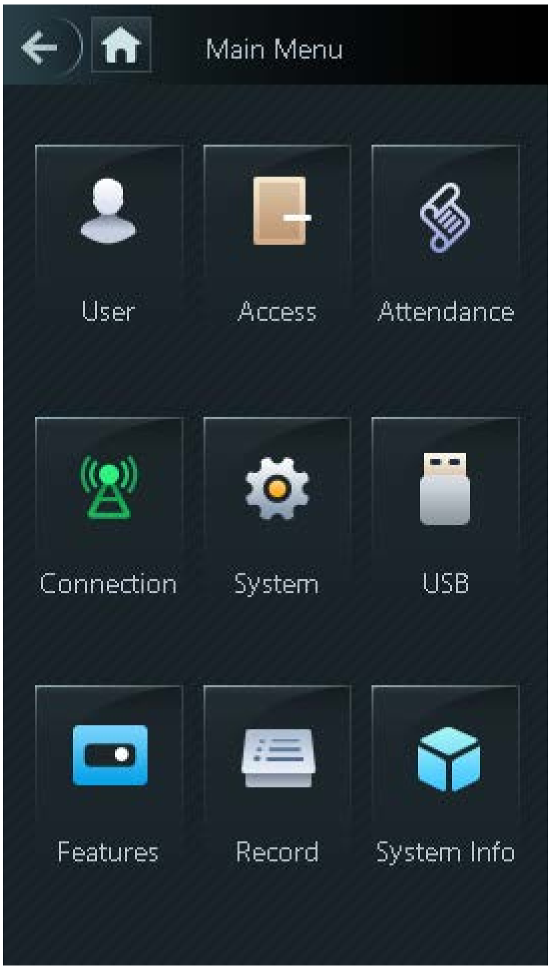


Figure 2-6 Main menu



2.6 Unlocking Methods

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

2.6.1 Cards

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

2.6.2 Face

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

2.6.3 Fingerprints

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

Only certain models support this function.

2.6.4 User Password

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

Step 1 Tap ⌨ on the homepage.

Step 2 Tap **PWD Unlock**.

Step 3 Enter the user ID and password, and then tap ☑.

The door is unlocked.

2.6.5 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 "2.8.1.5 NC Period."

Step 1 Tap ⌨ on the homepage.

Step 2 Tap **Admin PWD**.

Step 3 Enter the administrator password, and then tap ☑.

The door is unlocked.

2.7 User Management

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

2.7.1 Adding New Users

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

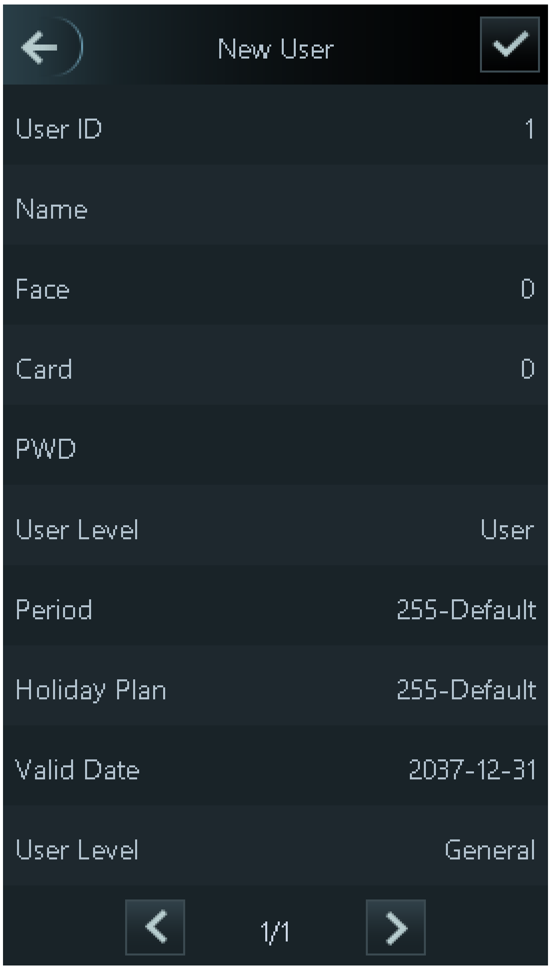
📖

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

Step 1 Log in to the **Main Menu** interface.

Step 2 Select **User > New User**.

Figure 2-7 New User Info



New User

User ID	1
Name	
Face	0
Card	0
PWD	
User Level	User
Period	255-Default
Holiday Plan	255-Default
Valid Date	2037-12-31
User Level	General

Step 3 Configure parameters on the interface.

Table 2-3 New user parameter description

Parameter	Description
User ID	Enter user IDs. The IDs can be numbers, letters, and their combinations, and the maximum length of the ID is 32 characters. Each ID is unique.
Name	Enter names with at most 32 characters (including numbers, symbols, and letters).
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.
Card	You can register five cards at most 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. You can enable the **Duress Card** function on the card registration interface. Alarms will be triggered if a duress card is used to unlock the door. Only certain models support card unlock.
PWD	The door unlocking password. The maximum length of the password is 8 digits. If the access controller is without touch screen, you need to connect the access controller to a peripheral card reader. There are buttons on the card reader.

Parameter	Description
User Level	You can select a user level for new users. There are two options: ● User: Users only have door unlock permission. ● Admin: Administrators can unlock the door and also have parameter configuration permission. 🕮 No matter whether there is an administrator in the access controller, administrator identity authentication is needed.
Period	You can set a period in which the user can unlock the door. "See 3.7 Time Section" for details.
Holiday Plan	You can set a holiday plan in which the user can unlock the door. "See 3.7 Time Section" for details.
Valid Date	You can set a period during which the unlocking information of the user is valid.
User Level	There are six levels: ● General: General users can unlock the door normally. ● Blocklist: Users in the blocklist do not have unlock permission. When they try to unlock the door, the access controller will prompt that this is a blocklist user. ● Guest: Guests are allowed to unlock the door certain times. Once they exceed the maximum times, they cannot unlock the door again. ● Patrol: Paroling users can get their attendance tracked, but they have no unlock permission. ● VIP: When VIP unlocks the door, service personnel will get a prompt. ● Other: When special people unlock the door, there will be a delay of 5 seconds before the door is closed. ● Custom User 1: Reserved for customization. Users can unlock the door normally. ● Custom User 2: Reserved for customization. Users can unlock the door normally.
Use Time	When the user level is Guest, you can set the maximum number of times that the user can unlock the door.

Step 4 Tap ✓ to save the configuration.

2.7.2 Viewing User information

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

2.8 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.

2.8.1 Period Management

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

2.8.1.1 Period Config

For model G access controllers, you can configure periods locally; for model J access controllers, you can configure periods through web interface.

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 periods that you set.

2.8.1.2 Holiday Group

For model G access controllers, you can configure holiday groups locally; for model J access controllers, you can configure holiday groups through web interface.

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 periods that you set.

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

2.8.1.3 Holiday Plan

For model G access controllers, you can configure holiday plans locally; for model J access controllers, you can configure holiday plans through web interface.

You can add holiday groups into holiday plans. You can use holiday plans to manage user access permission in different holiday groups. Users can only unlock the door in the period that you set.

2.8.1.4 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.

2.8.1.5 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.

2.8.1.6 Remote Verification Period

If you configured the remote verification period, 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 **Remote Verification Period**.

- ◉ means enabled.
- ○ means not enabled.

2.8.2 Unlock

There are two unlock modes: unlock mode and temperature monitoring mode. The unlock modes described in this section are for reference only, and might vary with the model.

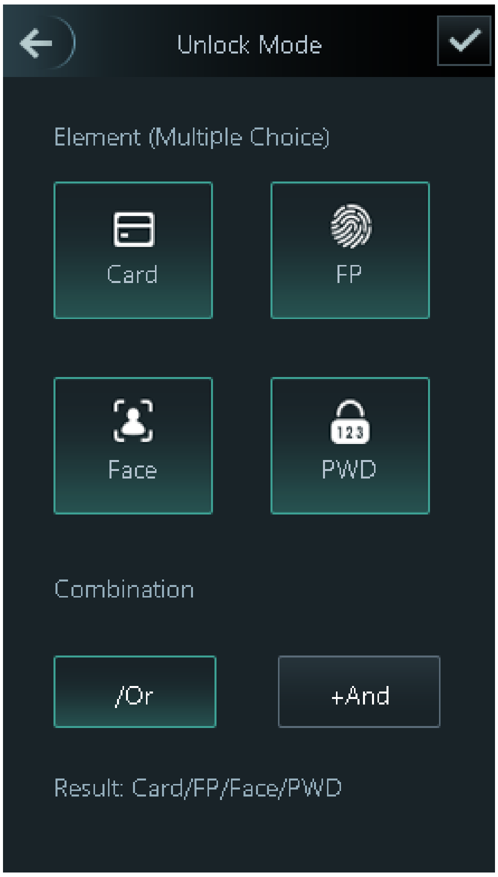
2.8.2.1 Unlock Mode

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

Step 1 Log in to the **Main Menu** interface.

Step 2 Select **Access** > **Unlock Mode** > **Unlock Mode**.

Figure 2-8 Element (multiple choice)



Result: Card/FP/Face/PWD

Step 3 Select one or more unlock methods.

- The unlock methods displayed in the figure above are for reference only, and might vary with different models.
- Tap a selected unlock method again to deselect it.

Step 4 Select a combination mode.

- **+ And**: For example, if you select card + PWD, you need to swipe your card first, and then enter the password to unlock the door.
- **/ Or**: For example, if you select card/PWD, you can swipe your card or enter the password to unlock the door.

Step 5 Tap ✓ to save the settings.

Step 6 Enable **Unlock Mode**.

- ◉ means enabled.
- ○ means not enabled.

2.8.2.2 Temperature Monitoring Mode

The access controller will unlock the door when your temperature is normal.

Step 1 Log in to the **Main Menu** interface.

Step 2 Select **Access > Unlock Mode**, and then enable **Temp Monitoring Mode Only**.

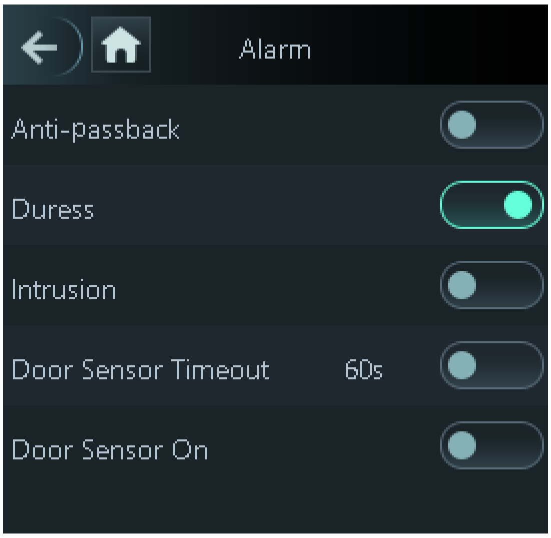
2.8.3 Alarm Configuration

Administrators can manage visitors' unlock permission through alarm configuration.

Step 1 Log in to the **Main Menu** interface.

Step 2 Select **Access** > **Alarm**.

Figure 2-9 Alarm



Alarm

Anti-passback: ☐

Duress: ☑

Intrusion: ☐

Door Sensor Timeout 60s: ☐

Door Sensor On: ☐

- ☑ means enabled.
- ☐ means disabled.

Table 2-4 Parameters on the alarm interface

Parameter	Description
Anti-passback	After the anti-passback is enabled, users need to verify identities both for entry and exit; otherwise an alarm will be triggered. ● If a person enters with the identity checked and exits without the identity checked, an alarm will be triggered when the person tries to enter again and the person will have no permission to unlock the door any more. ● If a person enters without the identity checked, an alarm will be triggered when the person tries to exit with the identity checked, and the person will have no permission to unlock the door any more.
Duress	An alarm will be triggered when a duress card or duress password is used to unlock the door.
Intrusion	An intrusion alarm will be triggered if a door is unlocked without having the door contact released.
Door Sensor Timeout	A timeout alarm will be triggered if the time that a user takes to unlock the door exceeds the Door Sensor Timeout time. The Door Sensor Timeout time range is 1–9999 seconds.
Door Sensor On	Only when the **Door Sensor On** is enabled can the intrusion alarm and door sensor timeout alarm be triggered.

2.8.4 Door Status

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

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

2.8.5 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.

2.9 Attendance

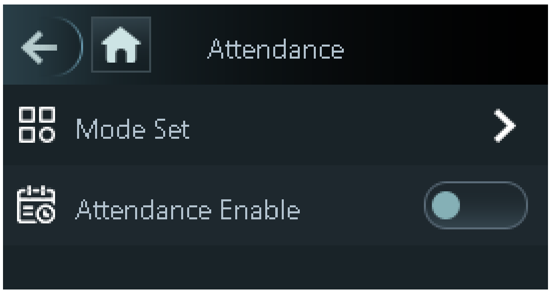
You can enable attendance and configure the attendance mode as needed.

This function needs to work with a platform. For details, see corresponding user's manual.

Step 1 Log in to the **Main Menu** interface.

Step 2 Tap **Attendance**, and then tap ○ to enable attendance.

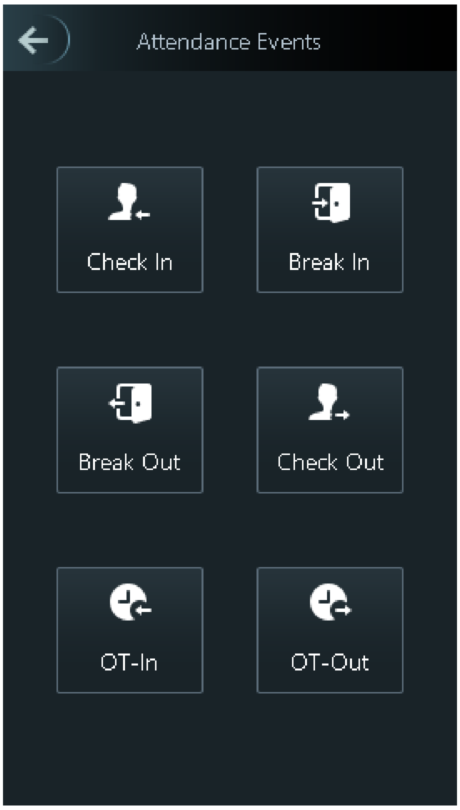
Figure 2-10 Attendance



Step 3 Tap **Mode Set** to set an attendance mode and the time for different attendance statuses.

- **Auto/Manual Mode**: Displays the attendance status according to the time you check in or out. If the time you check in or out is not defined, you can tap **Attendance Events** and select an attendance status as needed.
- **Auto Mode**: Displays the attendance status according to the time you check in or out.
- **Manual Mode**: You need to manually select an attendance status when you check in or out.
- **Fixed Mode**: The attendance status is fixed when you punch in or out on the standby interface.

Figure 2-11 Attendance status



Attendance Events

Check In

Break In

Break Out

Check Out

OT-In

OT-Out

For the six statuses, you can define them as needed, such as **Check In** for the start of a work day and **Break Out** for the start of lunch break.

2.10 Network Communication

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

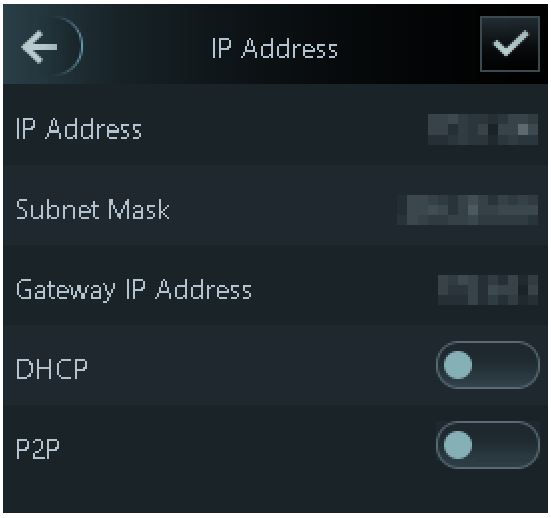
2.10.1 IP Configuration

Configure an IP address for the access controller to make it be connected to the network.

Step 1 Log in to the **Main Menu** interface.

Step 2 Select **Connection > Network > IP Address**, and then configure IP address parameters.

Figure 2-12 IP address configuration



IP Address

IP Address [redacted]

Subnet Mask [redacted]

Gateway IP Address [redacted]

DHCP ○

P2P ○

Table 2-5 IP configuration parameters

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

Make sure that the computer used to log in to the web interface is in the same LAN with the access controller.

2.10.2 Active Register

By active registering, you can connect the access controller to the management platform, and then you can manage the access controller through the management platform.

Configurations you have made can be cleared on the managing platform, and the access controller can be initialized, you need to protect the platform managing permission in case of data loss caused by improper operation.

Step 1 Log in to the **Main Menu** interface.

Step 2 Select **Connection > Network >Active Register**.

Step 3 Tap ○ to enable active register, and then configure parameters.

Table 2-6 Active register

Name	Parameter
Server IP Address	IP address of the managing platform.

Name	Parameter
Port	Port number of the managing platform.
Device ID	Subordinate device number on the managing platform.

2.10.3 Wi-Fi

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

Step 1 Log in to the **Main Menu** interface.

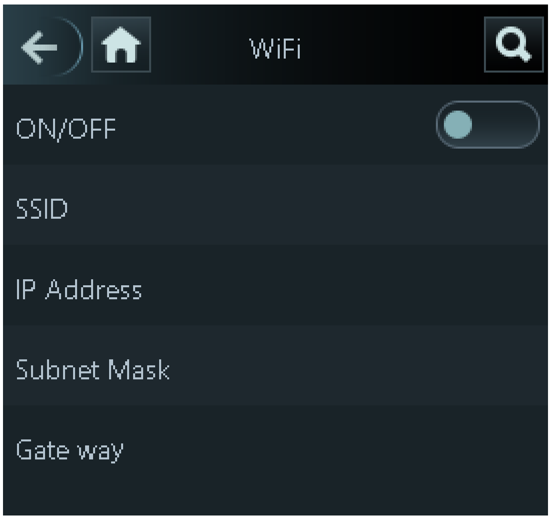
Step 2 Select **Connection > Network >WiFi**.

Step 3 Tap ● to enable Wi-Fi.

Step 4 Tap 🔍, select a network, and then enter the password.

You can see the information of the network in the following interface.

Figure 2-13 Wi-Fi



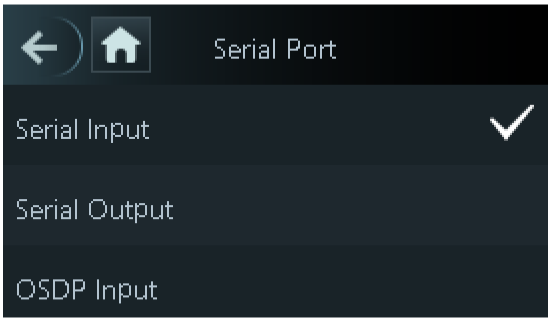
2.10.4 Serial Port Settings

Select serial input or serial output according to the use of the external devices.

Step 1 Log in to the **Main Menu** interface.

Step 2 Select **Connection > Serial Port**.

Figure 2-14 Serial port



- Select **Serial Input** when external devices that 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, card reading and writing functions, if you select **Serial Output**, access controller will send lock/unlock information to other access controllers. There are two types of lock/unlock information: User ID and card number.

- 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.

2.10.5 Wiegand Configuration

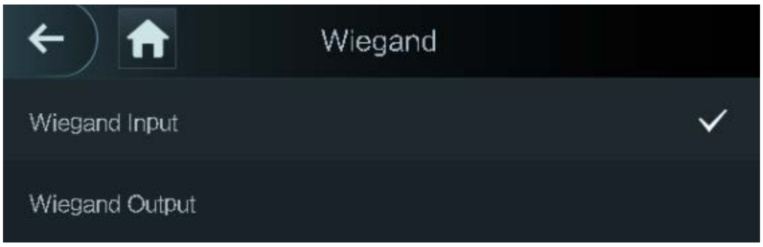
Only model J access controllers support this function.

Select **Wiegand Input** or **Wiegand Output** accordingly.

Step 1 Log in to the **Main Menu** interface.

Step 2 Select **Connection > Wiegand**.

Figure 2-15 Wiegand



- Select **Wiegand Input** when an external card swipe mechanism is connected to the access controller.

- Select **Wiegand Output** when the access controller works as a reader that can be connected to other controllers. See Table 2-7.

Table 2-7 Wiegand output

Parameter	**Description**
Wiegand Output Type	The **Wiegand Output Type** determines the card number or the digit of the number that can be recognized by the access controller. ● Wiegand26, three bytes, six digits. ● Wiegand34, four bytes, eight digits. ● Wiegand66, eight bytes, sixteen digits.
Pulse Width	Set the valur as needed.
Pulse Interval	
Output Data Type	● **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.

2.11 System

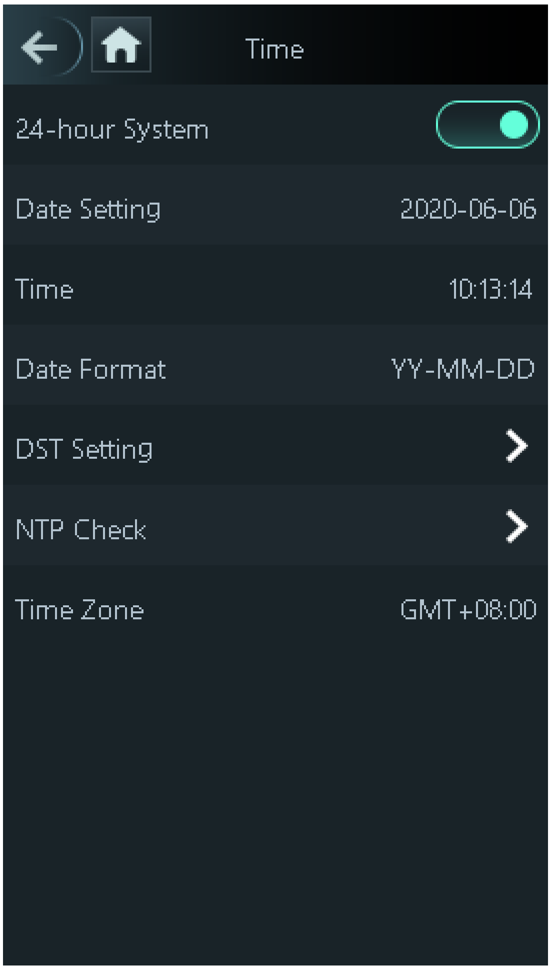
2.11.1 Time

You can do date format setting, date setting, time setting, DST setting, NTP check, and time zone settings.

Step 1 Log in to the **Main Menu** interface.

Step 2 Select **System > Time**, and then configure time parameters.

Figure 2-16 Time



Time

24-hour System

Date Setting 2020-06-06

Time 10:13:14

Date Format YY-MM-DD

DST Setting

NTP Check

Time Zone GMT+08:00

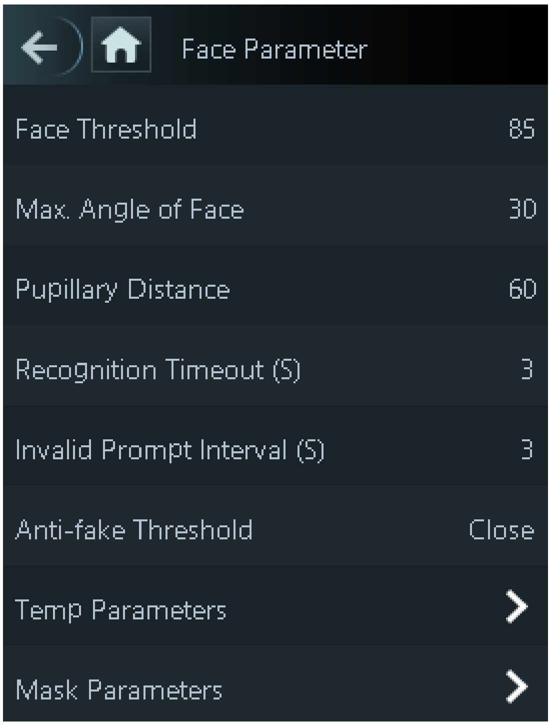
- When you select **Network Time Protocol** (NTP), you need to enable the NTP Check function first. Server IP Address: enter the IP address of the time server, time of the access controller will be synchronized with the time server.
- Port: Enter the port number of the time server.
- Interval (min):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

2.11.2 Face Parameter

Step 1 Log in to the **Main Menu** interface.

Step 2 Select **System > Face Parameter**.

Figure 2-17 Face parameter



Face Parameter

Face Threshold	85
Max. Angle of Face	30
Pupillary Distance	60
Recognition Timeout (S)	3
Invalid Prompt Interval (S)	3
Anti-fake Threshold	Close
Temp Parameters	>
Mask Parameters	>

Step 3 Tap a parameter and do configuration, and then tap ✓.

Table 2-8 Face parameters

Parameter	Description
Face Threshold	Face recognition accuracy can be adjusted. The larger the value is, the higher the accuracy will be.
Max. Angle of Face	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	The interval of the prompt during valid face recognition.
Invalid Face Prompt Interval (S)	For a face has no access permission, 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 face images or models.
Temp Parameters	● **Temperature Monitoring**: Enable or disable this function. ● **Temp Rect**: Set whether to display the temperature monitoring box or not. ● **Temp Monitoring Distance** (cm): 50 by default. You must monitor your temperature standing away from the access controller at the distance you define. Only certain models support this parameter. ● **Temp Correction Duration (ms)**: When monitoring the temperature,

Parameter	Description
	the access controller will take the temperature value after the time defined by this parameter. 📖 Only certain models support this parameter. ● **High Temp Threshold**: Set the temperature threshold. The monitored body temperature will be judged as high temperature if it is greater than or equal to the set value. 📖 Only certain models support this parameter. ● **Max/Min temperature**: Set the temperature range you need. If the monitored temperature is lower than the lower limit, it will prompt that the temperature is too low; if higher than the upper limit, it will prompt that there is a heat source interfering with the function. ● **Temp Correction Value**: This parameter is for testing. The difference of the temperature monitoring environment might cause the temperature deviation between the monitored temperature and the actual temperature. You can select multiple monitored samples for testing, and then correct the temperature deviation by this parameter according to the comparison between the monitored temperature and the actual temperature. For example, if the monitored temperature is 0.5℃ lower than the actual temperature, the correction value is set to 0.5℃; if the monitored temperature is 0.5℃ higher than the actual temperature, the correction value is set to -0.5℃. ● **Temp Monitoring Mode**: 📖 Only certain models support this parameter. ◇ Auto: Uses a face heat map for face recognition; if heat maps are not found, it will automatically change to calibration mode. ◇ Thermogram: Uses only a heat map for face recognition and temperature monitoring. ◇ Calibration: Uses a white light image of a face for face recognition, and then extract and apply the coordinates on the face heat map for temperature monitoring. ● **Temp Unit**: Select ° C or ° F. ● **Evn Compensation Value**: This value will be added to the monitored environment temperature. 📖 Only certain models support this parameter. ● **Temperature Strategy**: 📖 Only certain models support this parameter. ◇ **Maximum**: Take the highest temperature as the result. ◇ **Average**: Take the average temperature as the result. 📖

Parameter	Description
	Only the access controller with a temperature monitoring unit supports this parameter.
Mask Parameters	● **No detect**: Mask is not detected during face recognition. ● **Mask reminder**: Mask is detected during face recognition. If the person is detected without wearing a mask, the system will prompt mask reminder and passage is allowed. ● **Mask intercept**: Mask is detected during face recognition. If the person is detected without wearing a mask, the system will prompt mask reminder and passage is not allowed. ● **Mask Recognition Threshold**: When a mask is detected, this value will be applied to face recognition. The higher the value, the higher the precision requirements, and harder to recognize a person wearing a mask.

2.11.3 Image Mode

There are three options:

- Indoor: Select **Indoor** when the access controller is installed indoors;
- Outdoor: Select **Outdoor** when the access controller is installed outdoors;
- Other: Select **Other** when the access controller is installed at places with backlights like corridors and hallways.

2.11.4 Volume

Tap − or + to adjust the volume.

2.11.5 Language

The following languages are available: English, Italian, Spanish, Japanese, Russian, Turkish, Polish, Korean, Arabic, Spanish (Latin America), and Thai.

2.11.6 Infrared Light

Tap − or + to adjust the infrared light brightness.

The larger the value is, the brighter the infrared light will be.

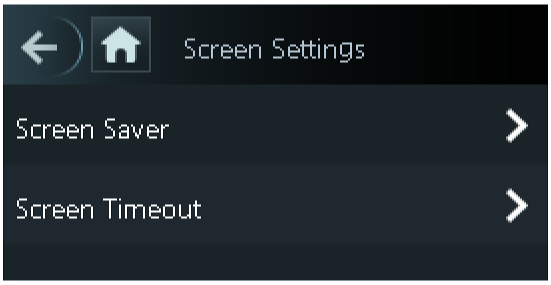
2.11.7 Screen Settings

You can set the screen saver time and screen off time.

Step 1 Log in to the **Main Menu** interface.

Step 2 Select **System > Screen Settings**.

Figure 2-18 Screen settings



Screen Settings

Screen Saver

Screen Timeout

2.11.8 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 whether to retained user information and logs.

- You can select to restore the access controller to the factory settings with all user information and device information deleted.
- You can select to restore the access controller to the factory settings with user information and device information retained.

2.11.9 Reboot

Step 1 Log in to the **Main Menu** interface.

Step 2 Select **System > Reboot**, and the access controller will be rebooted.

2.12 USB

⚠

- Make sure that the USB is inserted to the access controller before exporting user information and updating.
- During exporting or updating, do not pull out the USB or operate the access controller; otherwise the exporting or updating will fail.
- Export information from one access controller to the USB, and then import it to another access controller. Different models support different types of information, such as faces and fingerprints.
- USB can also be used to update the program.

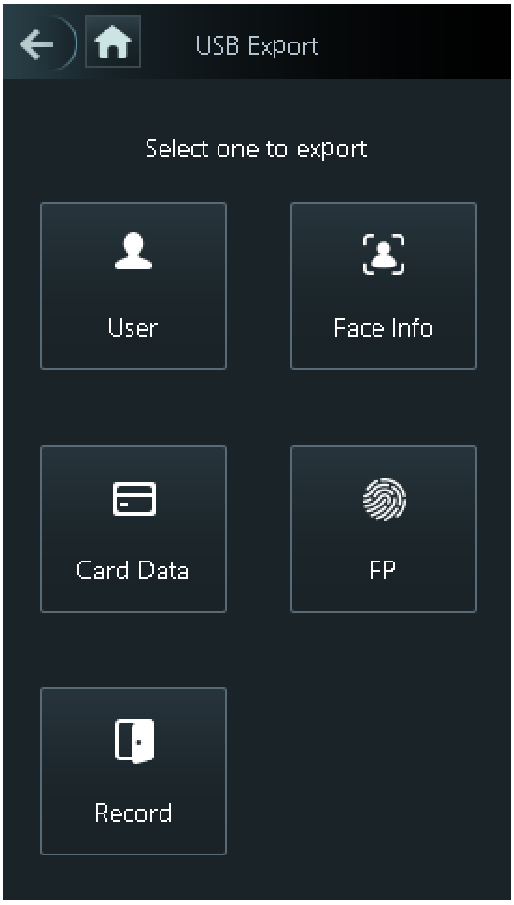
2.12.1 USB Export

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 Log in to the **Main Menu** interface.

Step 2 Select **USB** > **USB Export**.

Figure 2-19 USB export



Step 3 Select the data type that you want to export.

Only certain models support fingerprint.

Step 4 Tap **OK**.

The data will be saved in the USB.

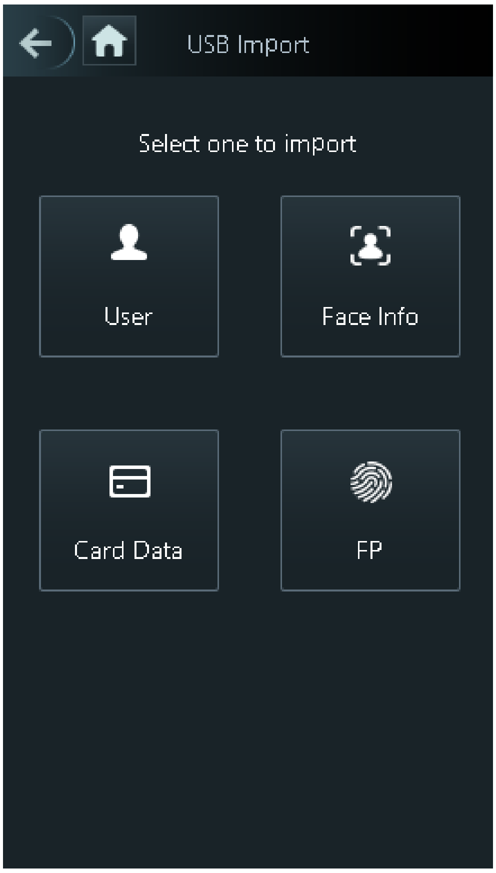
2.12.2 USB Import

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

Step 1 Log in to the **Main Menu** interface.

Step 2 Select **USB** > **USB Import**.

Figure 2-20 USB Import



Step 3 Select the data type that you want to import.

Step 4 Tap **OK**.

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

2.12.3 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 Log in to the **Main Menu** interface.

Step 3 Select **USB** > **USB Update**.

Step 4 Tap **OK**.

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

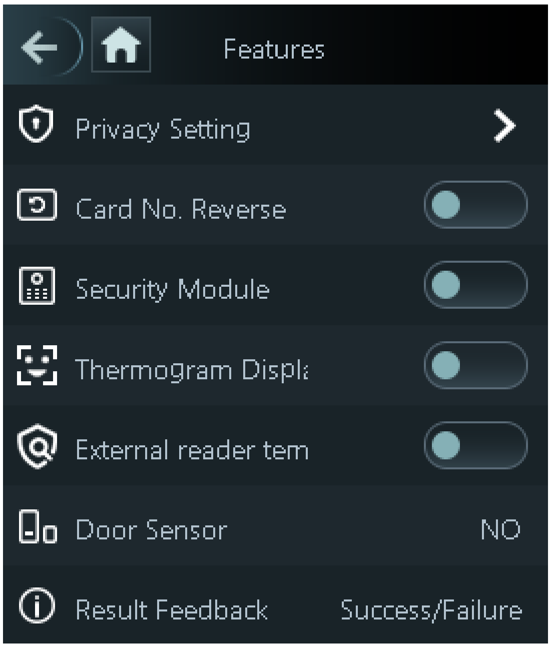
2.13 Features

You can do settings about privacies, card number reverse, security module, door sensor type, and result feedback.

Step 1 Log in to the **Main Menu** interface.

Step 2 Tap **Features**.

Figure 2-21 Features



Features

Privacy Setting >

Card No. Reverse

Security Module

Thermogram Displ

External reader tem

Door Sensor NO

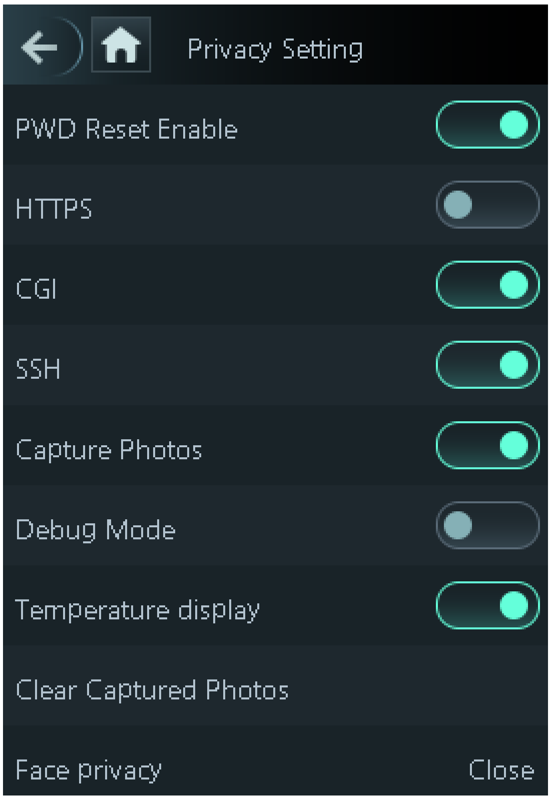
Result Feedback Success/Failure

Table 2-9 Feature description

Parameter	**Description**
Privacy Setting	See "2.13.1 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 number reverse function; otherwise the communication between the access controller and the third party card reader might fail due to protocol discrepancy.
Security Module	● 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.
Thermogram Display	Display a heat map at the upper-left corner. Only certain models support this function.
External Reader Temp Monitoring	Turn it on and the card reader will also monitor the temperature of a person.
Door Sensor	**NO** for normally open or **NC** for normally closed.
Result Feedback	Select a result feedback mode during unlock. See "2.13.2 Result Feedback".

2.13.1 Privacy Setting

Figure 2-22 Privacy setting



Privacy Setting

PWD Reset Enable ●

HTTPS ○

CGI ●

SSH ●

Capture Photos ●

Debug Mode ○

Temperature display ●

Clear Captured Photos

Face privacy Close

Table 2-10 Privacy setting

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 similarly to console applications running on a server that dynamically generates web pages. When CGI is enabled, CGI commands can be used. The CGI is enabled by default.
SSH	Secure Shell (SSH) is a cryptographic network protocol for operating network services securely over an unsecured network. When SSH is enabled, SSH provides cryptographic service for the data transmission.
Capture Photos	If you select ON, when a user unlocks the door, the user's photo will be automatically taken. This function is ON by default.

Parameter	Description
Debug Mode	Enable this mode to display the temperature of the blackbody on the standby interface. You can correct the temperature of the blackbody accordingly. 📖 ● Only certain models support this function. ● When this mode is enabled, the door cannot be opened by any method.
Temperature Display	If enabled, temperature will be displayed in unlock results.
Clear Captured Photos	Delete all captured photos.
Face Privacy	If enabled, the standby interface will be covered in mosaic.

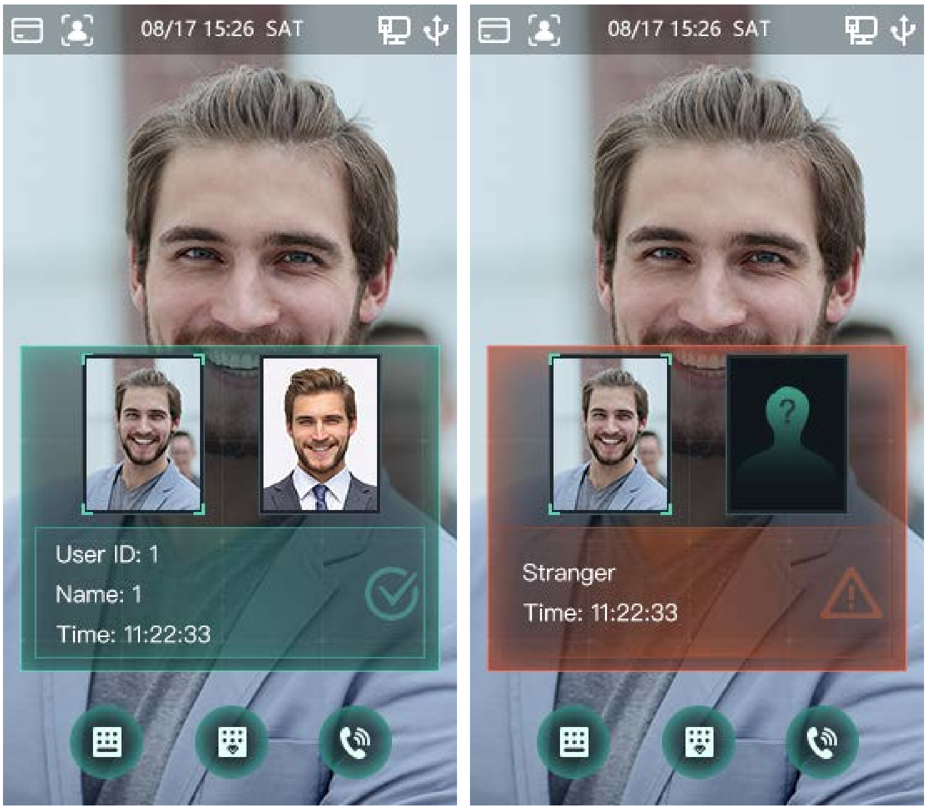
2.13.2 Result Feedback

There are 4 result feedback modes: Success/Failure, Only Name, Photo&Name, and Photos&Name. You can select a result feedback mode as needed.

Photos&Name Mode

The captured face image, the image saved in the face database, user ID, user name and time are all displayed during unlock.

Figure 2-23 Photos and name mode (1)



08/17 15:26 SAT

User ID: 1

Name: 1

Time: 11:22:33

08/17 15:26 SAT

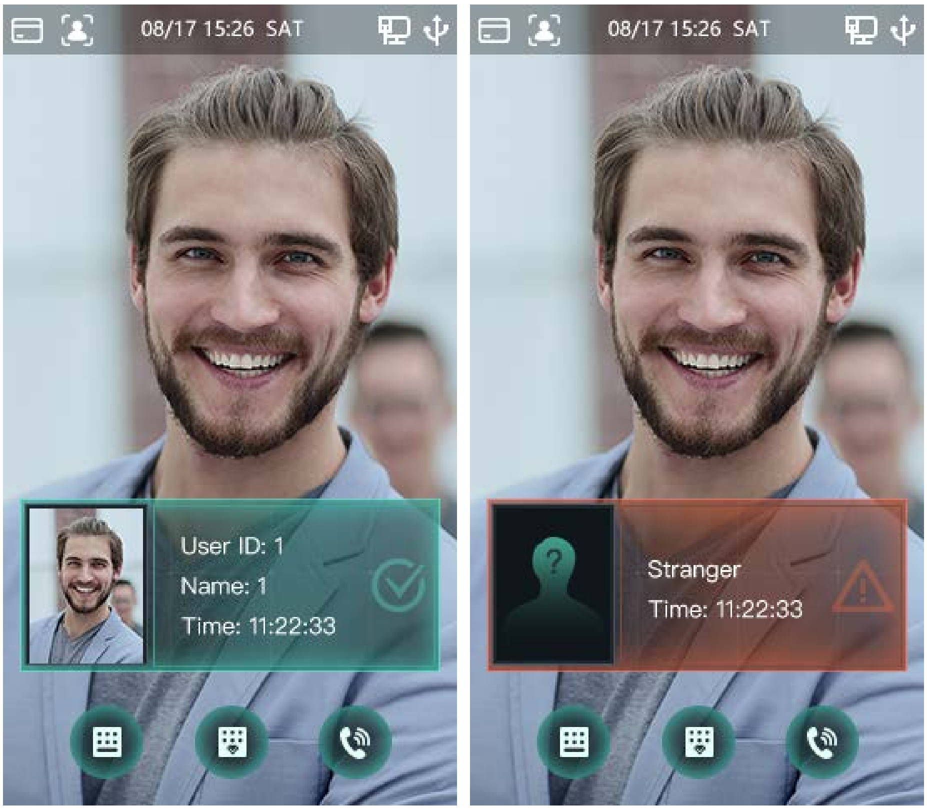
Stranger

Time: 11:22:33

Photo&Name Mode

The image saved in the face database, user ID, user name and time are all displayed during unlock.

Figure 2-24 Photo and name mode (2)



User ID: 1

Name: 1

Time: 11:22:33

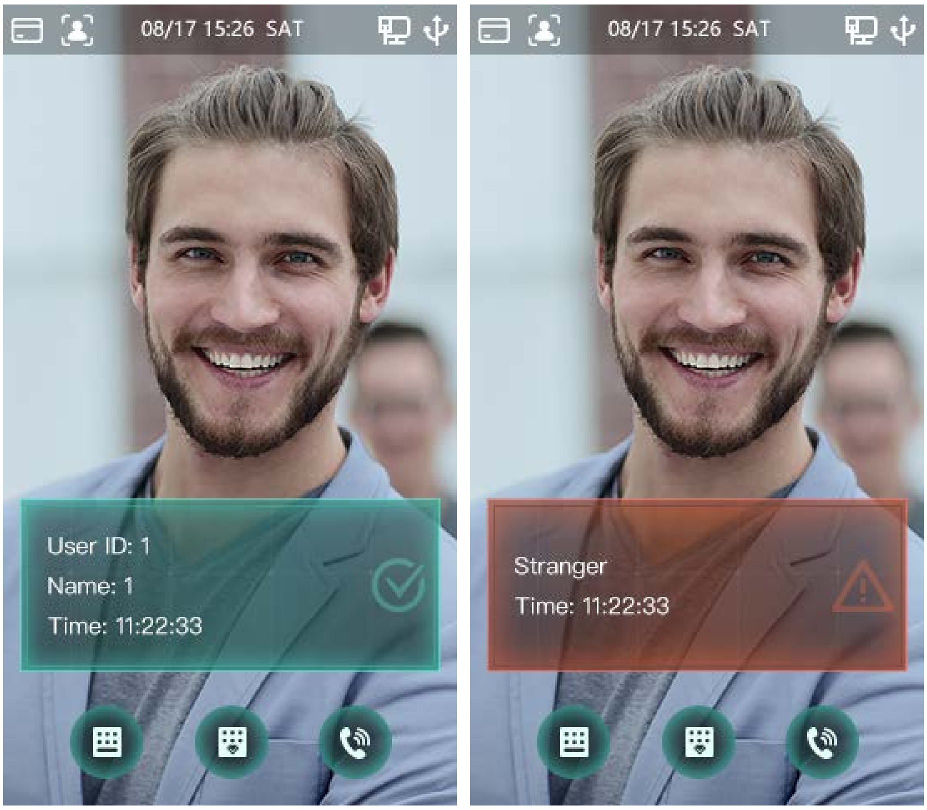
Stranger

Time: 11:22:33

Only Name Mode

Only user ID, user name and time are displayed during unlock.

Figure 2-25 Only name mode



User ID: 1

Name: 1

Time: 11:22:33

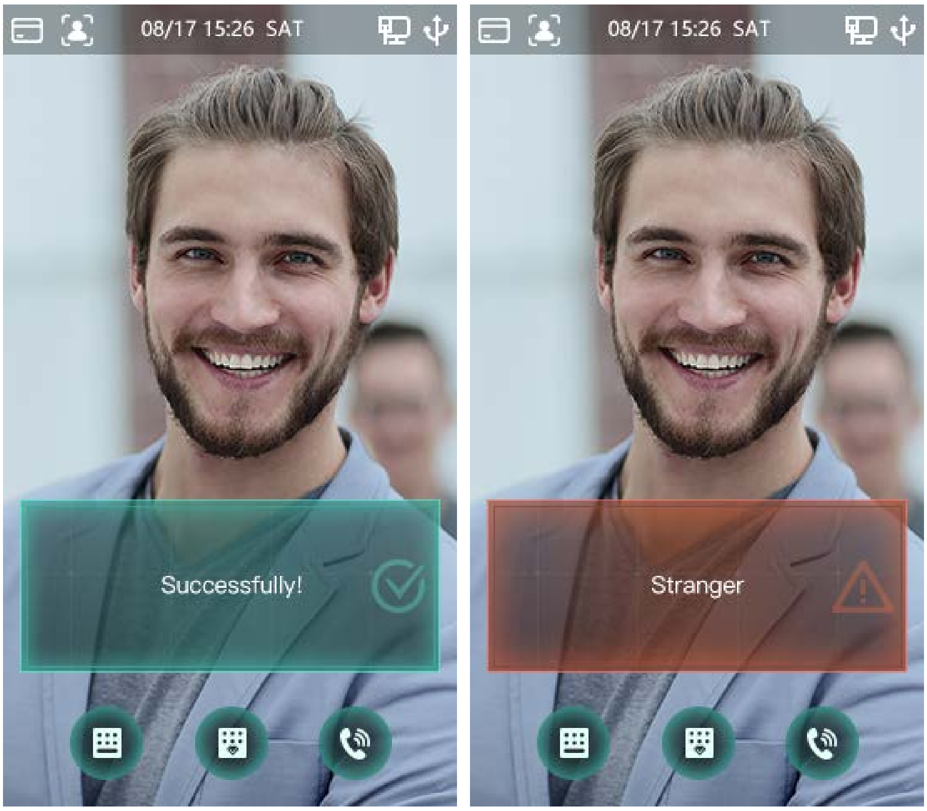
Stranger

Time: 11:22:33

Success/Failure Mode

Only display success or failure during unlock.

Figure 2-26 Success/Failure mode



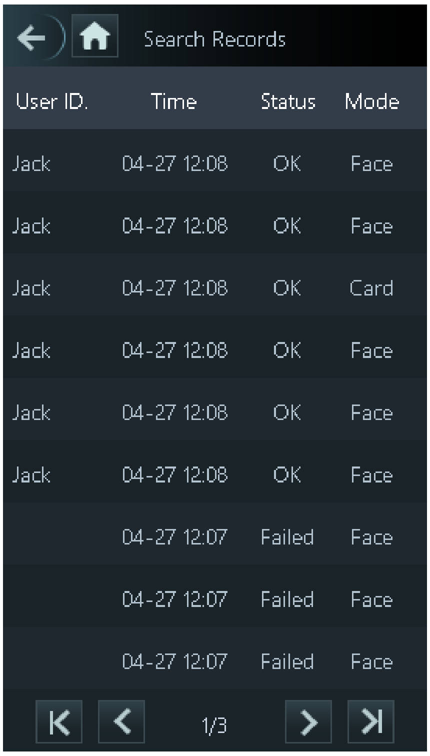
Successfully!

Stranger

2.14 Record

You can query all unlocking records.

Figure 2-27 Search punch records



User ID.	Time	Status	Mode
Jack	04-27 12:08	OK	Face
Jack	04-27 12:08	OK	Face
Jack	04-27 12:08	OK	Card
Jack	04-27 12:08	OK	Face
Jack	04-27 12:08	OK	Face
Jack	04-27 12:08	OK	Face
	04-27 12:07	Failed	Face
	04-27 12:07	Failed	Face
	04-27 12:07	Failed	Face

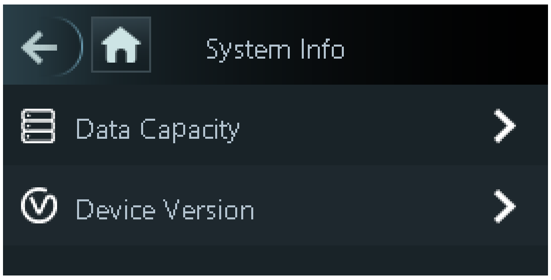
2.15 System Info

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

Step 1 Log in to the **Main Menu** interface.

Step 2 Tap **System Info**.

Figure 2-28 System info



3 Web Operations

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.

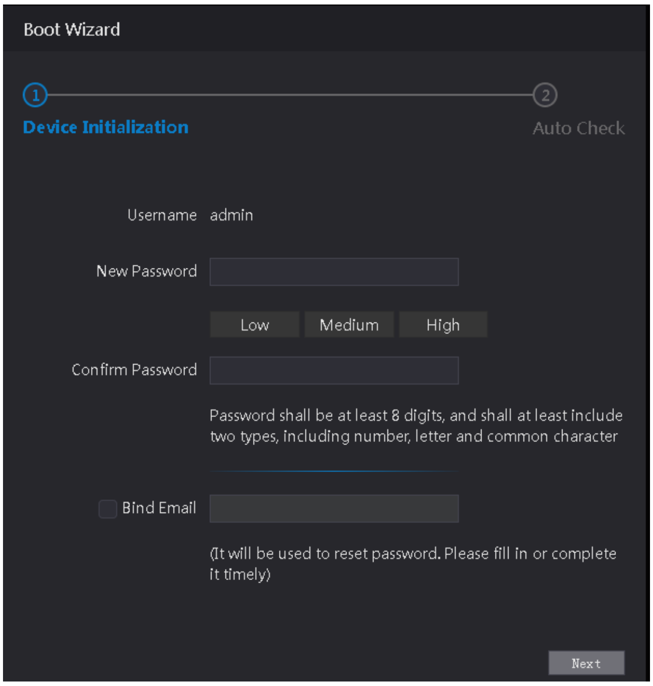
3.1 Initialization

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 Enter.

- Use browser newer than IE 8, 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 access controller.

Figure 3-1 Initialization



Boot Wizard

Username admin

New Password

Confirm Password

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

□ Bind Email

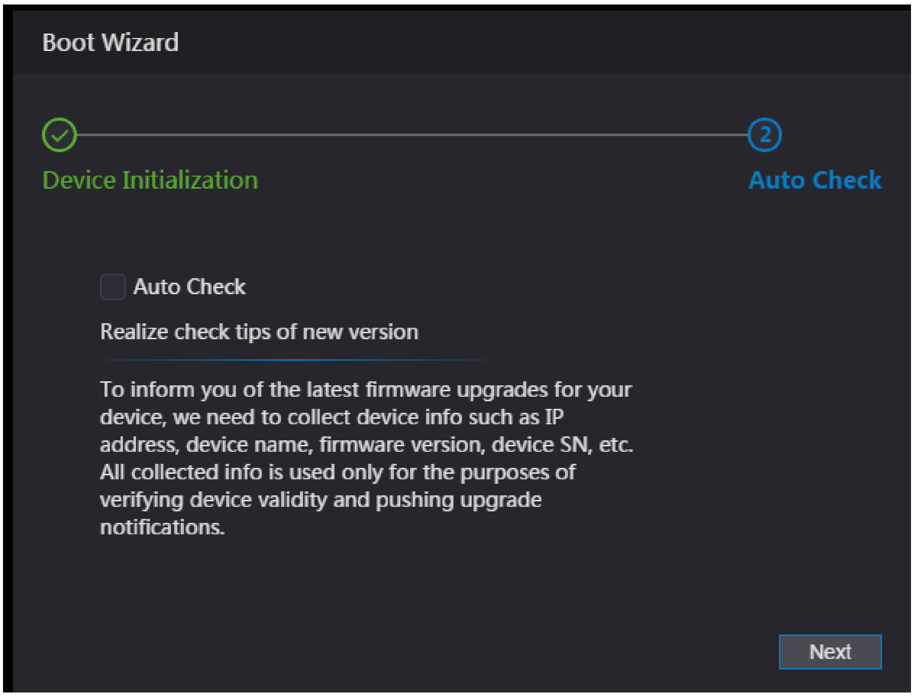
(It will be used to reset password. Please fill in or complete it timely)

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

- The password must consist of 8 to 32 non-blank characters and contain at least two types of characters among upper case, lower case, number, and special character (excluding ' " ; : &). Set a password of high security level according to the password strength prompt.
- For security, keep the password properly after initialization and change the password regularly.
- 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 3-2 Auto check



□ Auto Check

Realize check tips of new version

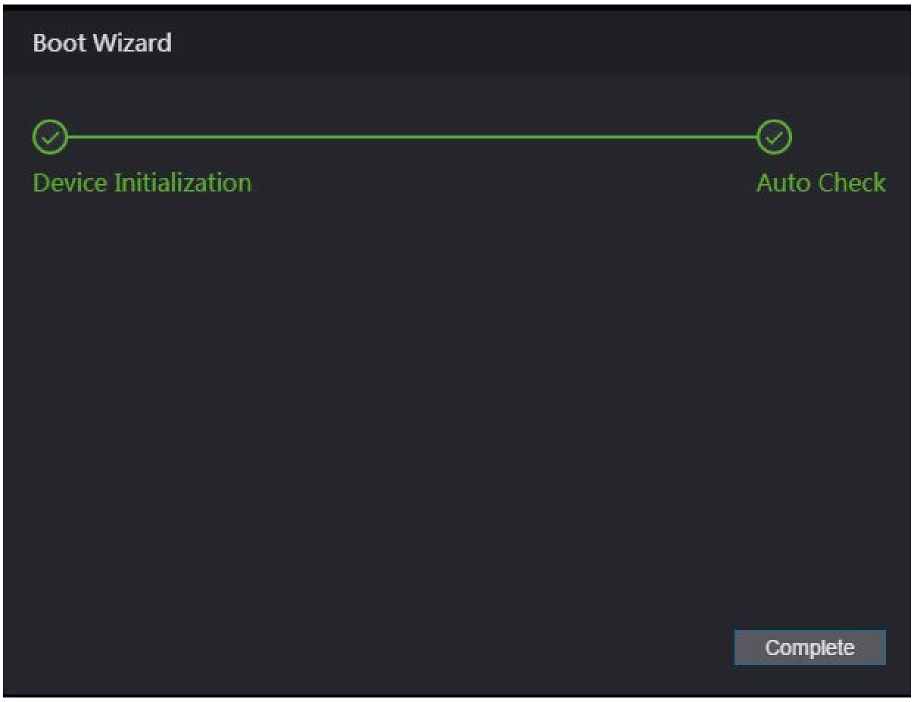
To inform you of the latest firmware upgrades for your device, we need to collect device info such as IP address, device name, firmware version, device SN, etc. All collected info is used only for the purposes of verifying device validity and pushing upgrade notifications.

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

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

Step 5 Click **Next**.

Figure 3-3 Finished configuration



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

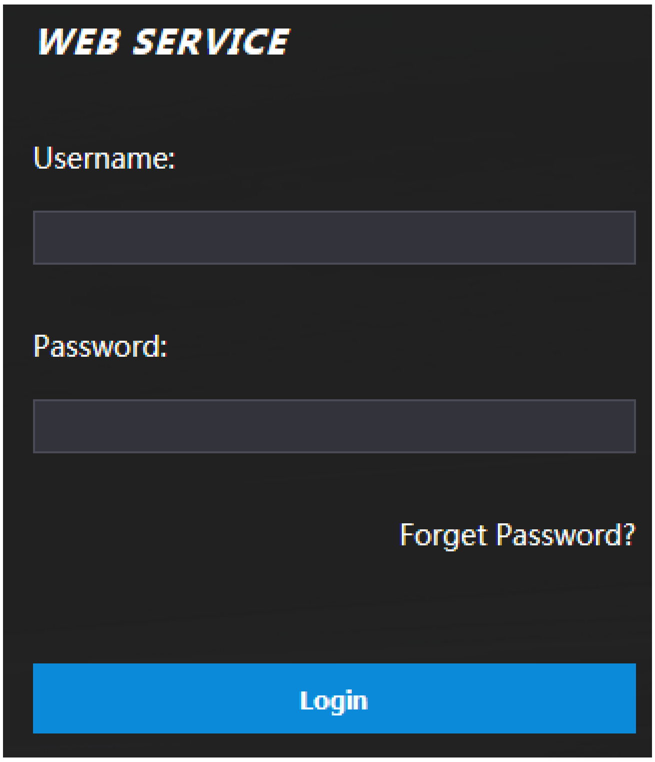
3.2 Login

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

📖

- Use browser newer than IE 8, 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 access controller.
- The default IP address is 192.168.1.108.

Figure 3-4 Login



Step 2 Enter the user name and password.

📖

- The default administrator name is admin, and the password is the login password after initializing the access controller. Change the administrator password regularly and keep it properly.
- If you forget the administrator login password, you can click **Forget Password?** to reset it. See "3.3 Resetting the Password."

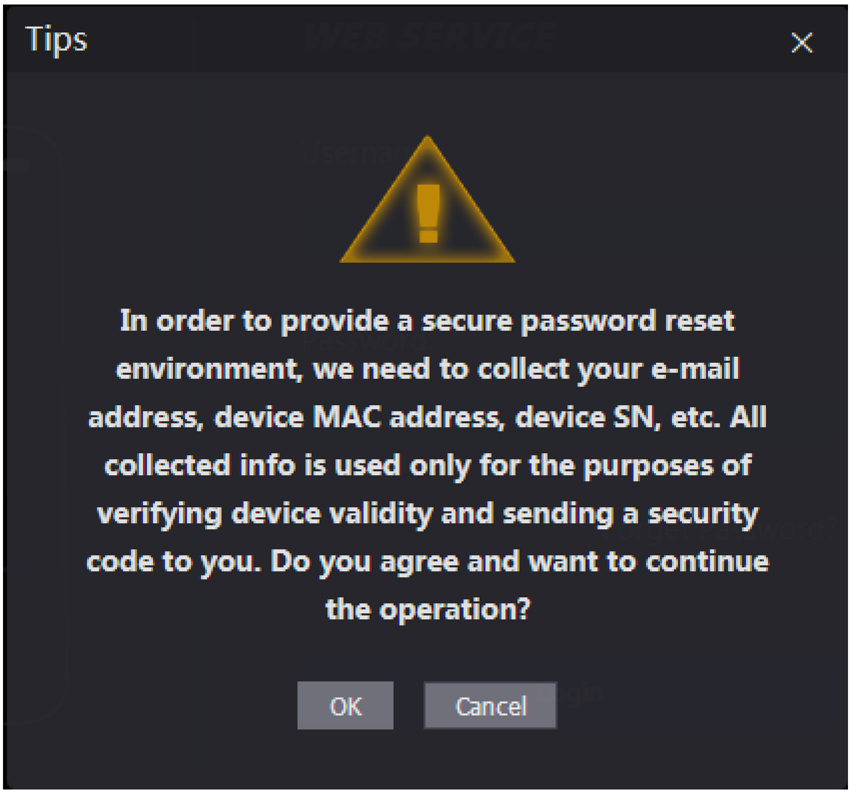
Step 3 Click **Login**.

3.3 Resetting the Password

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

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

Figure 3-5 Tips



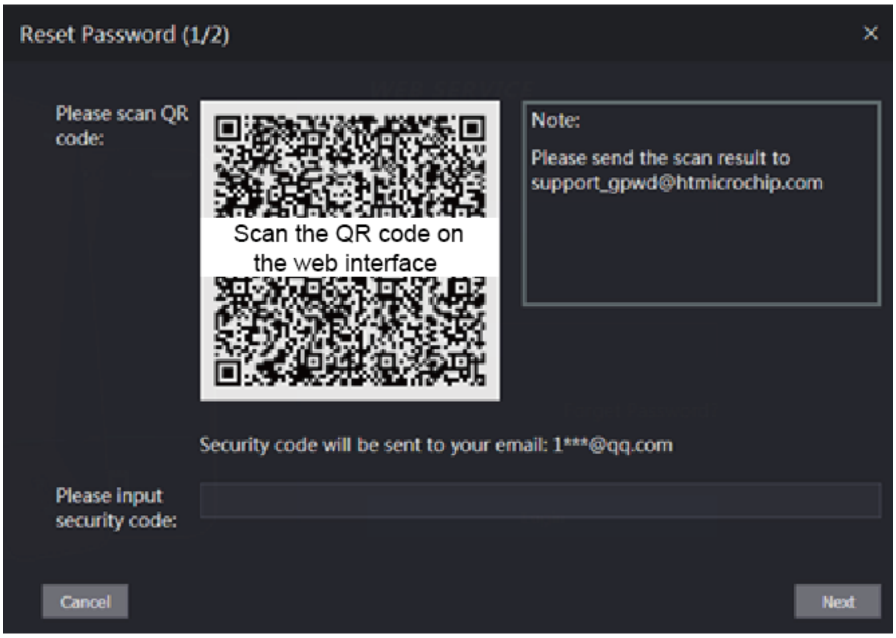
Tips

In order to provide a secure password reset environment, we need to collect your e-mail address, device MAC address, device SN, etc. All collected info is used only for the purposes of verifying device validity and sending a security code to you. Do you agree and want to continue the operation?

Step 2 Read the tips.

Step 3 Click **OK**.

Figure 3-6 Reset Password



Reset Password (1/2)

Please scan QR code:

Note:

Please send the scan result to support_gpwd@htmicrochip.com

Security code will be sent to your email: 1***@qq.com

Please input security code:

Step 4 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 5 Enter the security code you have received.

Step 6 Click **Next**.

Step 7 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 8 Click **OK**, and the reset is completed.

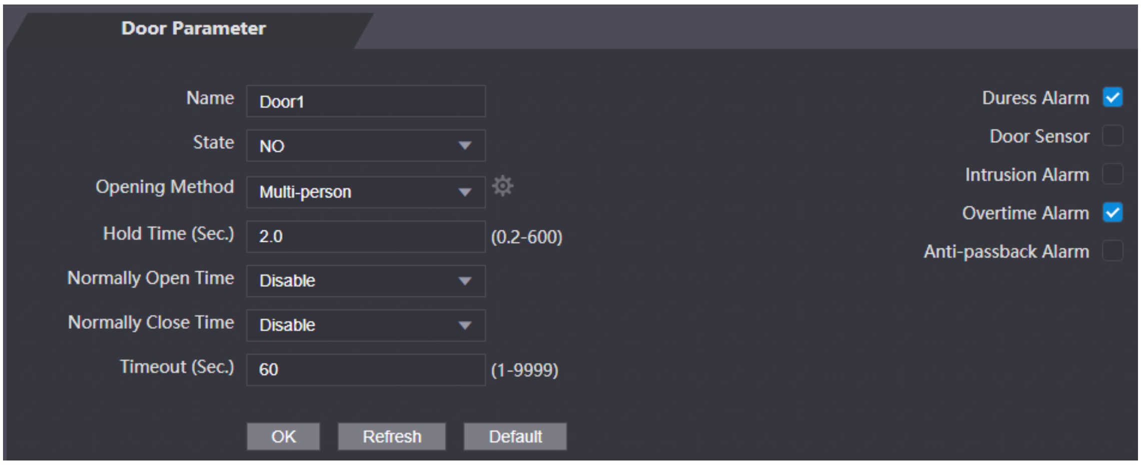
3.4 Door Parameter

Configure the access control parameters.

Step 1 Log in to the web interface.

Step 2 Select **Door Parameter**.

Figure 3-7 Door parameters



Door Parameter

Name: Door1

State: NO

Opening Method: Multi-person ⚙

Hold Time (Sec.): 2.0 (0.2-600)

Normally Open Time: Disable

Normally Close Time: Disable

Timeout (Sec.): 60 (1-9999)

Duress Alarm ☑

Door Sensor □

Intrusion Alarm □

Overtime Alarm ☑

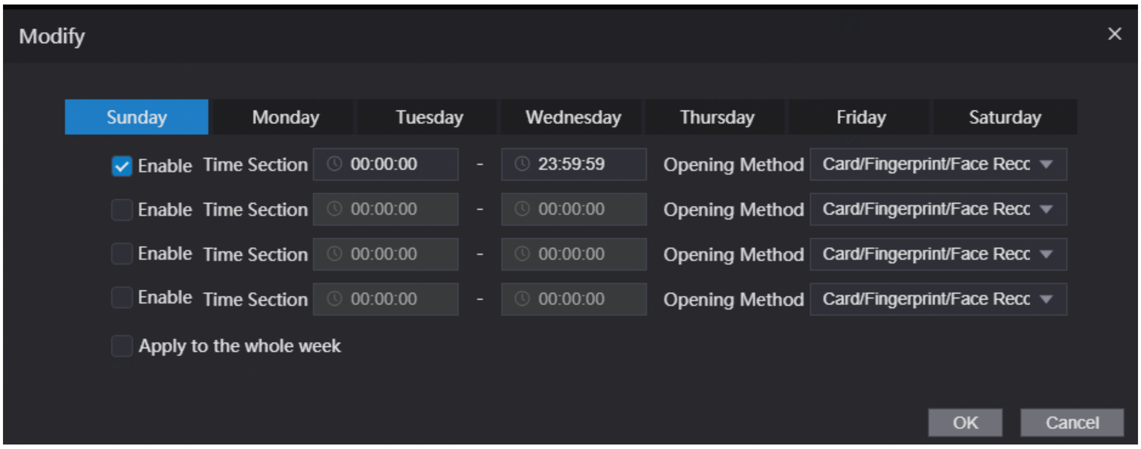
Anti-passback Alarm □

Step 3 Configure **Opening Method**.

- Time section

1) Click ⚙.

Figure 3-8 Time section parameter



Modify

Sunday | Monday | Tuesday | Wednesday | Thursday | Friday | Saturday

☑ Enable Time Section 00:00:00 - 23:59:59 Opening Method Card/Fingerprint/Face Recc

□ Enable Time Section 00:00:00 - 00:00:00 Opening Method Card/Fingerprint/Face Recc

□ Enable Time Section 00:00:00 - 00:00:00 Opening Method Card/Fingerprint/Face Recc

□ Enable Time Section 00:00:00 - 00:00:00 Opening Method Card/Fingerprint/Face Recc

□ Apply to the whole week

2) Configure the time and opening method for a time section. You can configure up to four time sections for each day.

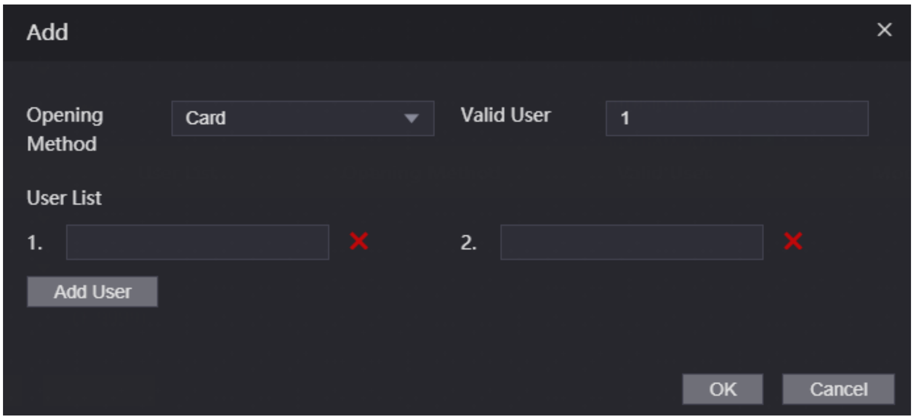
3) (Optional) Select **Apply to the whole week** to copy the configuration to other days.

4) Click **OK**

- Multi-person

1) Click ⚙, and then click **Add**.

Figure 3-9 Multi-person parameter



Add

Opening Method: Card

Valid User: 1

User List

1.

2.

2) Select an opening method, and enter a number for valid user.

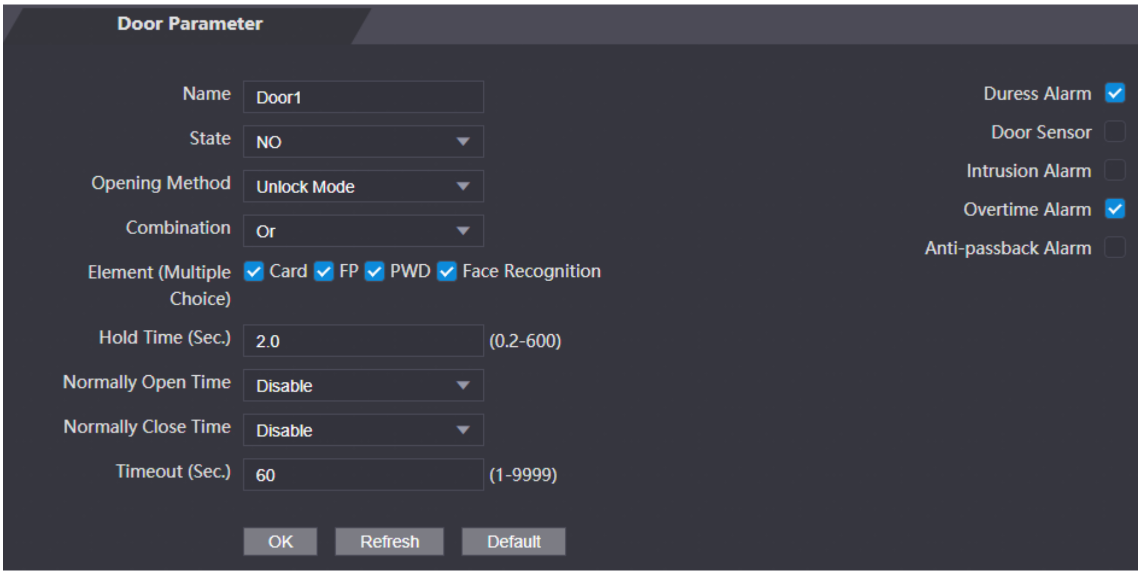
3) In the **User List** section, enter the ID of the users as needed. For user ID, see "2.7 User Management".

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

- Unlock mode

1) Select the unlock method(s) in **Element (Multiple Choice)**.

Figure 3-10 Unlock mode parameters



Door Parameter

Name: Door1

State: NO

Opening Method: Unlock Mode

Combination: Or

Element (Multiple Choice): ☑ Card ☑ FP ☑ PWD ☑ Face Recognition

Hold Time (Sec.): 2.0 (0.2-600)

Normally Open Time: Disable

Normally Close Time: Disable

Timeout (Sec.): 60 (1-9999)

Duress Alarm ☑

Door Sensor □

Intrusion Alarm □

Overtime Alarm ☑

Anti-passback Alarm □

2) Select **Or** or **And**. **Or** means you must use all the defined methods to open the door; **And** means you can open the door with any of the defined methods.

3) Select the unlock methods for **Element (Multiple Choice)**.

Step 4 Configure other parameters.

Table 3-1 Parameter description

Parameter	Description
Name	Enter a name for the door that this access controller controls.
State	Select **NC** for normally closed, or **NO** for normally open. If either is selected, the defined opening method will not be effective.
Opening Method	See Step 3 above.
Hold Time (Sec.)	Unlock duration. If expired, the door will be locked.
Normally Open Time	The door will be always open or closed.
Normally Close Time	
Timeout (Sec.)	A timeout alarm will be triggered if the door stays unlock for longer than this value.
Duress Alarm	See Table 2-4.
Door Sensor	
Intrusion Alarm	
Overtime Alarm	
Anti-passback Alarm	

Step 5 Click **OK**.

3.5 Alarm Linkage

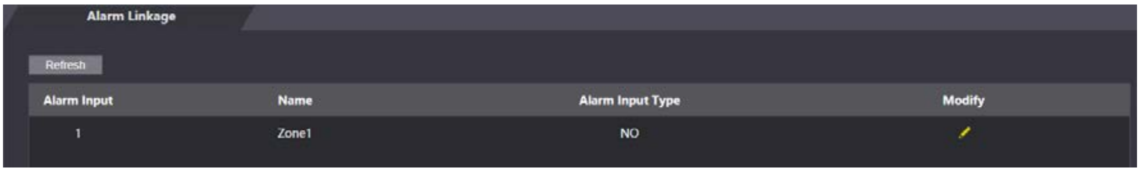
3.5.1 Setting Alarm Linkage

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

Step 1 Log in to the web interface.

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

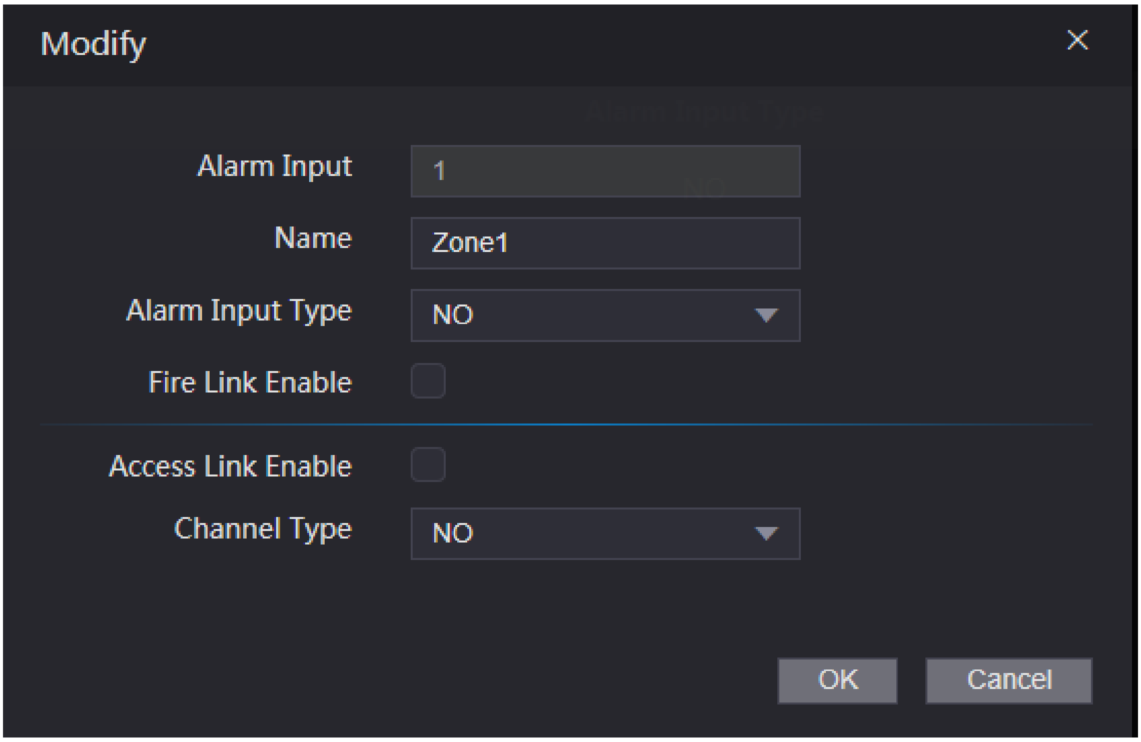
Figure 3-11 Alarm linkage



Alarm Input	Name	Alarm Input Type	Modify
1	Zone1	NO	✎

Step 3 Click ✎ to modify the alarm linkage parameters.

Figure 3-12 Change alarm linkage parameters


Modify

Alarm Input: 1

Name: Zone1

Alarm Input Type: NO

Fire Link Enable: □

Access Link Enable: □

Channel Type: NO

Table 3-2 Alarm linkage parameter description

Parameter	Description
Alarm Input	You cannot modify the value. Keep it default.
Name	Enter a zone name.
Alarm Input Type	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 intput and access link are NO by default if fire link is enabled.
Access Link Enable	If 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 4 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.

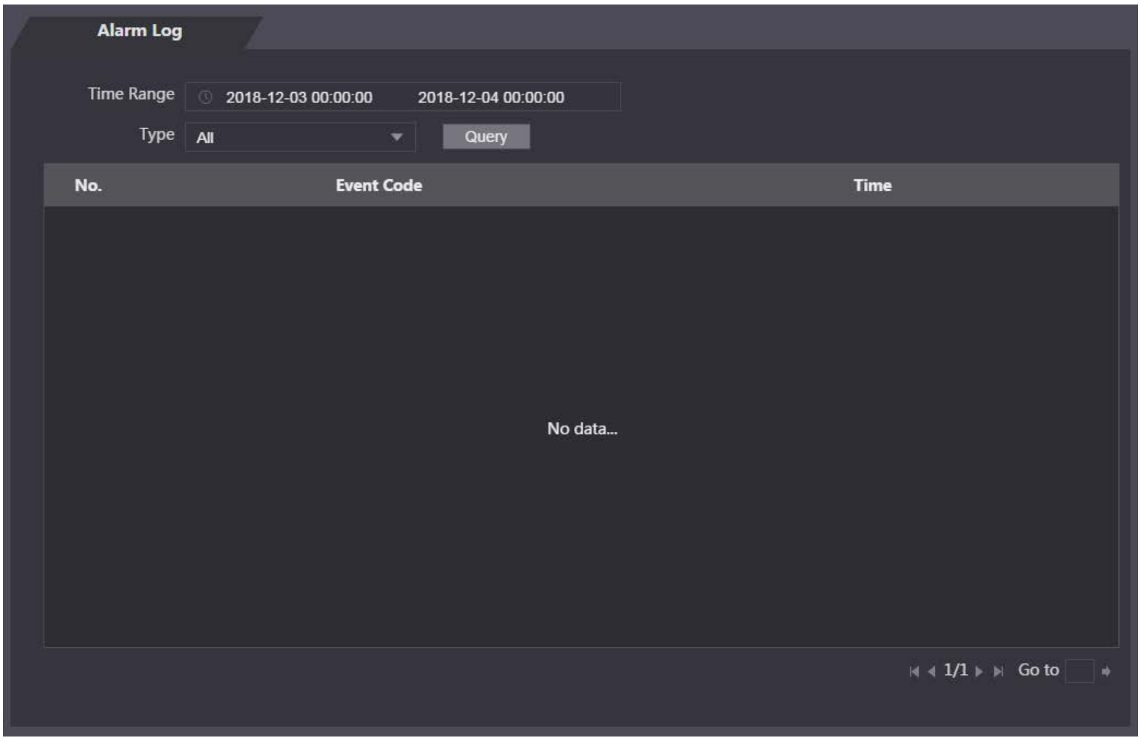
3.5.2 Alarm Log

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

Step 1 Log in to the web interface.

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

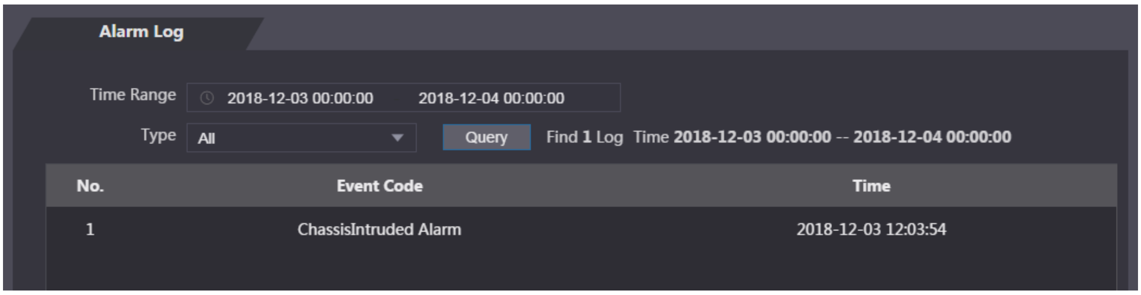
Figure 3-13 Alarm log



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

The query results are displayed.

Figure 3-14 Query results



No.	Event Code	Time
1	ChassisIntruded Alarm	2018-12-03 12:03:54

3.6 Talkback Setting

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

3.6.1 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 (VTH) combined.

3.6.1.1 Access Controller as SIP Server

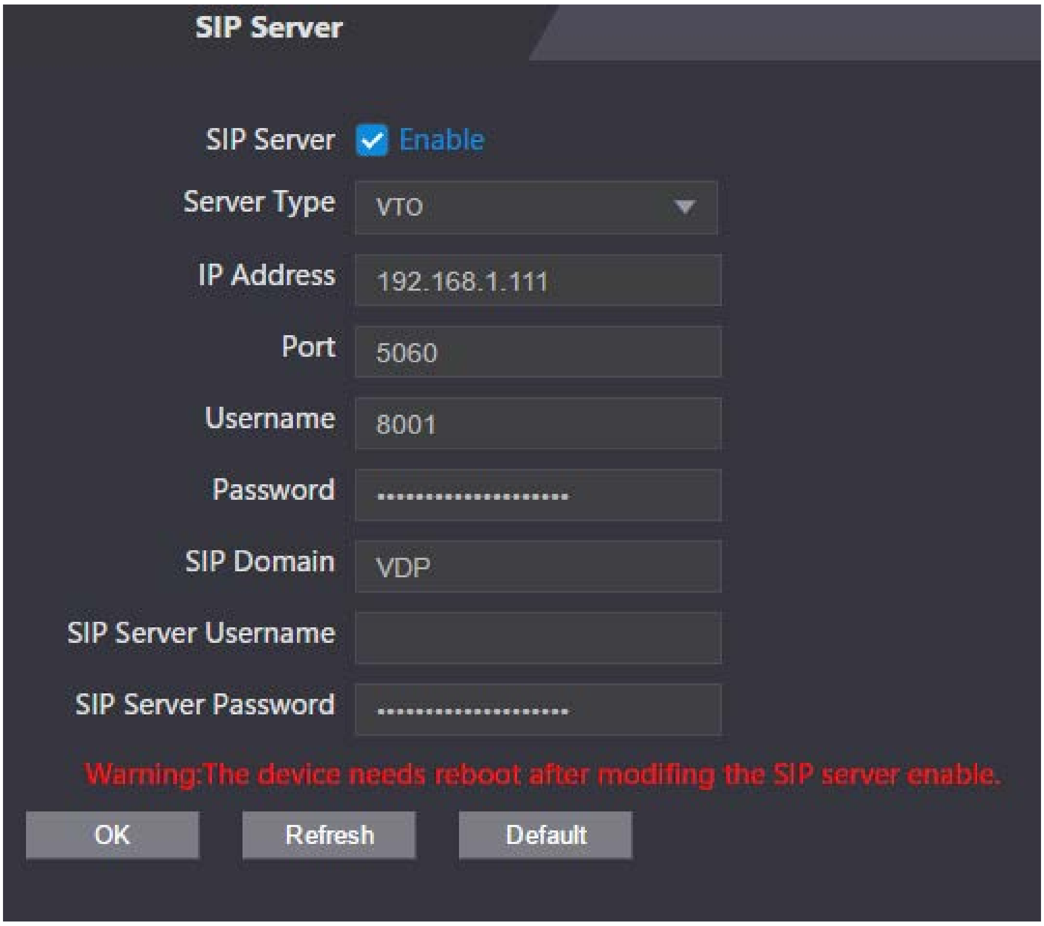
Step 1 Log in to the web interface.

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

Step 3 Enable **SIP Server**, and then click **OK**.

The access controller will restart.

Figure 3-15 SIP server (1)



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 modifing the SIP server enable.

3.6.1.2 Other Device as SIP Server

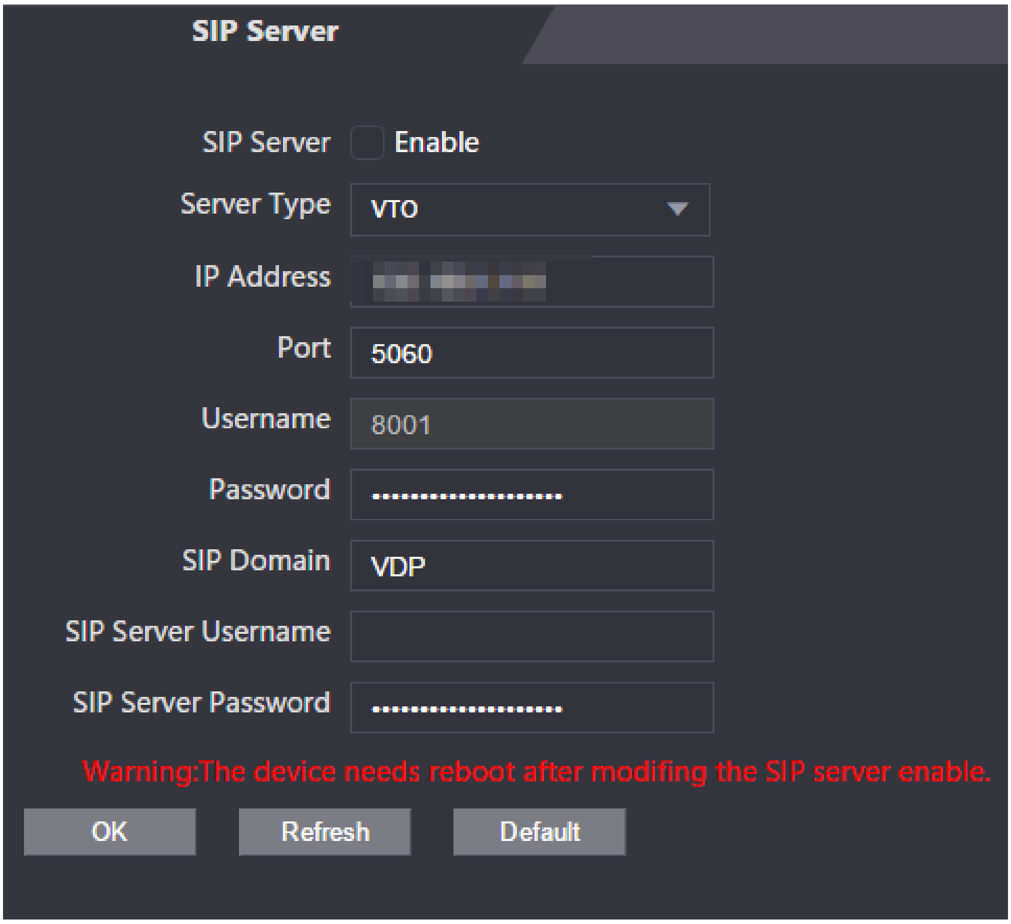
Step 1 Log in to the web interface.

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

Step 3 Disable **SIP Serve**, and then set **Server Type** to **VTO**.

Step 4 Configure the parameters

Figure 3-16 SIP server (2)



SIP Server

SIP Server □ Enable

Server Type: VTO

IP Address: [redacted]

Port: 5060

Username: 8001

Password: ••••••••••••••••••••

SIP Domain: VDP

SIP Server Username:

SIP Server Password: ••••••••••••••••••••

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

Table 3-3 SIP server parameter description (1)

Parameter	Description
IP Address	The IP address of the VTO 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**.

3.6.2 Local Configuration

Set the device type and number.

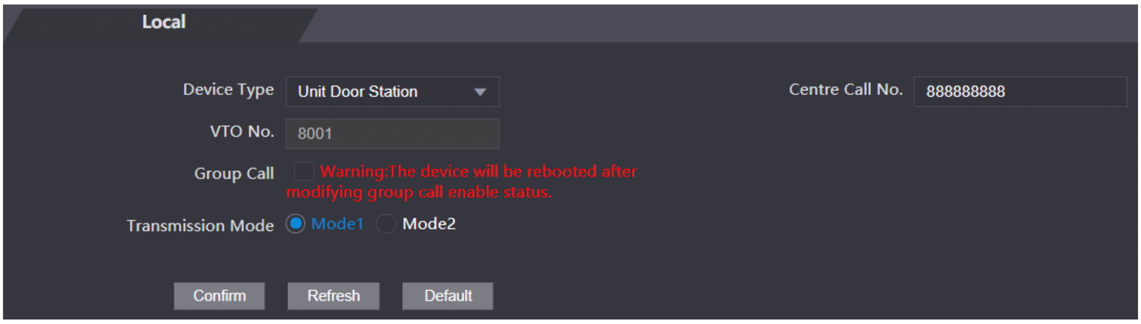
3.6.2.1 Access Controller as SIP Server

Step 1 Log in to the web interface.

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

Step 3 Configure the parameters.

Figure 3-17 Local (1)



Local

Device Type: Unit Door Station

Centre Call No.: 888888888

VTO No.: 8001

Group Call: □ Warning:The device will be rebooted after modifying group call enable status.

Transmission Mode: ● Mode1 ○ Mode2

Table 3-4 Parameter description

Parameter	Description
Device Type	The access controller can only work as a unit VTO.
Centre Call No.	Enter a number for the management center. It can contain up tp nine digits.
VTO No.	Cannot be configured when the access controller is working as the SIP server.
Group Call	When enabled, all sub VTHs will also receive the call when the access controller is calling a main VTH. 📖 This function is only available when the access controller is working as the SIP server.
Transmission Mode	● 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**.

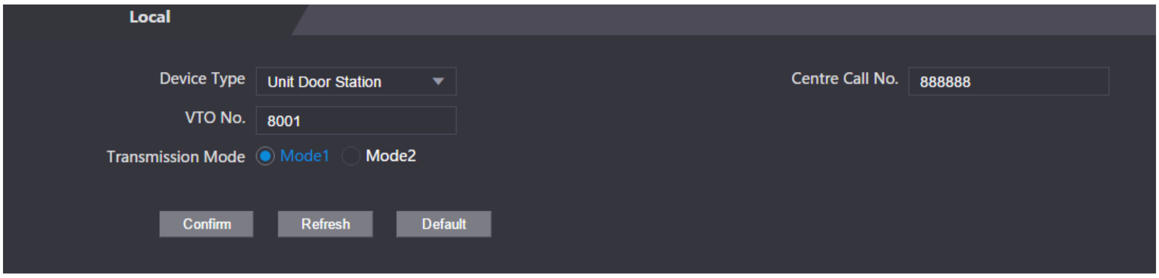
3.6.2.2 Other Device as SIP Server

Step 1 Log in to the web interface.

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

Step 3 Configure the parameters.

Figure 3-18 Local (2)



Local

Device Type: Unit Door Station

Centre Call No.: 888888

VTO No.: 8001

Transmission Mode: ● Mode1 ○ Mode2

Table 3-5 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 for the management center. It can contain up tp nine digits.
VTO No.	Set a number. 📖 ● It should be four digits. The first two should be 80 and the last

Parameter	Description
	two starts with 01, such as 8001. ● If there are multiple VTOs, their VTO numbers cannot be the same.
Transmission Mode	● **Mode1**: Real-time call but the video and sound may lag with poor network. ● **Mode2**: Not real-time call but ensures smooth video and sound.

3.6.3 VTO Number Management

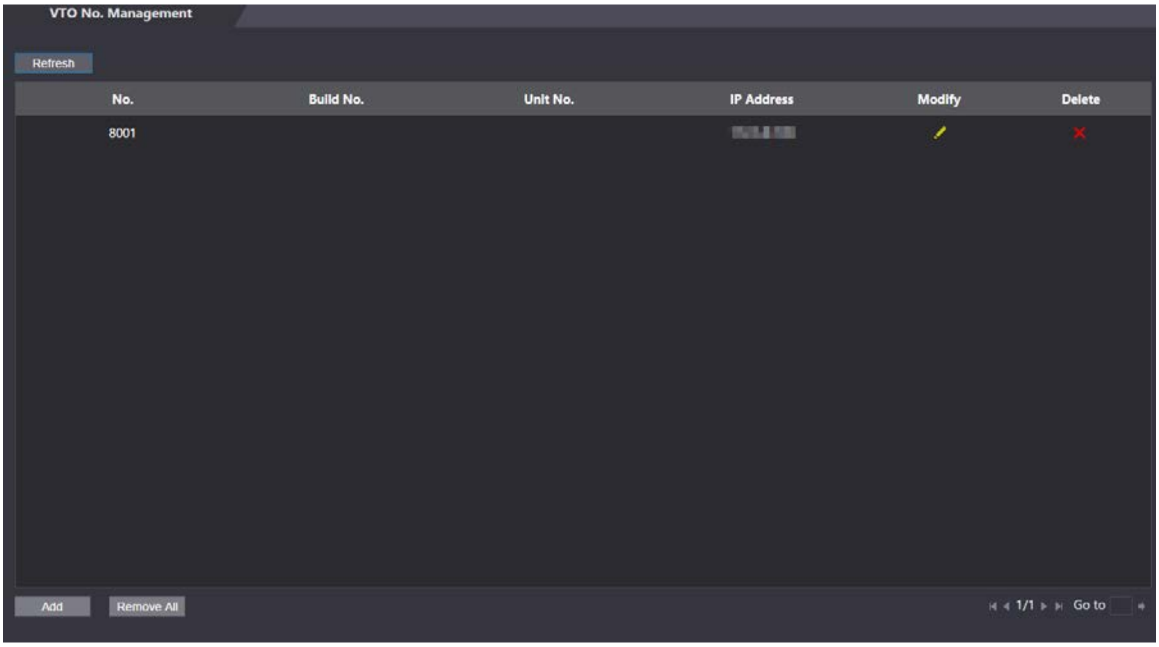
When the access controller works as the SIP server, add other VTOs to call them.

Step 1 Log in to the web interface.

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

Step 3 Click **Add**.

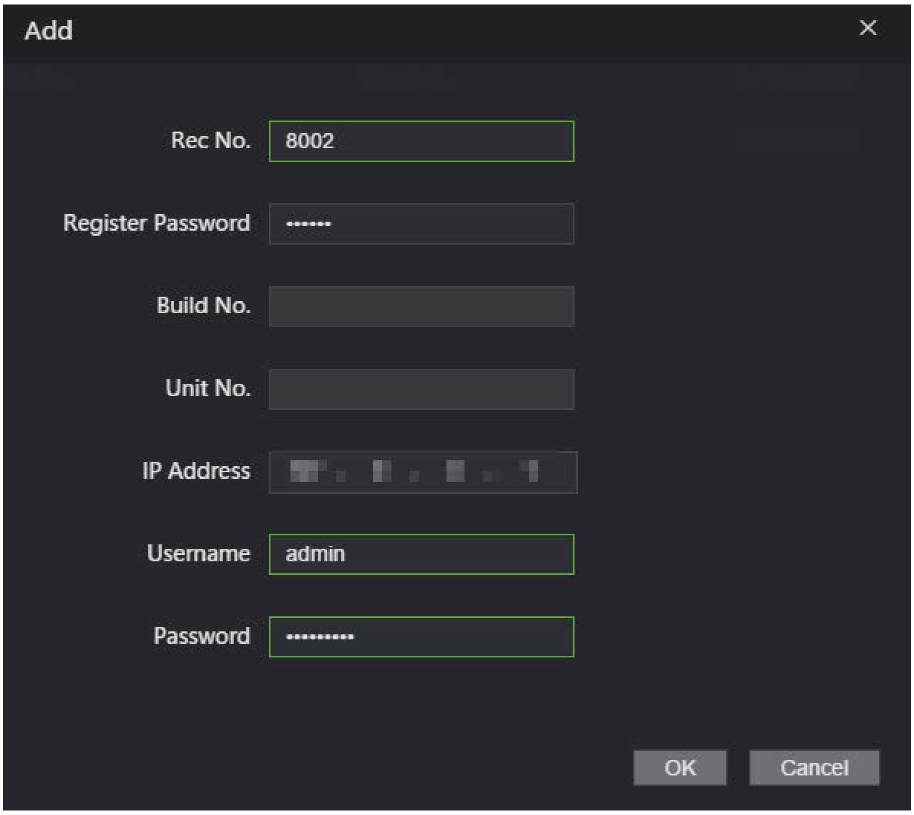
Figure 3-19 VTO No. management



No.	Build No.	Unit No.	IP Address	Modify	Delete
8001			[redacted]	✎	✕

Step 4 Configure the parameters.

Figure 3-20 Add a door station



Add

Rec No. 8002

Register Password ••••••

Build No.

Unit No.

IP Address [redacted]

Username admin

Password •••••••••

Table 3-6 Parameter description

Parameter	Description
Rec No.	Enter a number for the VTO you want to add.
Register Password	Keep it default.
Build No.	Cannot be configured.
Unit No.	
IP Address	IP address of the VTO you want to add.
Username	Web interface login username and password of the VTO you want to add.
Password	

Step 5 Click **OK**.

3.6.4 VTH Number Management

When the access controller works as the SIP server, add VTHs to call them.

When there are main and sub VTHs, you need to enable group call function first before adding them. See "3.6.2.1 Access Controller as SIP Server".

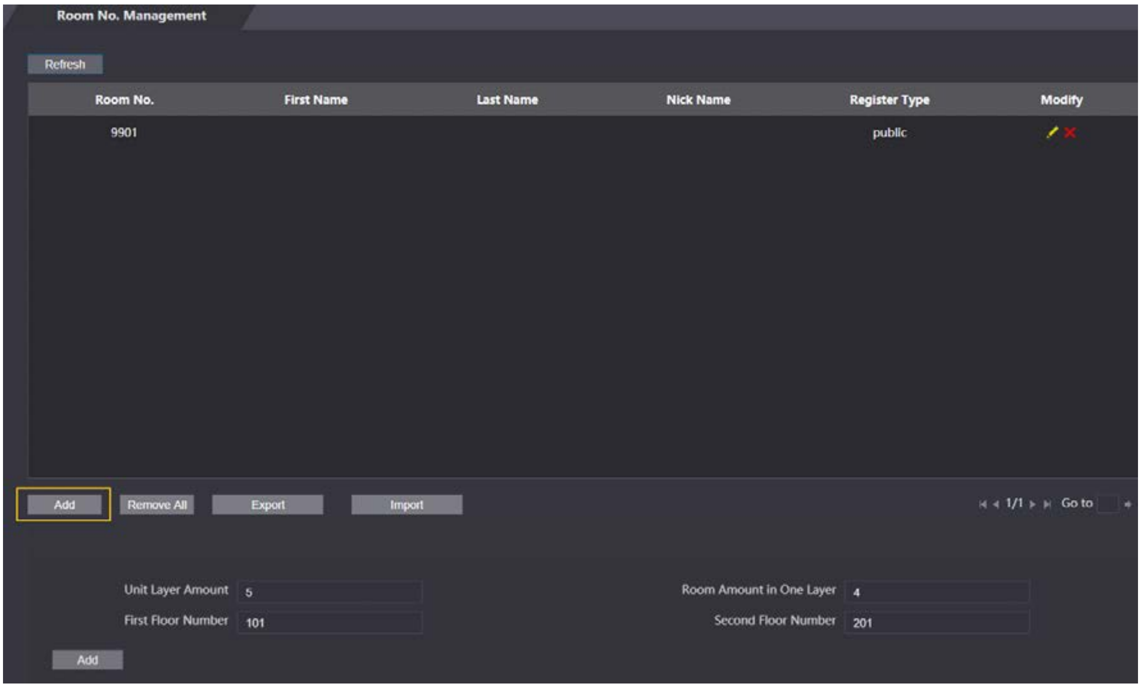
3.6.4.1 Add VTHs One by One

Step 1 Log in to the web interface.

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

Step 3 Click **Add**.

Figure 3-21 Room number management



Room No.	First Name	Last Name	Nick Name	Register Type	Modify
9901				public	

Unit Layer Amount: 5

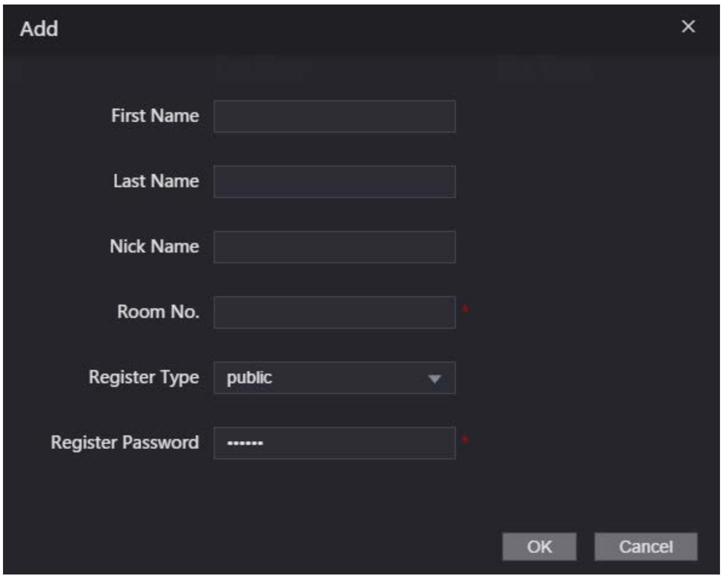
Room Amount in One Layer: 4

First Floor Number: 101

Second Floor Number: 201

Step 4 Enter the information.

Figure 3-22 Add one VTH



First Name:

Last Name:

Nick Name:

Room No.: *

Register Type: public

Register Password: •••••• *

Table 3-7 Parameter description

Parameter	Description
First Name	To differentiate from othe rVTHs.
Last Name	
Nick Name	
Room No.	Room number of the VTH. ● 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 sub VTHs, the room number of main VTH should end with "-0", and that of sub VTHs with "-1", "-2", "-3"…For example, the main VTH is 101-0, sub VTHs are 101-1, 101-2 and 101-3.

Parameter	Description
Register Type	Keep it default.
Register Password	

Step 5 Click **OK**.

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

3.6.4.2 Add VTHs in Batches

You can add up to 1024 VTHs.

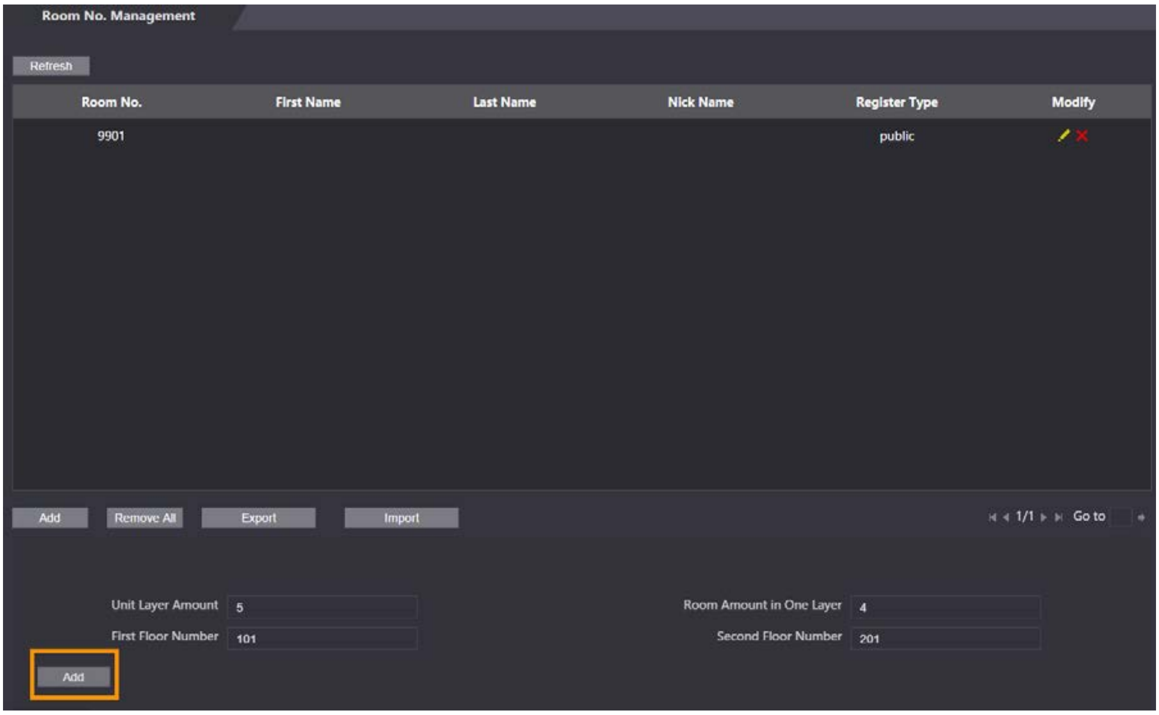
Step 1 Log in to the web interface.

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

Step 3 Configure **Unit Layer Amount**, **Room Amount in One Layer**, **First Floor Number** and **Second Floor Number**.

Step 4 Click **Add**.

Figure 3-23 Add indoor monitors in batches



Room No.	First Name	Last Name	Nick Name	Register Type	Modify
9901				public	

Unit Layer Amount: 5

Room Amount in One Layer: 4

First Floor Number: 101

Second Floor Number: 201

3.6.5 VTS Management

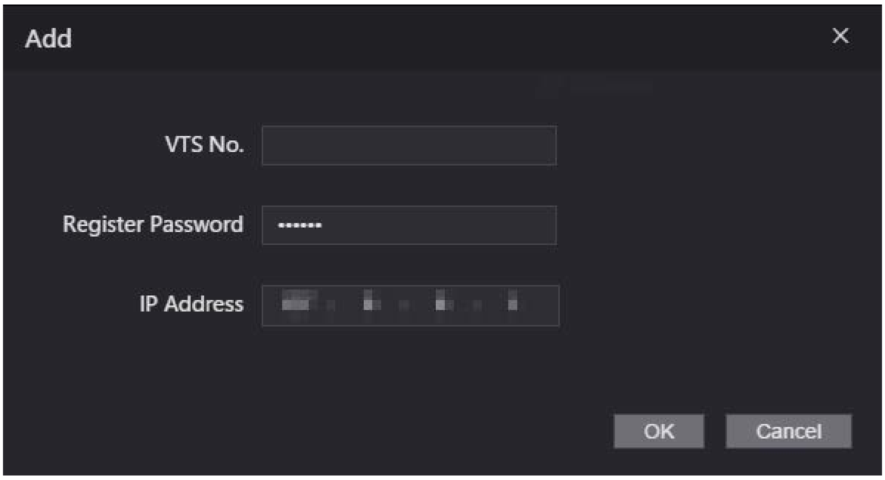
When the access controller works as the SIP server, add master stations (VTS) to call them.

Step 1 Log in to the web.

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

Step 3 Click **Add**.

Figure 3-24 Add managing devices



VTS No.

Register Password ••••••

IP Address [redacted]

Step 4 Enter the information.

- **VTS No.**: It can contain up to nine digits.
- **Register Password**: Keep it default.
- **IP Address**: IP address of the VTS.

Step 5 Click **OK**.

Related Operations

- ✎: Modify the information of a VTS.
- ✖: Delete a VTS.

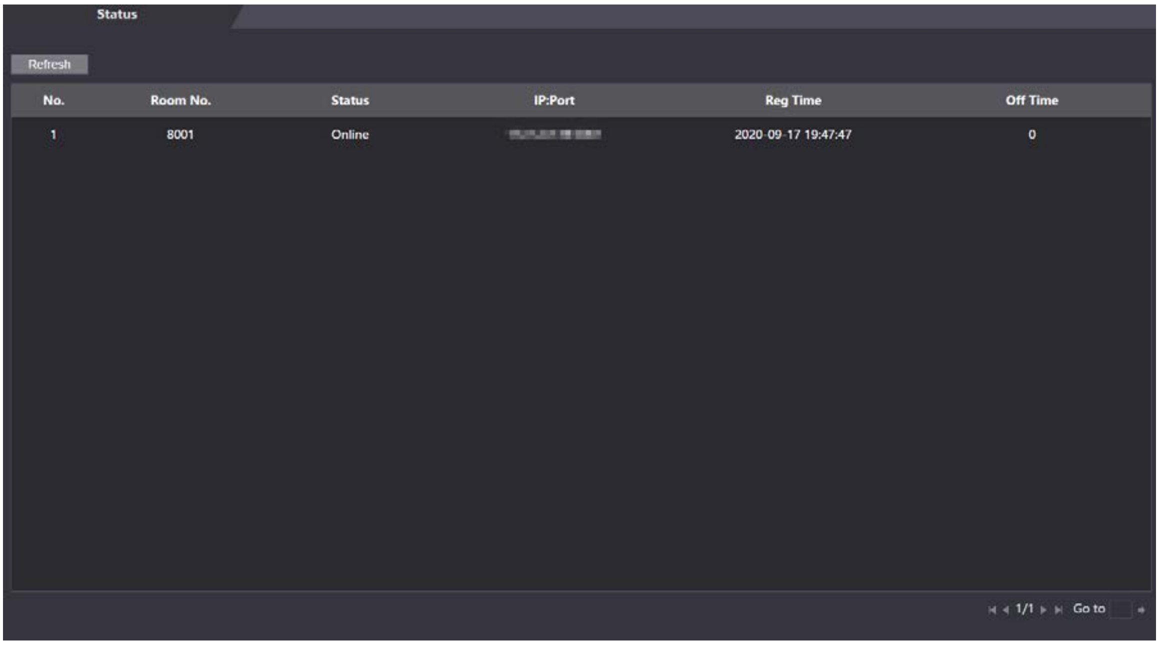
3.6.6 Online Status

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

Step 1 Log in to the web.

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

Figure 3-25 Status



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

3.6.7 Call Logs

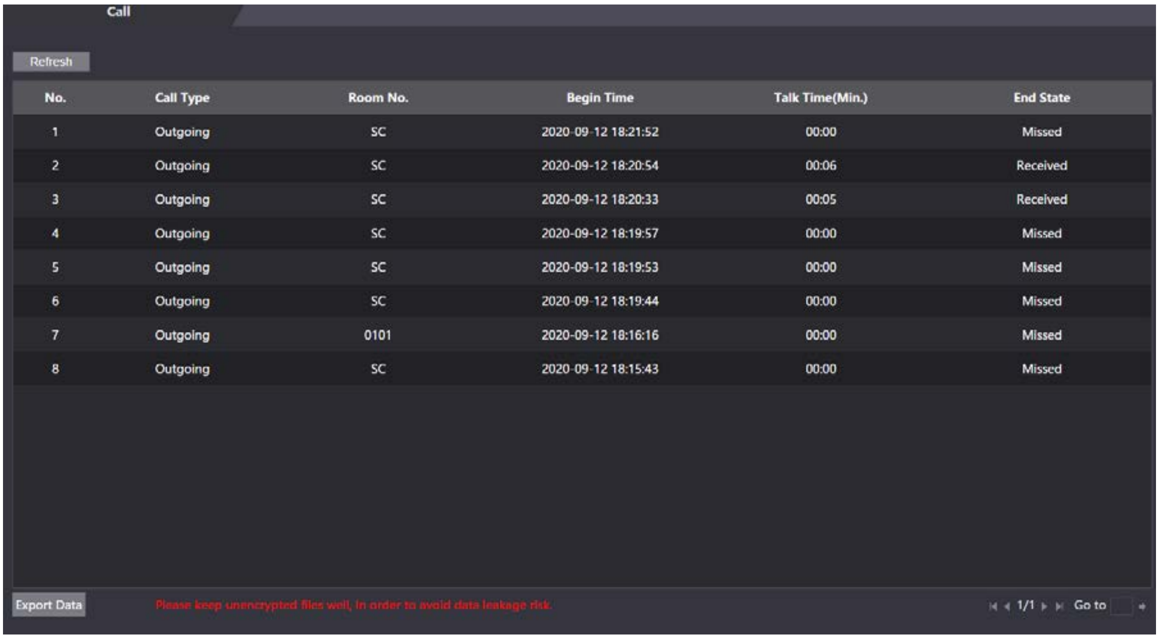
You can check up to 1024 call logs.

Step 1 Log in to the web interface.

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

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

Figure 3-26 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

Please keep unencrypted files well, in order to avoid data leakage risk.

3.7 Time Section

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

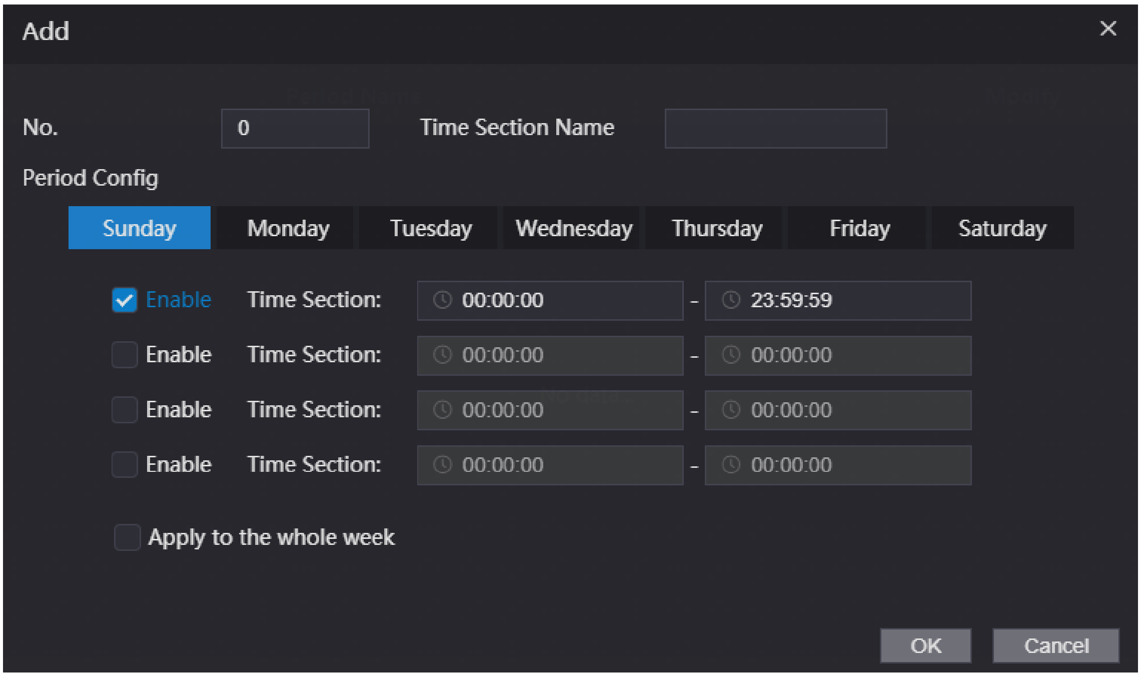
3.7.1 Configuring Time Section

Set when a user can unlock doors each day.

Step 1 Log in to the web interface.

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

Figure 3-27 Time section parameters



No. 0 Time Section Name

☑ Enable Time Section: 00:00:00 - 23:59:59

□ Enable Time Section: 00:00:00 - 00:00:00

□ Enable Time Section: 00:00:00 - 00:00:00

□ Enable Time Section: 00:00:00 - 00:00:00

□ Apply to the whole week

Step 3 Enter a number and name for the time section.

Step 4 Configure periods for each day. You can configure up to four periods.

Step 5 (Optional) Click **Apply to the whole week** to copy the configuration to other days.

Step 6 Click **OK**.

3.7.2 Configuring Holiday Group

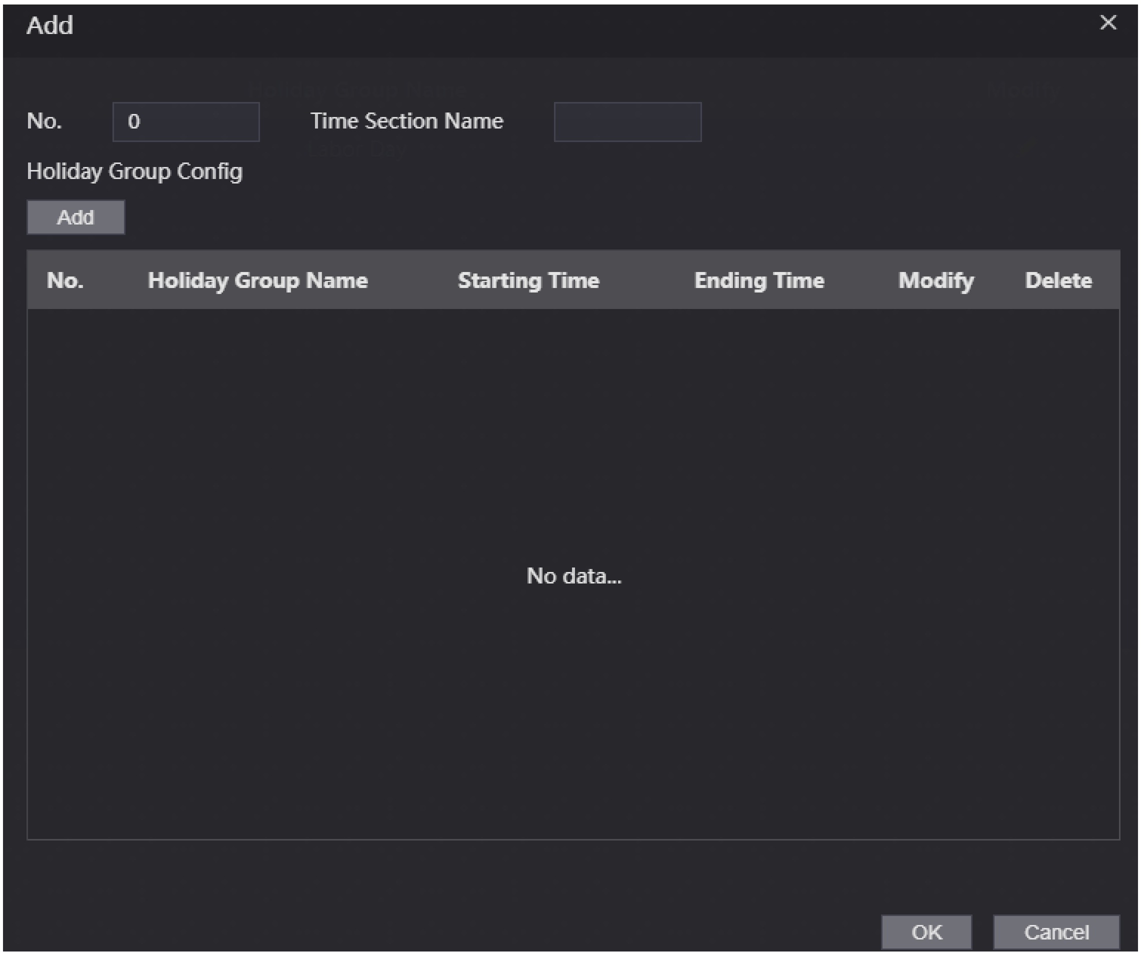
Before setting up a holiday plan, you need to set up holiday groups.

Step 1 Log in to the web interface.

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

Step 3 Click **Add**.

Figure 3-28 Add a holiday group



No. 0

Time Section Name

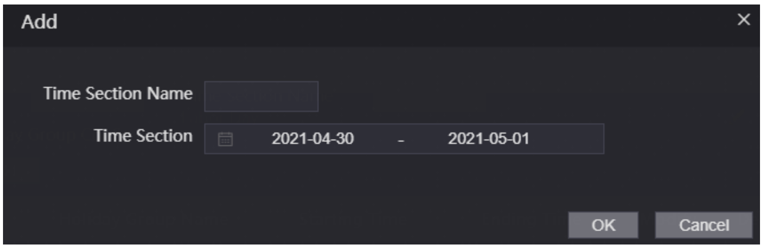
No.	Holiday Group Name	Starting Time	Ending Time	Modify	Delete

No data...

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

Step 5 Click **Add**.

Figure 3-29 Add a holiday



Time Section Name

Time Section 2021-04-30 - 2021-05-01

Step 6 Enter a name for the holiday, select the start and end date, and then click **OK**.

You can add multiple holidays for one holiday group.

Step 7 Click **OK**.

3.7.3 Configuring Holiday Group

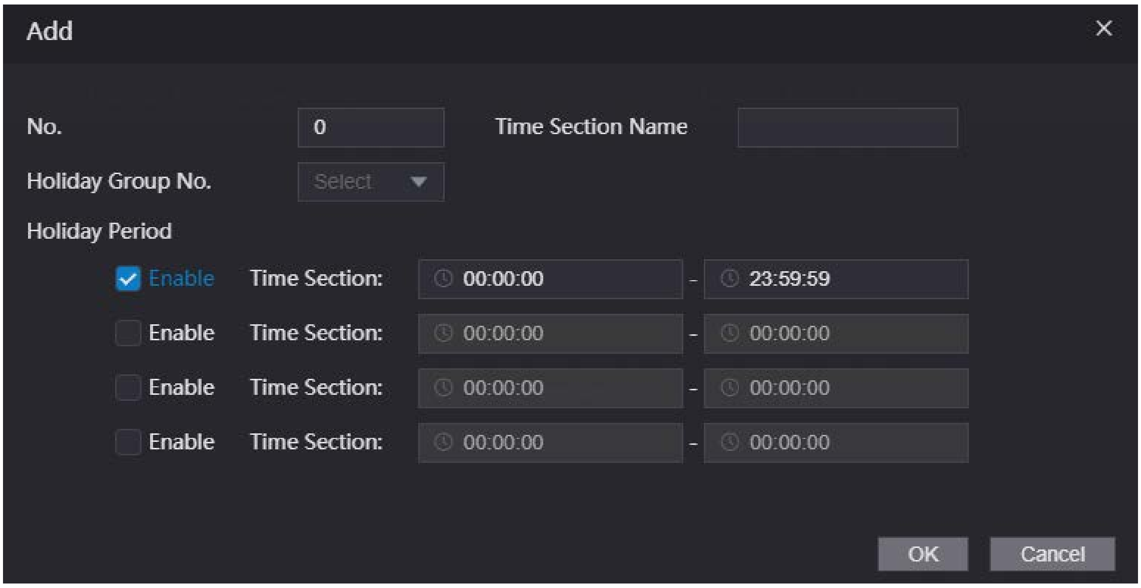
Set up a holiday plan. When adding a user on the access controller, you can select the holiday plan, and then the user can only open the doors within the days defined in the holiday plan.

Step 1 Log in to the web interface.

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

Step 3 Click **Add**.

Figure 3-30 Add a holiday plan



No. 0

Time Section Name

Holiday Group No. Select

Holiday Period

☑ Enable Time Section: 00:00:00 - 23:59:59

□ Enable Time Section: 00:00:00 - 00:00:00

□ Enable Time Section: 00:00:00 - 00:00:00

□ Enable Time Section: 00:00:00 - 00:00:00

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

Step 5 Select the number of a holiday group you configured.

Select **255** if you do not want to select a holiday group.

Step 6 Configure periods for every day in the holiday group you selected. You can configure up to four periods.

Step 7 Click **OK**.

3.8 Data Capacity

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

Step 1 Log in to the web interface.

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

3.9 Video Setting

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

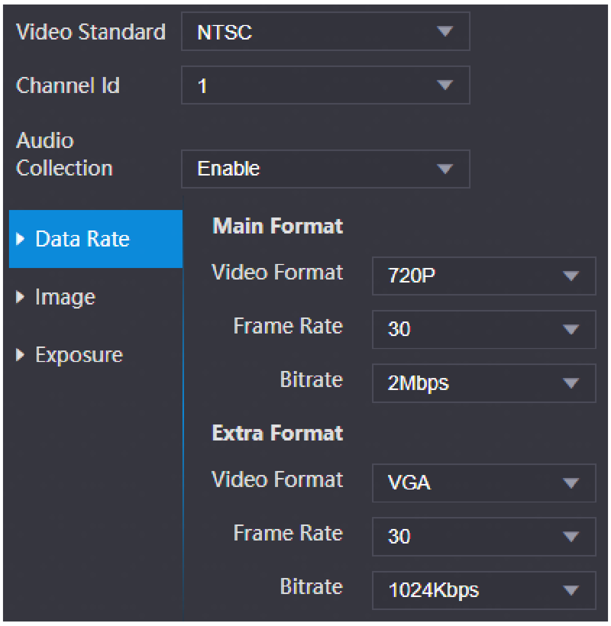
3.9.1 Data Rate

You can configure stream parameters for channel 1.

Step 1 Log in to the web interface.

Step 2 Select **Video Setting** > **Video Setting** > **Data Rate**.

Figure 3-31 Data rate



Video Standard: NTSC

Channel Id: 1

Audio Collection: Enable

Main Format

Video Format: 720P

Frame Rate: 30

Bitrate: 2Mbps

Extra Format

Video Format: VGA

Frame Rate: 30

Bitrate: 1024Kbps

Table 3-8 stream parameter description

Parameter		**Description**
Video Standard		Select **NTSC** or **PAL** 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.
Audio Collection		If enabled, other devices will also receive the audio stream when they pull the video stream from the access controller.
Main Format	Video Format	Select **D1**, **VGA**, **720p** or **1080p** option according to the video quality you want.
	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.
	Bit Rate	The number of bits that are conveyed or processed per unit of time. There are options: 512Kbps, 640Kbps, 768Kbps, 896Kbps, 1024Kbps, 1.25 Mbps, 1.5 Mbps, 1.75 Mbps, and 2 Mbps.

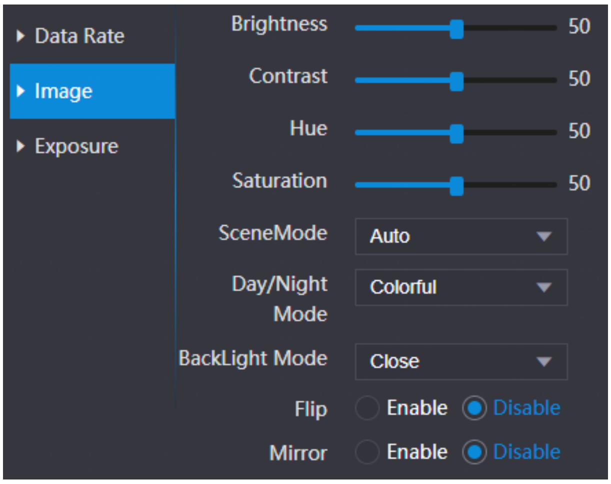
3.9.2 Image

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

Step 1 Log in to the web interface.

Step 2 Select **Video Setting** > **Video Setting** > **Image**.

Figure 3-32 Image



Brightness 50

Contrast 50

Hue 50

Saturation 50

SceneMode: Auto

Day/Night Mode: Colorful

BackLight Mode: Close

Flip: ○ Enable ● Disable

Mirror: ○ Enable ● Disable

Step 3 Select **Wide Dynamic** in the **Backlight Mode**.

Table 3-9 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	● 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. ● 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
Backlight Mode	● Close: Without backlight compensation. ● 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. 📖 When human faces are in the backlight, you need to enable WDR. ● Inhibition: 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, images can be flipped over.

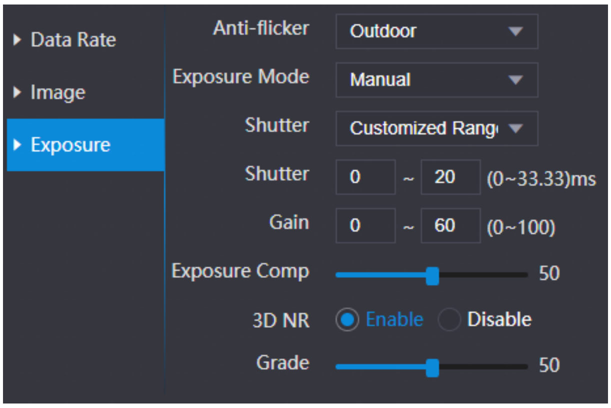
3.9.3 Exposure

You can configure exposure parameters.

Step 1 Log in to the web interface.

Step 2 Select **Video Setting** > **Video Setting** > **Exposure**.

Figure 3-33 Exposure



Anti-flicker: Outdoor

Exposure Mode: Manual

Shutter: Customized Rang

Shutter: 0 ~ 20 (0~33.33)ms

Gain: 0 ~ 60 (0~100)

Exposure Comp: 50

3D NR: ● Enable ○ Disable

Grade: 50

Table 3-10 Exposure parameter description

Parameter	Description
Anti-flicker	● **50Hz**: When the utility frequency of alternating current is 50 Hz, the exposure is automatically adjusted to make sure that there are no stripes on images. ● **60Hz**: When the utility frequency of alternating current is 60 Hz, 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	● **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. 📖 ● When you select **Outdoor** in the Anti-flicker drop-down list, you can select **Shutter Priority** as the exposure mode. ● Exposure modes listed below are for reference only, and might vary with different models.
Shutter	If you select **Customized Range**, you can customize the speed range of the shutter.
	The lower the shutter speed is, the shorter the exposure time and the darker the images will be.
Gain	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	You can adjust the value of the 3D NR when 3D NR is enabled. The larger the value is, the less the noise there will be.

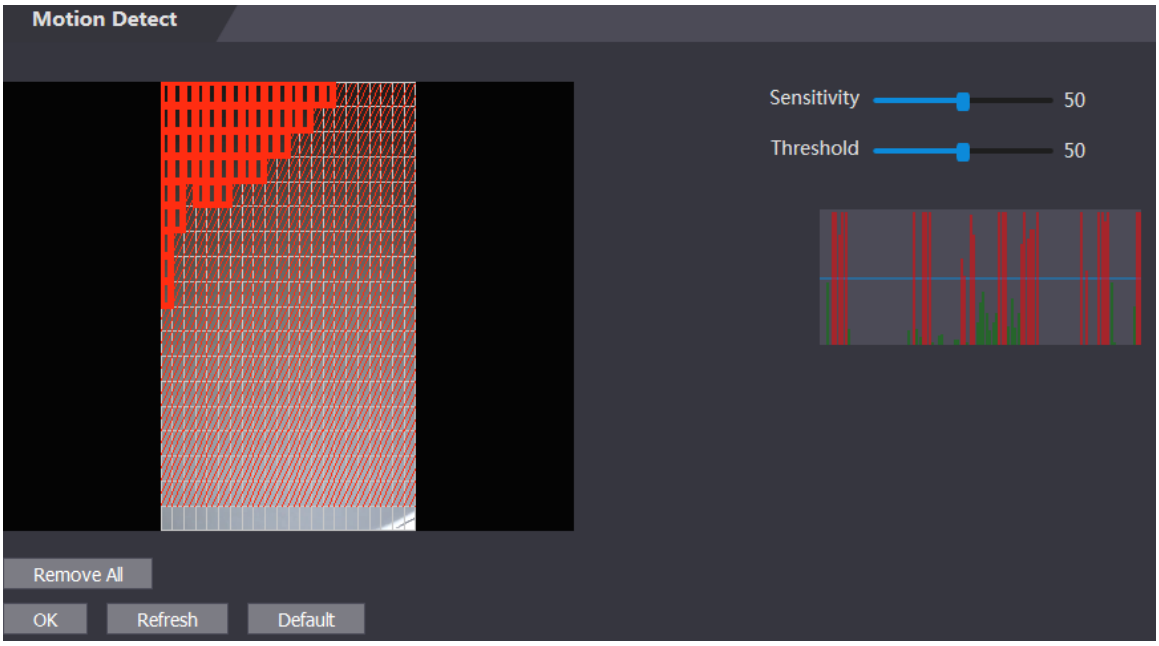
3.9.4 Motion Detection

Set a range in which moving objects can be detected.

Step 1 Log in to the web interface.

Step 2 Select **Video Setting > Motion Detection**.

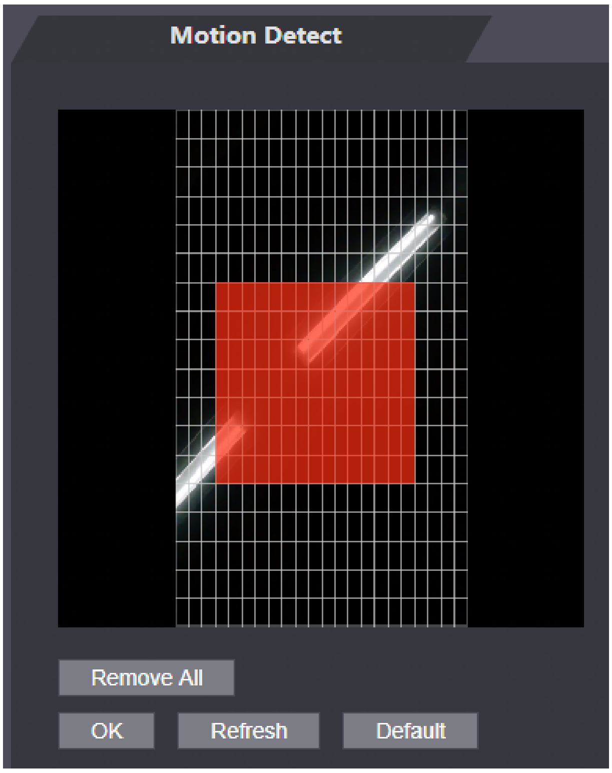
Figure 3-34 Motion detection



Step 3 Press and hold the left mouse button, and then drag the mouse in the red area.

- 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 3-35 Motion detection area



Step 4 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. See Figure 3-34.

Step 5 Click **OK** to finish the setting.

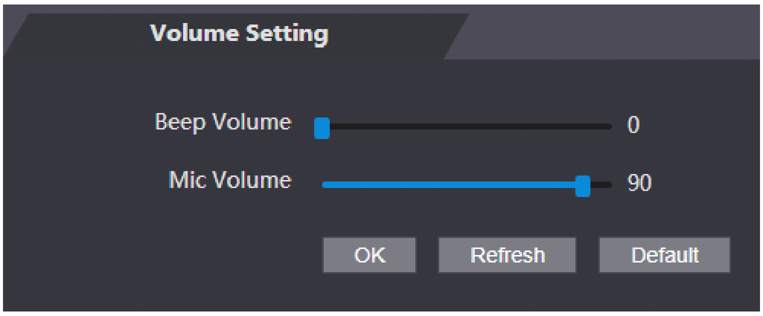
3.9.5 Volume Setting

Adjust the volume of the speaker or the beeping prompt.

Step 1 Log in to the web interface.

Step 2 Select **Video Setting > Volume Setting**.

Figure 3-36 Volume setting



Volume Setting

Beep Volume 0

Mic Volume 90

3.9.6 Image Mode

Select indoor, outdoor or other according to where the access controller is installed.

Step 1 Log in to the web interface.

Step 2 Select **Video Setting > Image Mode**.

- **Indoor**: The access controller is installed indoors.
- **Outdoor**: The access controller is installed outdoors.
- **Other**: The access controller is installed at places with backlights, such as hallways.

Figure 3-37 Image mode

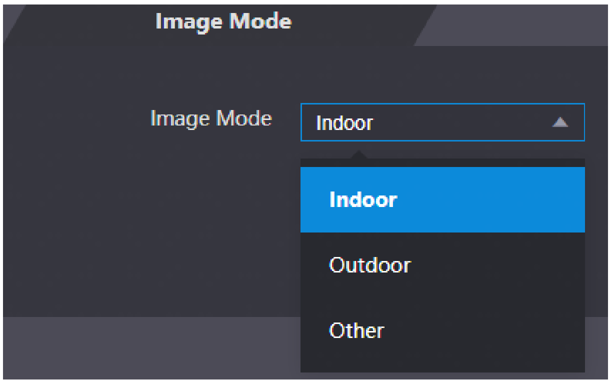


Image Mode

Image Mode: Indoor

3.9.7 Local Coding

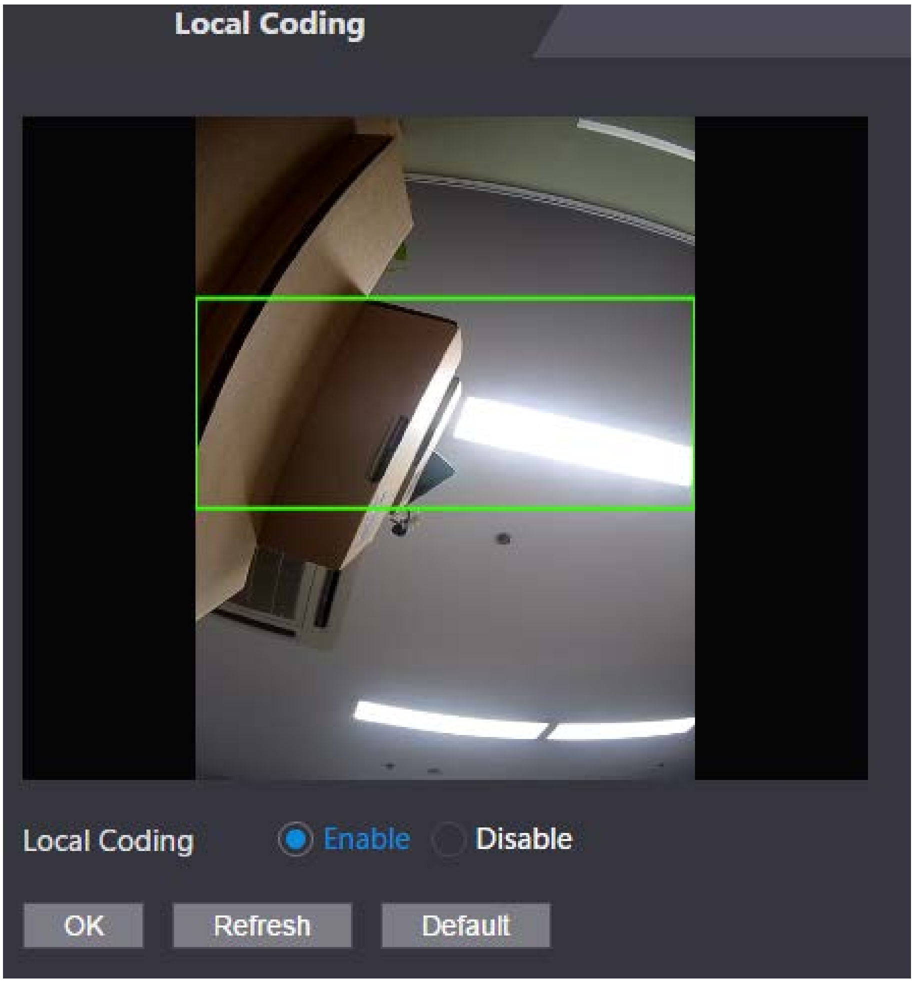
Set up the area to be displayed on the indoor monitors.

Step 1 Log in to the web.

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

Step 3 Enable the function.

Figure 3-38 Local coding



Local Coding

Local Coding ● Enable ○ Disable

Step 4 Click **OK**.

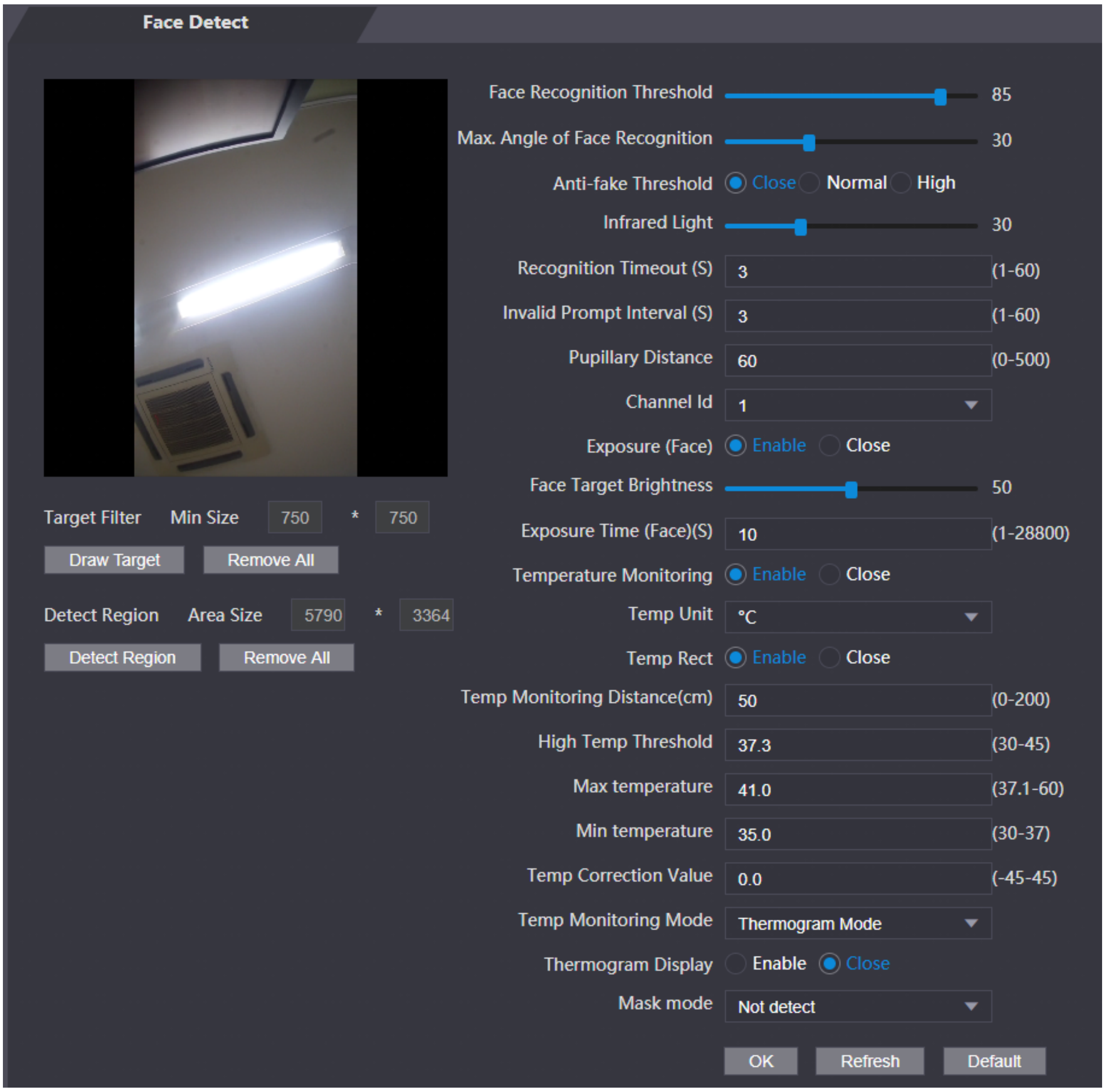
3.10 Face Detection

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

Step 1 Log in to the web interface.

Step 2 Select **Face Detect**.

Figure 3-39 Face detect


Face Detect

Target Filter Min Size 750 * 750

Draw Target Remove All

Detect Region Area Size 5790 * 3364

Detect Region Remove All

Face Recognition Threshold 85

Max. Angle of Face Recognition 30

Anti-fake Threshold ● Close ○ Normal ○ High

Infrared Light 30

Recognition Timeout (S) 3 (1-60)

Invalid Prompt Interval (S) 3 (1-60)

Pupillary Distance 60 (0-500)

Channel Id 1

Exposure (Face) ● Enable ○ Close

Face Target Brightness 50

Exposure Time (Face)(S) 10 (1-28800)

Temperature Monitoring ● Enable ○ Close

Temp Unit ℃

Temp Rect ● Enable ○ Close

Temp Monitoring Distance(cm) 50 (0-200)

High Temp Threshold 37.3 (30-45)

Max temperature 41.0 (37.1-60)

Min temperature 35.0 (30-37)

Temp Correction Value 0.0 (-45-45)

Temp Monitoring Mode Thermogram Mode

Thermogram Display ○ Enable ● Close

Mask mode Not detect

Step 3 Configure parameters.

Table 3-11 Face detect parameter description

Parameter	Description
Face Recognition Threshold	The larger the value is, the higher the accuracy will be.
Max. Angle of Face Recognition	The larger the angle is, the wider range of the profiles will be recognized.
Anti-fake Threshold	This function prevents people from unlocking by face images or models.
Infrared Light	Adjust IR brightnees by dragging the scroll bar.
Recognition Timeout	The interval of the prompt during valid face recognition.
Invalid Prompt Interval	The interval of the prompt during invalid face recognition.
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.

Parameter	Description
Channel ID	There are two options: 1 and 2. 1 is white light camera and 2 is IR light camera.
Exposure(Face)	After face exposure is enabled, human face will be clearer when the access controller is installed outdoors.
Face Target Brightness	The default value is 50. Adjust the brightness as needed.
Exposure Time (Face)(S)	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.
Temperature Monitoring	Enable or disable the temperature monitoring function.
Temp Unit	Select ° C or ° F.
Temp Rect	Set whether to display the temperature monitoring box on the standby interface or not.
Temp Correction Duration (ms)	When monitoring the temperature, the access controller will take the temperature value after the time defined by this parameter. 📖 Only certain models support this parameter.
Temp Monitoring Distance (cm)	50 by default. You can correct the monitored temperature as needed according to the distance you set. 📖 Only certain models support this parameter.
High Temp Threshold	Set the temperature threshold. The monitored body temperature will be judged as high temperature if it is greater than or equal to the set value.
Max Temperature	Set the temperature range you need. If the monitored temperature is lower than the lower limit, it will prompt that the temperature is too low; if higher than the upper limit, it will prompt that there is a heat source interfering with the function.
Min Temperature	
Temp Correction Value	This parameter is for testing. The difference of the temperature monitoring environment might cause the temperature deviation between the monitored temperature and the actual temperature. You can select multiple monitored samples for testing, and then correct the temperature deviation by this parameter according to the comparison between the monitored temperature and the actual temperature. For example, if the monitored temperature is 0.5°C lower than the actual temperature, the correction value is set to 0.5°C; if the monitored temperature is 0.5°C higher than the actual temperature, the correction value is set to -0.5°C.

Parameter	Description
Temp Monitoring Mode	● Auto: Uses a face heat map for face recognition; if heat maps are not found, it will automatically change to calibration mode. ● Thermogram: Uses only a heat map for face recognition and temperature monitoring. ● Calibration: Uses a white light image of a face for face recognition, and then extract and apply the coordinates on the face heat map for temperature monitoring. 📖 Only certain models support this parameter.
Thermogram Display	Display a heat map at the upper-left corner. 📖 Only certain models support this parameter.
Mask Mode	● **No detect**: Mask is not detected during face recognition. ● **Mask reminder**: Mask is detected during face recognition. If the person is detected without wearing a mask, the system will prompt mask reminder and passage is allowed. ● **Mask intercept**: Mask is detected during face recognition. If the person is detected without wearing a mask, the system will prompt mask reminder and passage is not allowed.
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.

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

3.11 Network Setting

3.11.1 TCP/IP

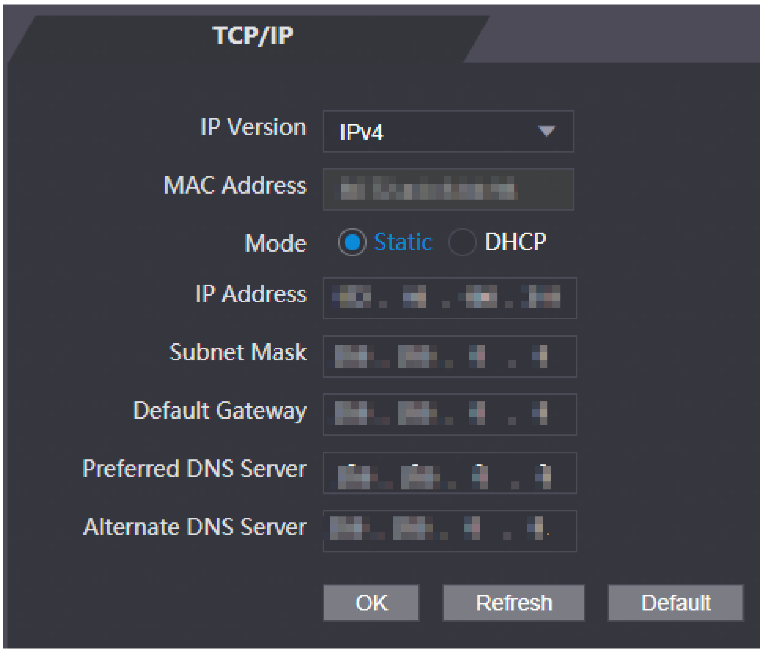
You need to configure IP address and DNS server to make sure that the access controller can communicate with other devices.

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

Step 1 Log in to the web interface.

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

Figure 3-40 TCP/IP



TCP/IP

IP Version: IPv4

MAC Address: [redacted]

Mode: ● Static ○ DHCP

IP Address: [redacted]

Subnet Mask: [redacted]

Default Gateway: [redacted]

Preferred DNS Server: [redacted]

Alternate DNS Server: [redacted]

Step 3 Configure parameters.

Table 3-12 TCP/IP

Parameter	Description
IP Version	There is one option: IPv4.
MAC Address	MAC address of the access controller.
Mode	● Static: Set IP address, subnet mask, and gateway address manually. ● DHCP ◇ After DHCP is enabled, IP address, subnet mask, and gateway address cannot be configured. ◇ If DHCP is effective, IP address, subnet mask, and gateway address will be displayed automatically; if DHCP is not effective, IP address, subnet mask, and gateway address will all be zero. ◇ If you want to see the default IP when DHCP is effective, you need to disable DHCP.
Link-local address	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.
IP Address	Enter IP address, and then configure subnet mask and gateway address. 📖 IP address and gateway address must be in the same network segment.
Subnet Mask	
Default Gateway	
Preferred/ Alternate DNS Server	Set IP address of the preferred DNS server.

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

3.11.2 Port

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

Step 1 Log in to the web interface.

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

Step 3 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 3-13 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 AC 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 4 Click **OK** to complete the setting.

3.11.3 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 Log in to the web interface.

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

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

Table 3-14 Auto register description

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

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

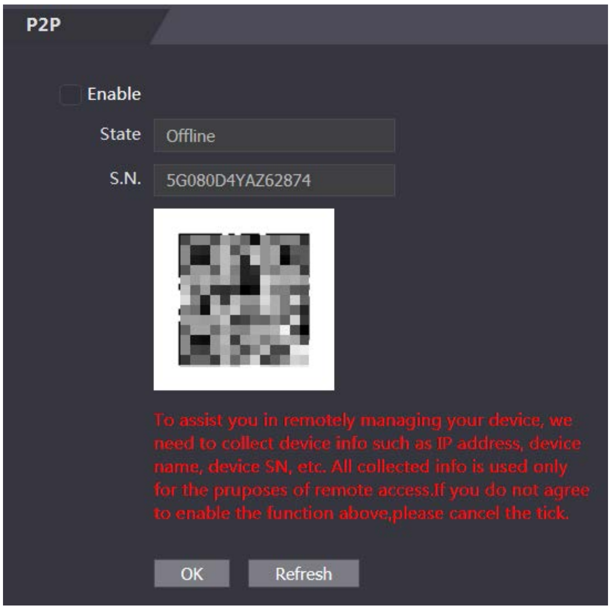
3.11.4 P2P

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 3-41 P2P



P2P

□ Enable

State: Offline

S.N.: 5G080D4YAZ62874

To assist you in remotely managing your device, we need to collect device info such as IP address, device name, device SN, etc. All collected info is used only for the purposes of remote access.If you do not agree to enable the function above,please cancel the tick.

Step 1 Log in to the web interface.

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

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

Step 4 Click **OK**.

🕮

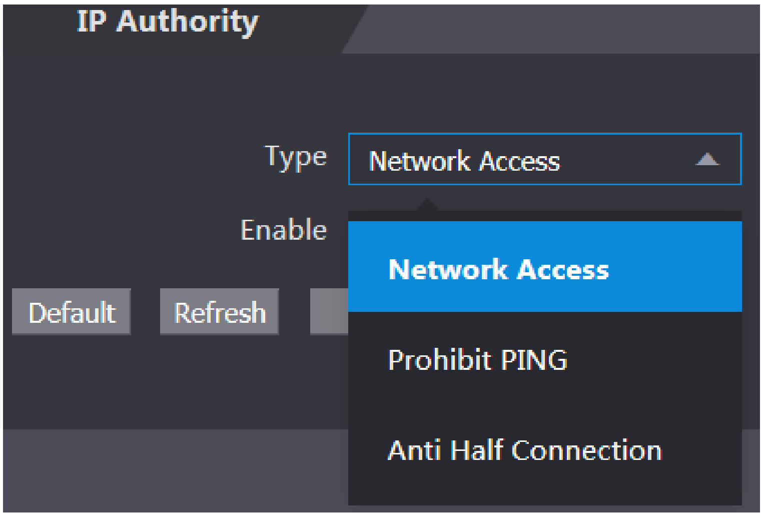
Scan the QR code on your web interface to get the serial number of the access controller.

3.12 Safety Management

3.12.1 IP Authority

Select a cybersecurity mode as needed.

Figure 3-42 IP authority



IP Authority

Type: Network Access

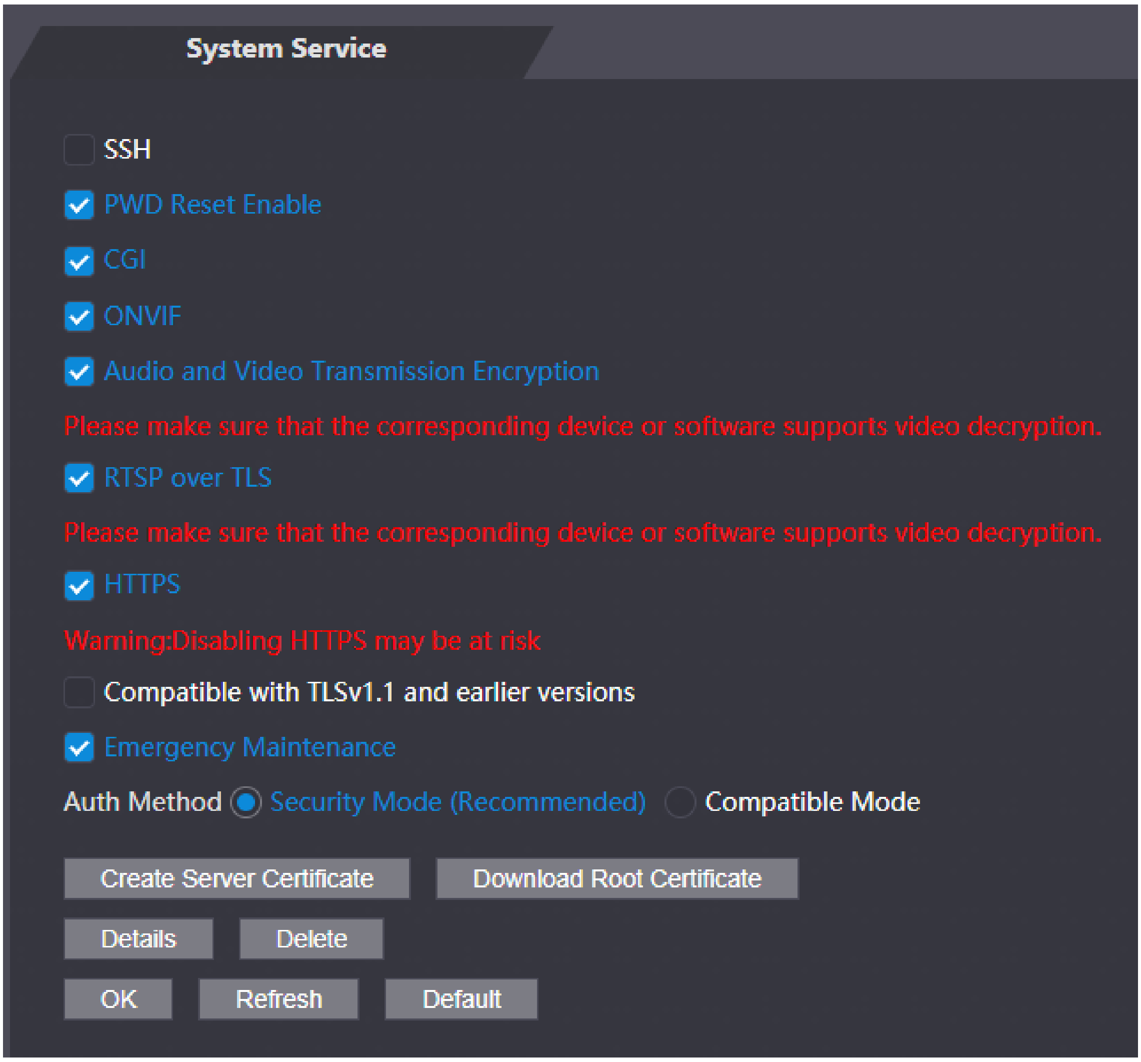
3.12.2 Systems

3.12.2.1 System Service

Enable or disable the system services as needed.

The system service configuration on the web interface is synchronized to the **Features** interface of the access controller.

Figure 3-43 System service



System Service

☐ SSH

☑ PWD Reset Enable

☑ CGI

☑ ONVIF

☑ Audio and Video Transmission Encryption

Please make sure that the corresponding device or software supports video decryption.

☑ RTSP over TLS

Please make sure that the corresponding device or software supports video decryption.

☑ HTTPS

Warning:Disabling HTTPS may be at risk

☐ Compatible with TLSv1.1 and earlier versions

☑ Emergency Maintenance

Auth Method ● Security Mode (Recommended) ○ Compatible Mode

Table 3-15 Parameter description

Parameter	Description
SSH	Secure Shell (SSH) is a cryptographic network protocol for operating network services securely over an unsecured network. When SSH is enabled, SSH provides cryptographic service for the data transmission.
PWD Reset Enable	If enabled, you can reset the password. This function is enabled by default.

Parameter	Description
CGI	Common Gateway Interface (CGI) offers a standard protocol for web servers to execute programs similarly to console applications running on a server that dynamically generates web pages. When CGI is enabled, CGI commands can be used. The CGI is enabled by default.
ONVIF	Enable other devices to pull video stream of the VTO through the ONVIF protocol.
Audio and Video Transmission Encryption	Encrypt all data during voice or video call.
RTSP over TLS	Output encrypted bit stream through RTSP.
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.
Compatible with TLSv1.1 and earlier versions	Enable this function if your browser is using TLS V1.1 or earlier versions.
Emergency Maintenance	Enable it for fault analysis and repair. This function will occupy 8088 and 8087 ports.
Auth Method	● **Security Mode** (recommended): Support logging in with Digest authentication. ● **Compatible Mode**: Use the old login method.

3.12.2.2 Creating Server Certificate

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

3.12.2.3 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.

3.13 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.

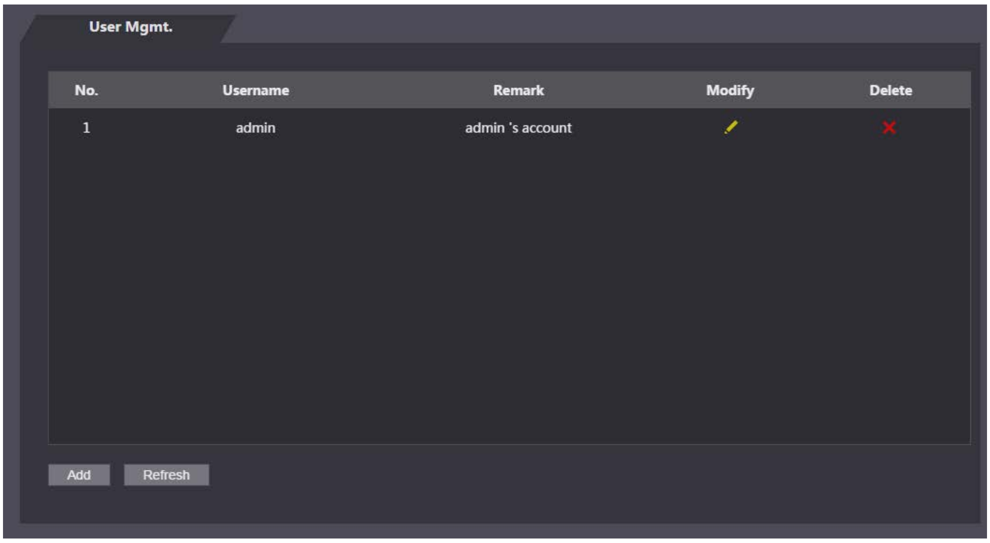
3.13.1 Adding Users

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.

3.13.2 Modifying User Information

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

Figure 3-44 User management

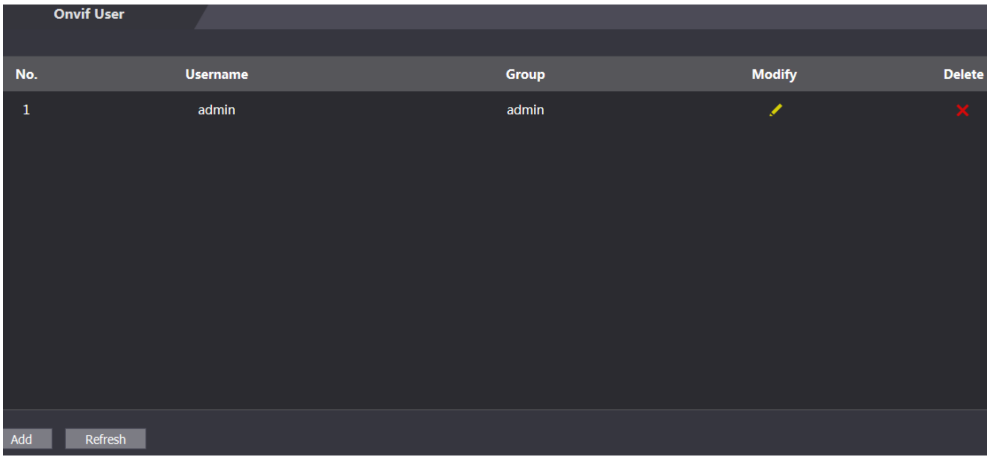


No.	Username	Remark	Modify	Delete
1	admin	admin 's account	✎	✕

3.13.3 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 3-45 Onvif user



No.	Username	Group	Modify	Delete
1	admin	admin	✎	✕

3.14 Maintenance

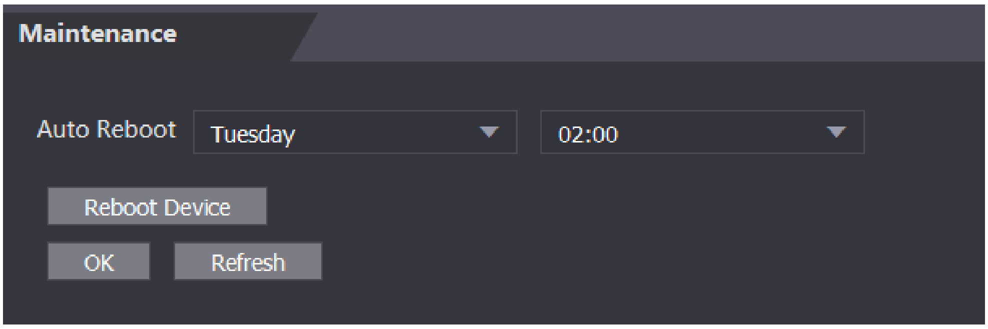
You can make the access controller reboot itself in idle time to improve the running speed of the access controller. You need to set the auto reboot date and time.

Step 1 Log in to the web interface.

Step 2 Select **Maintenance**.

Step 3 Set the auto reboot time, and then click **OK**.

Figure 3-46 Maintenance



Maintenance

Auto Reboot: Tuesday, 02:00

For example, the access controller will reboot at 2 O'clock in the morning every Tuesday.

Click **Reboot Device**, the access controller will reboot immediately.

3.15 Configuration Management

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

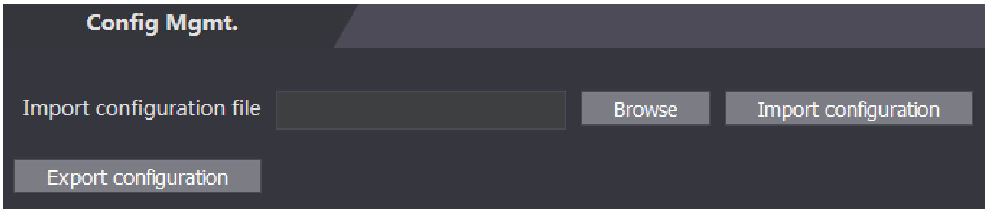
3.15.1 Exporting Configuration File

You can export the configuration file of the access controller for backup.

Step 1 Log in to the web interface.

Step 2 Select **Config Mgmt.** on the navigation bar.

Figure 3-47 Configuration management



Config Mgmt.

Import configuration file

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

📖

IP information of the access controller will not be exported.

3.15.2 Importing Configuration File

You can import the configuration file that is exported from an access controller to another access controller with the same model.

Step 1 Log in to the web interface.

Step 2 Select **Config Mgmt.** on the navigation bar.

Step 3 On the configuration management interface, click **Browse** to select the configuration file that you want to import, and then click **Import configuration**.

The access controller will reboot after importing configuration file.

3.15.3 Default

- **Restore Factory:** Reset all the data and configuration of the access controller.
- **Restore Factory (Save user & log)**: Reset all data and configuration, except for user information and logs.

3.16 Upgrade

📖

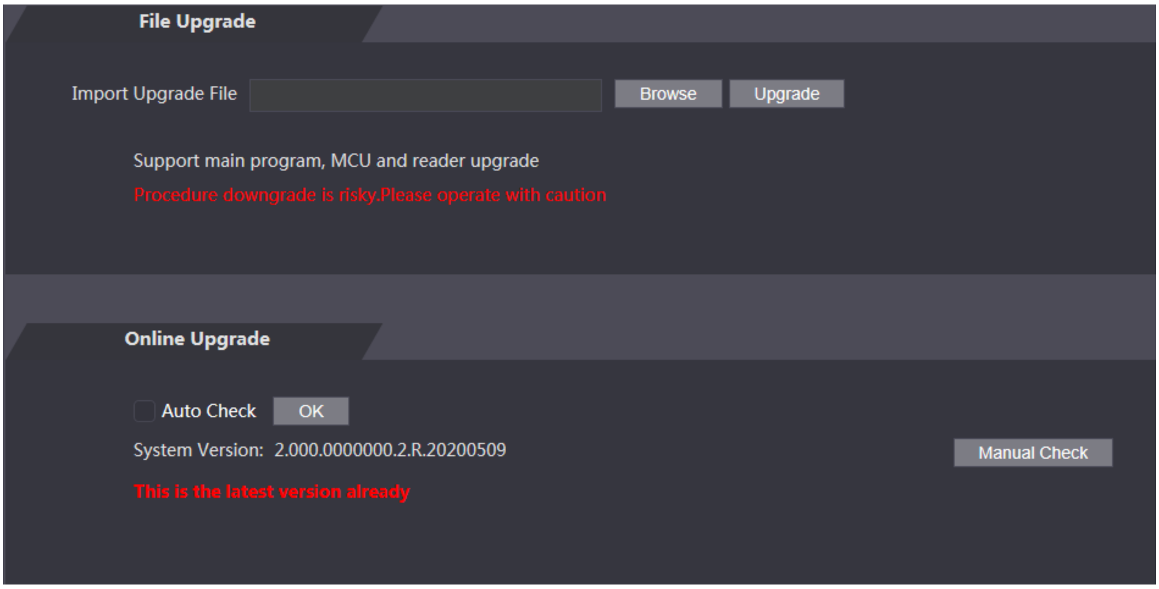
- Export the configuration file for backup before upgrade, and then import it after the upgrade is completed.
- Make sure that the upgrade file has been obtained. You can get it from technical support.
- Do not disconnect the power or network, or reboot or shutdown the access controller during upgrade.

Step 1 Log in to the web interface.

Step 2 Select **Upgrade** on the navigation bar.

Step 3 On the **Upgrade** interface, click **Browse** to select the upgrade file, and then click **Upgrade**.

Figure 3-48 Upgrade



Support main program, MCU and reader upgrade

Procedure downgrade is risky.Please operate with caution

□ Auto Check

System Version: 2.000.0000000.2.R.20200509

This is the latest version already

If the upgrade is succeeded, the system pops up a message indicating that the upgrade is completed. If the upgrade is failed, there will be corresponding prompts.

- You can select **Auto Check** to upgrade the system automatically. You can also select **Manual Check** to upgrade the system manually.
- The access controller will reboot after upgrade.
- You click **Version Info** on the left navigation menu to check version after upgrade.

3.17 Version Information

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

Step 1 Log in to the web interface.

Step 2 Select **Version Info** on the navigation bar.

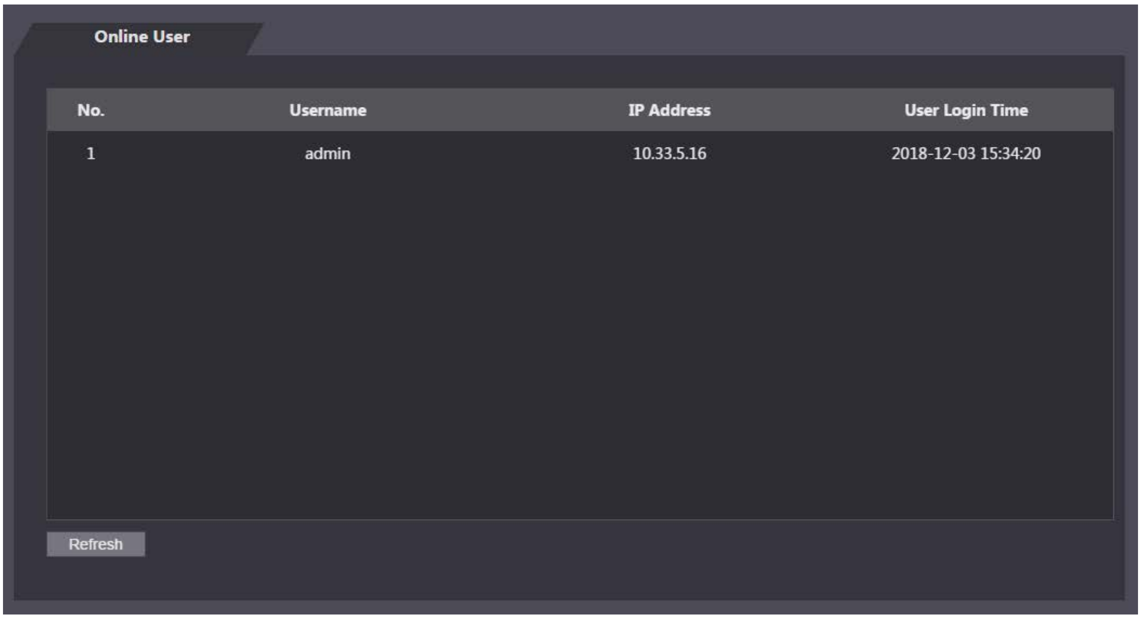
3.18 Online User

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

Step 1 Log in to the web interface.

Step 2 Select **Online User** on the navigation bar.

Figure 3-49 Online user



No.	Username	IP Address	User Login Time
1	admin	10.33.5.16	2018-12-03 15:34:20

3.19 System Log

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

3.19.1 System Logs

View and search for system logs.

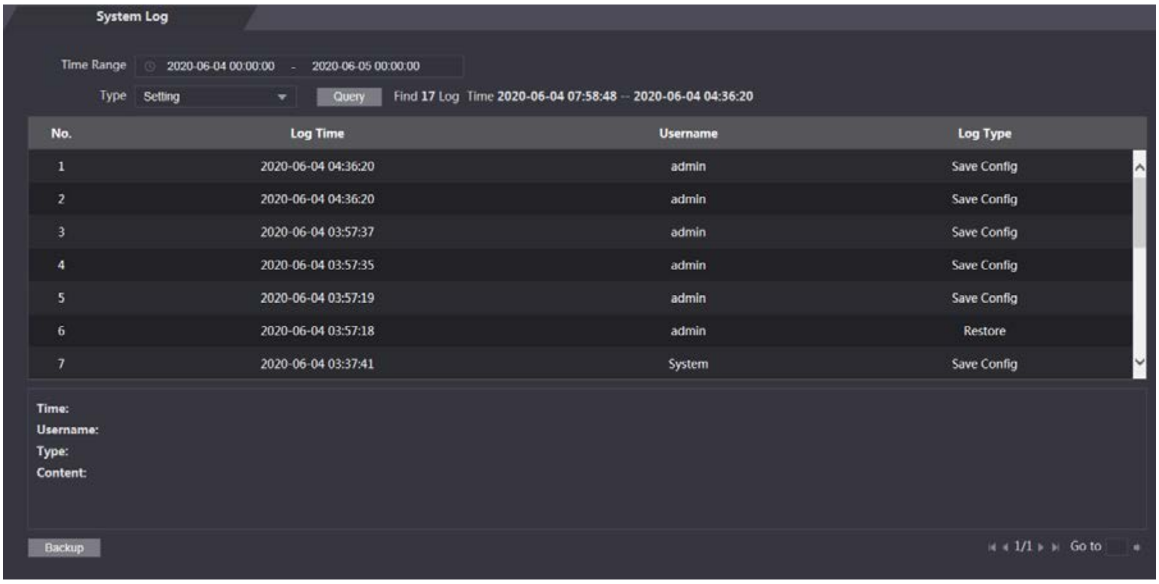
Step 1 Log in to the web interface.

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

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

Click **Backup** to download the results.

Figure 3-50 Seach for logs



System Log

Time Range 2020-06-04 00:00:00 - 2020-06-05 00:00:00

Type Setting

Query Find 17 Log Time 2020-06-04 07:58:48 -- 2020-06-04 04:36:20

No.	Log Time	Username	Log Type
1	2020-06-04 04:36:20	admin	Save Config
2	2020-06-04 04:36:20	admin	Save Config
3	2020-06-04 03:57:37	admin	Save Config
4	2020-06-04 03:57:35	admin	Save Config
5	2020-06-04 03:57:19	admin	Save Config
6	2020-06-04 03:57:18	admin	Restore
7	2020-06-04 03:37:41	System	Save Config

Time:
Username:
Type:
Content:

3.19.2 Admin Log

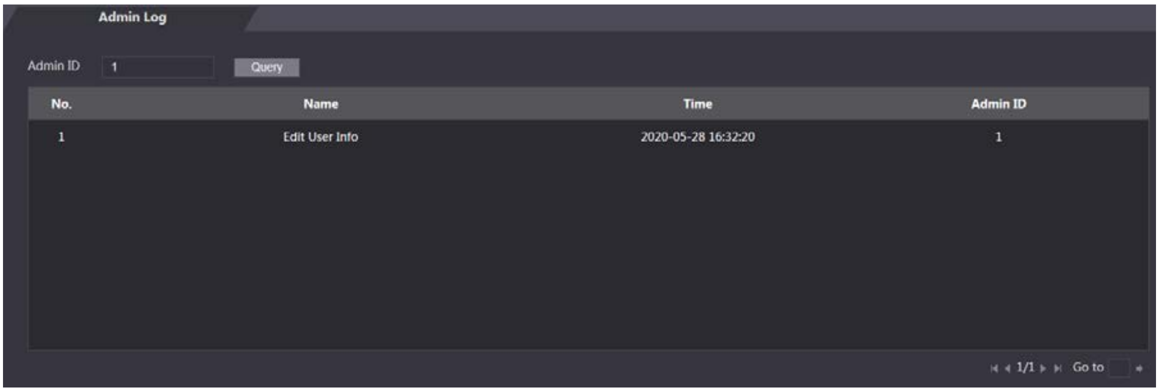
Search for admin logs by admin ID.

Step 1 Log in to the web interface.

Step 2 Select **System Log** > **Admin Log**.

Step 3 Enter the admin ID, and then click **Query**.

Figure 3-51 Admin log



Admin Log

Admin ID 1 Query

No.	Name	Time	Admin ID
1	Edit User Info	2020-05-28 16:32:20	1

3.19.3 Unlock Records

Search for unlock records and export them.

Step 1 Log in to the web interface.

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

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

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

3.20 Fusion Calibration

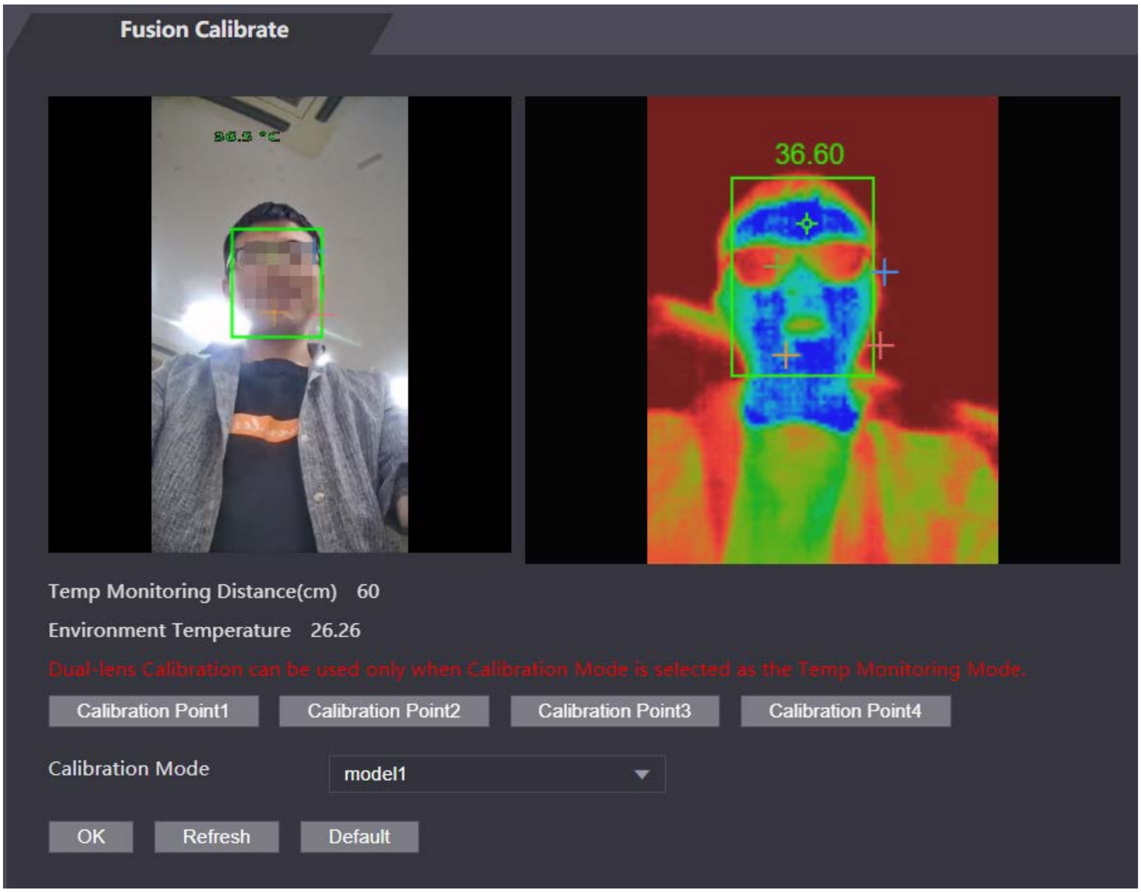
Set up the coordinate relationship between the white light face image and face heat map. When calibration mode is enabled, the access controller will use the coordinate relationship to measure temperature on the face heat map.

- Only certain models support this function.
- Select **Temp Monitoring Mode** to **Calibration Mode**. See "3.10 Face Detection" for details.

Step 1 Select **Fusion Calibrate**.

Step 2 Select a model from **Calibration Mode** according to the type of the access controller.

Figure 3-52 Set up coordinate relationship



Fusion Calibrate

Temp Monitoring Distance(cm) 60

Environment Temperature 26.26

Dual-lens Calibration can be used only when Calibration Mode is selected as the Temp Monitoring Mode.

Calibration Mode: model1

Step 3 Click **Calibration Point1**.

Step 4 Click the image on the left, and then left to set up a relationship between the two locations.

Step 5 Click **Calibration Confirmed**.

Step 6 Repeat step 2–4 for calibration point 2–4.

Step 7 Click **OK**.

Step 8 (Optional) Click **Default** to reset all configuration the default settings.

3.21 Advanced

You can view environment temperature, and core temperature and body surface temperature of a target.

Only certain models support this function.

3.22 Exit

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

4 SmartPSS AC Configuration

You can manage the access controller through the SmartPSS AC client. For detailed configurations, see the SmartPSS AC user manual.

SmartPSS AC interfaces might vary with versions, and the actual interface shall prevail.

4.1 Login

Step 1 Install the SmartPSS AC.

Step 2 Double-click SmartPSS..., and then follow the instructions to finish the initialization and log in.

4.2 Adding Devices

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

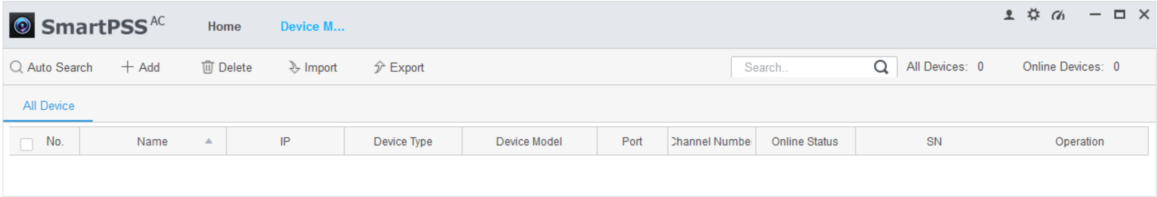
4.2.1 Auto Search

You can search and add access controllers at the same network segment to the SmartPSS AC.

Step 1 Log in to SmartPSS AC.

Step 2 Click **Device Manager** at the lower left corner.

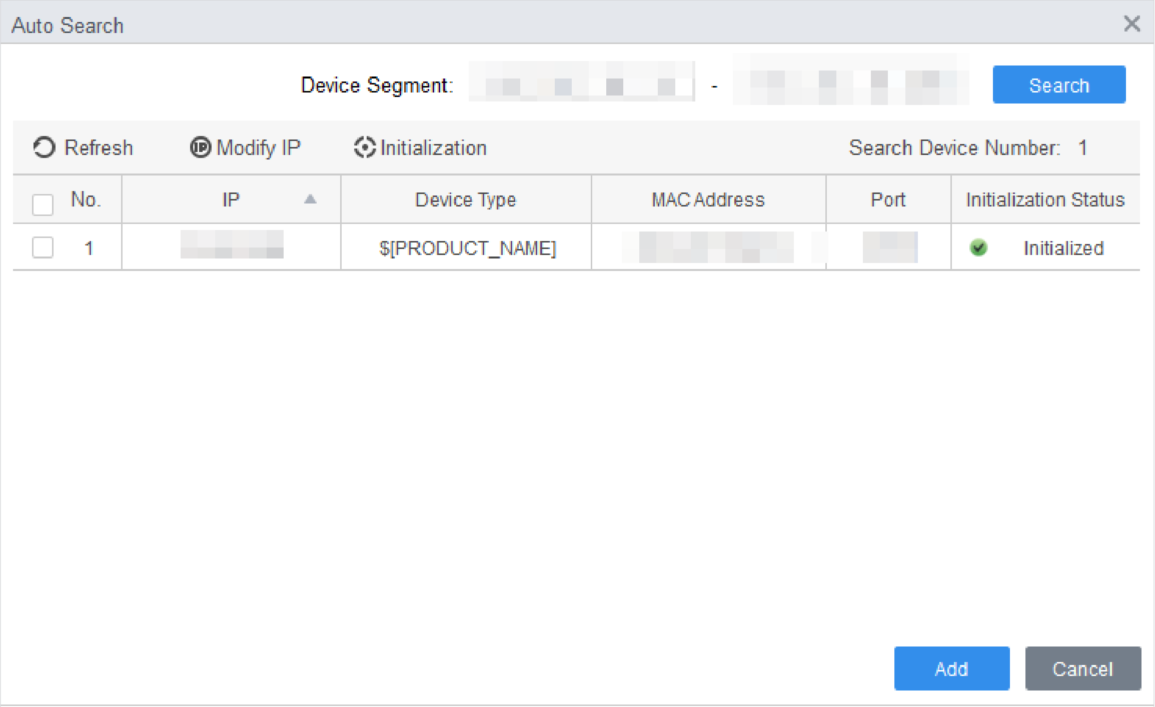
Figure 4-1 Devices



□ No.	Name	IP	Device Type	Device Model	Port	Channel Numbe	Online Status	SN	Operation

Step 3 Click **Auto Search**.

Figure 4-2 Auto search



Auto Search

Device Segment: [redacted] - [redacted] Search

Refresh Modify IP Initialization Search Device Number: 1

□ No.	IP	Device Type	MAC Address	Port	Initialization Status
□ 1	[redacted]	$[PRODUCT_NAME]	[redacted]	[redacted]	✓ Initialized

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

A search result list will be displayed.

Step 5 Select access controllers that you want to add to the SmartPSS AC, and then click **Add**. The Login information dialog box will be displayed.

Step 6 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 SmartPSS AC user manual.

4.2.2 Manual Add

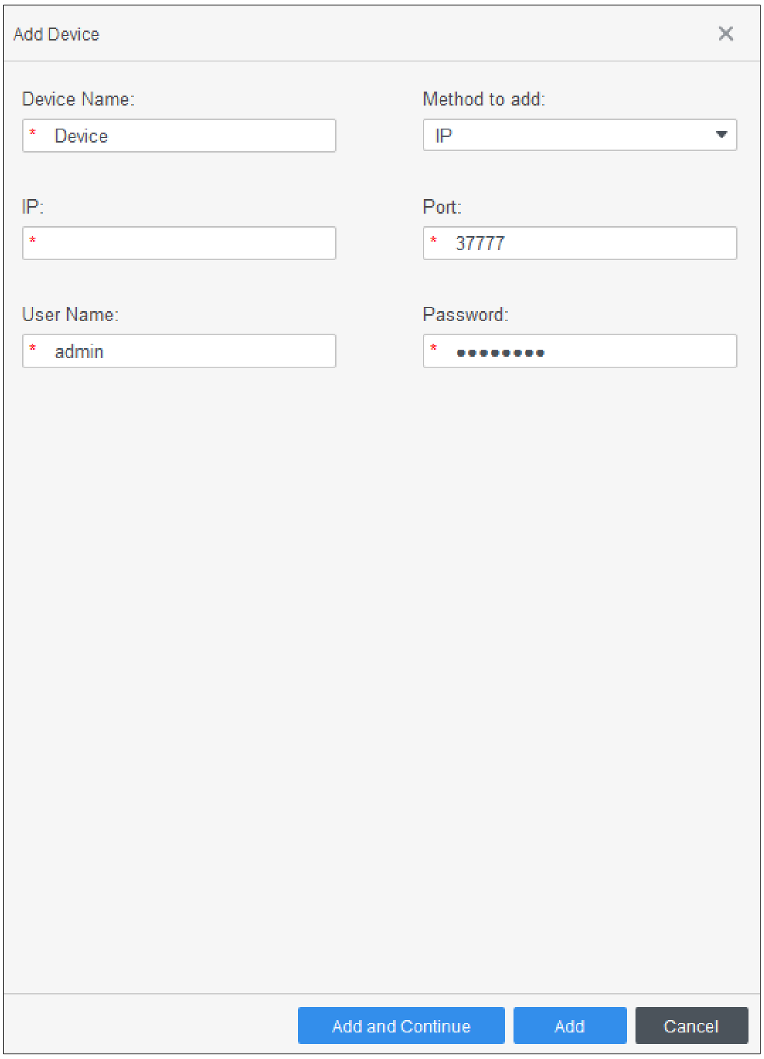
You can add access controllers manually. You need to know IP addresses and domain names of access controllers that you want to add.

Step 1 Log in to SmartPSS AC.

Step 2 Click **Device Manager** at the lower left corner.

Step 3 Click **Add** on the **Devices** interface, and the **Manual Add** interface will be displayed.

Figure 4-3 Manual add


Add Device

Device Name: * Device

Method to add: IP

IP: *

Port: * 37777

User Name: * admin

Password: * ●●●●●●●●●

Step 4 Enter the device name, select a method to add, enter the IP, Port number (37777 by default), User Name, and Password.

Step 5 Click **Add**, and then you can see the added access controller on the **Devices** interface.

4.3 User Management

4.3.1 Card Type Setting

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

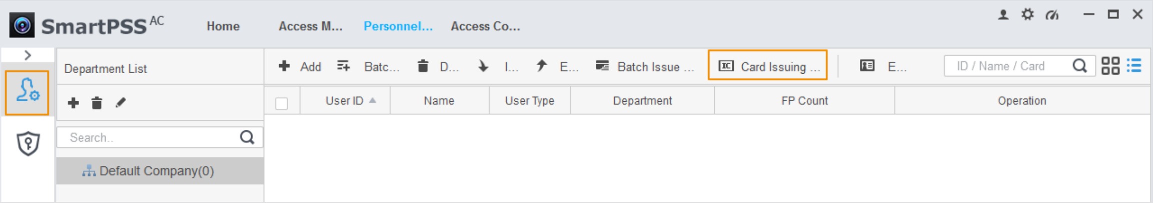
⚠

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

Step 1 Log in to SmartPSS AC.

Step 2 Click **Personnel Manager**.

Figure 4-4 Personnel manager

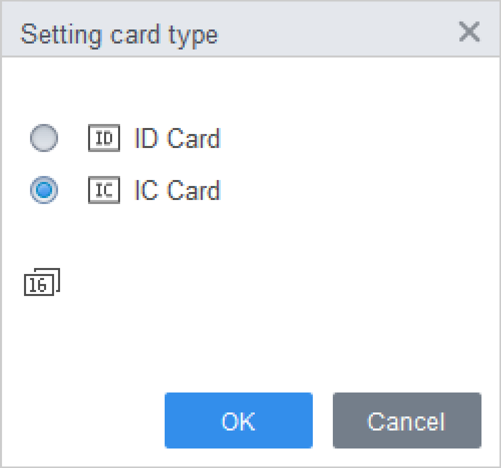


Step 3 On the **Personnel Manager** interface, click , then click .

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

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

Figure 4-5 Setting card type



Setting card type

○ ID Card

● IC Card

Step 6 Click **OK**.

4.3.2 Adding User

Select one of the methods to add user.

- Add user one by one manually.
- Add user in batches.
- Extract user information from other devices.
- Import user information from the local.

4.3.2.1 Manual Add

You can add user one by one manually.

Step 1 Log in to SmartPSS AC.

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

Step 3 Add basic information of the user.

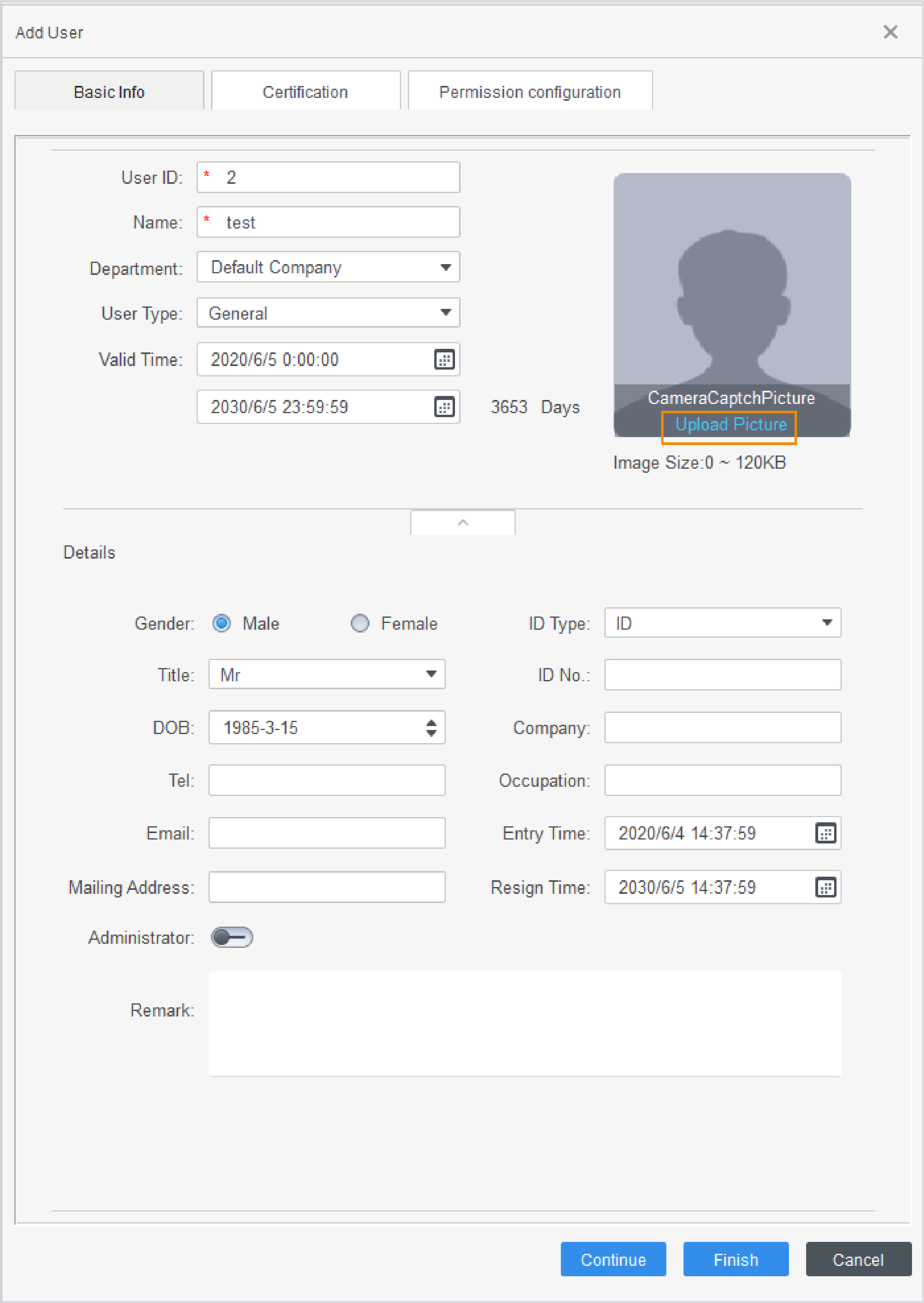
1) Click the **Basic Info** tab on the **Add User** interface, and then add basic information of the user.

2) Click the image, and then click **Upload Picture** to add a face image.

The uploaded face image will display on the capture frame.

Make sure that the image pixels are more than 500 × 500; image size is less than 120 KB.

Figure 4-6 Add basic information



Add User

Basic Info | Certification | Permission configuration

User ID: * 2

Name: * test

Department: Default Company

User Type: General

Valid Time: 2020/6/5 0:00:00

2030/6/5 23:59:59 3653 Days

Image Size:0 ~ 120KB

Details

Gender: ● Male ○ Female

ID Type: ID

Title: Mr

ID No.:

DOB: 1985-3-15

Company:

Tel:

Occupation:

Email:

Entry Time: 2020/6/4 14:37:59

Mailing Address:

Resign Time: 2030/6/5 14:37:59

Administrator:

Remark:

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

- Configure password.

  Set password. For the second generation access controllers, set the personnel password; for other devices, set the card password. The new password must consist of 6 digits.

- Configure card.

🕮

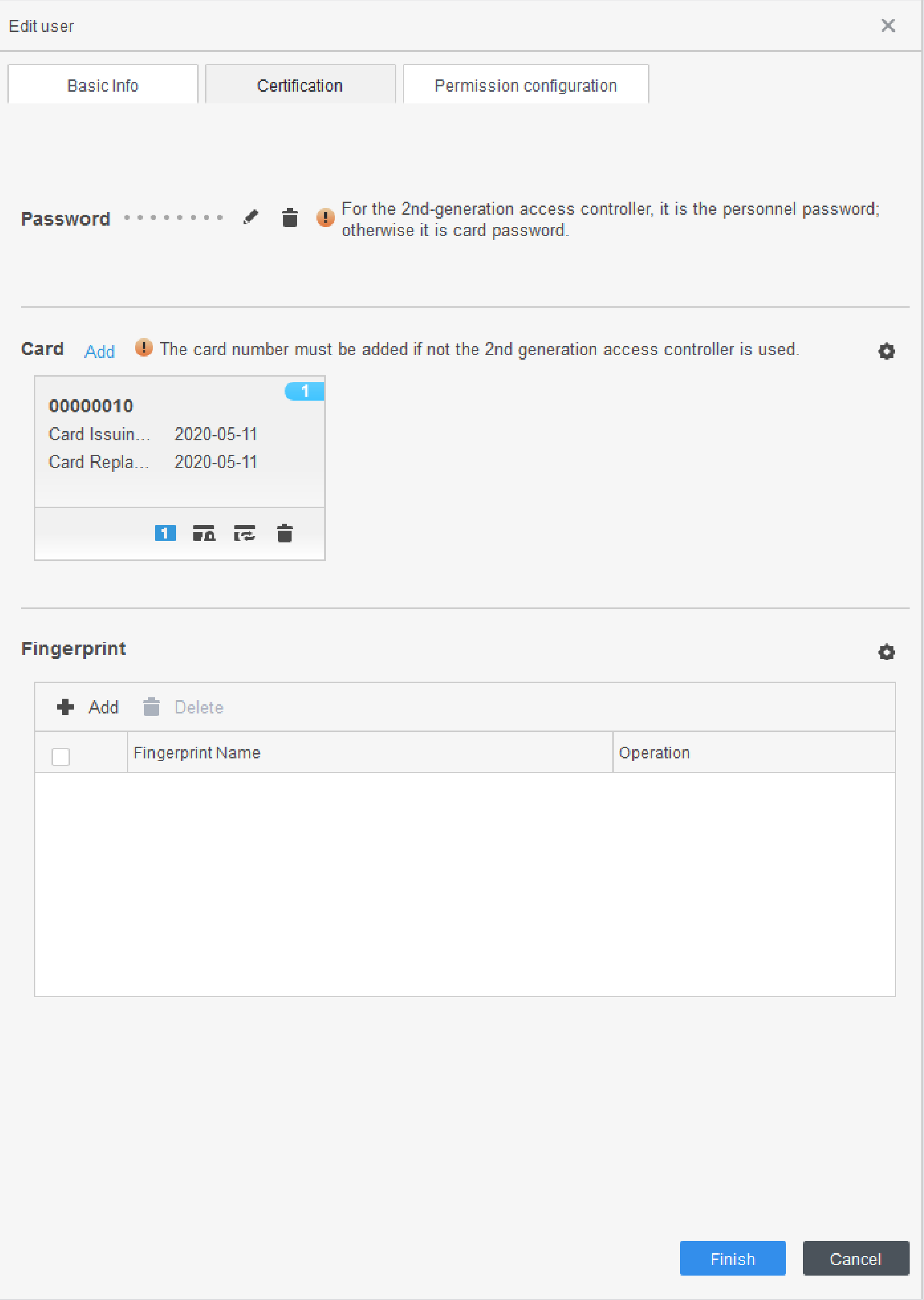
The card number can be read automatically or filled in manually. For automatically read, select a card reader, and then place the card on the card reader. The card number is read automatically after that.

1) Click ⚙ to select **Device** or **Card issuer** as card reader.
2) Add card. The card number must be added if the non-second generation access controller is used.
3) After adding, you can select the card as main card or duress card, or replace the card with new one, or delete the card.

- Configure fingerprint.

1) Click ⚙ to select **Device** or **Fingerprint Scanner** as fingerprint collector.
2) Add fingerprint. Click **Add Fingerprint** and press finger on the scanner three times continuously.

Figure 4-7 Configure certification



Edit user

Password •••••••• For the 2nd-generation access controller, it is the personnel password; otherwise it is card password.

Card Add The card number must be added if not the 2nd generation access controller is used.

00000010
Card Issuin... 2020-05-11
Card Repla... 2020-05-11

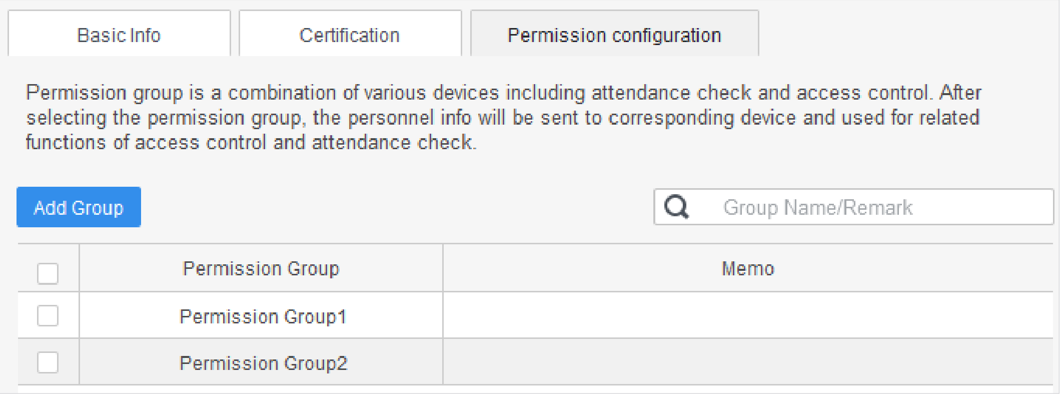
Fingerprint

□	Fingerprint Name	Operation

Step 5 Configure permission for the user.

For details, see "4.4 Permission Configuration".

Figure 4-8 Permission configuration



Permission group is a combination of various devices including attendance check and access control. After selecting the permission group, the personnel info will be sent to corresponding device and used for related functions of access control and attendance check.

□	Permission Group	Memo
□	Permission Group1	
□	Permission Group2	

Step 6 Click **Finish**.

4.3.2.2 Batch Add

You can add users in batches.

Step 1 Log in to SmartPSS AC.

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

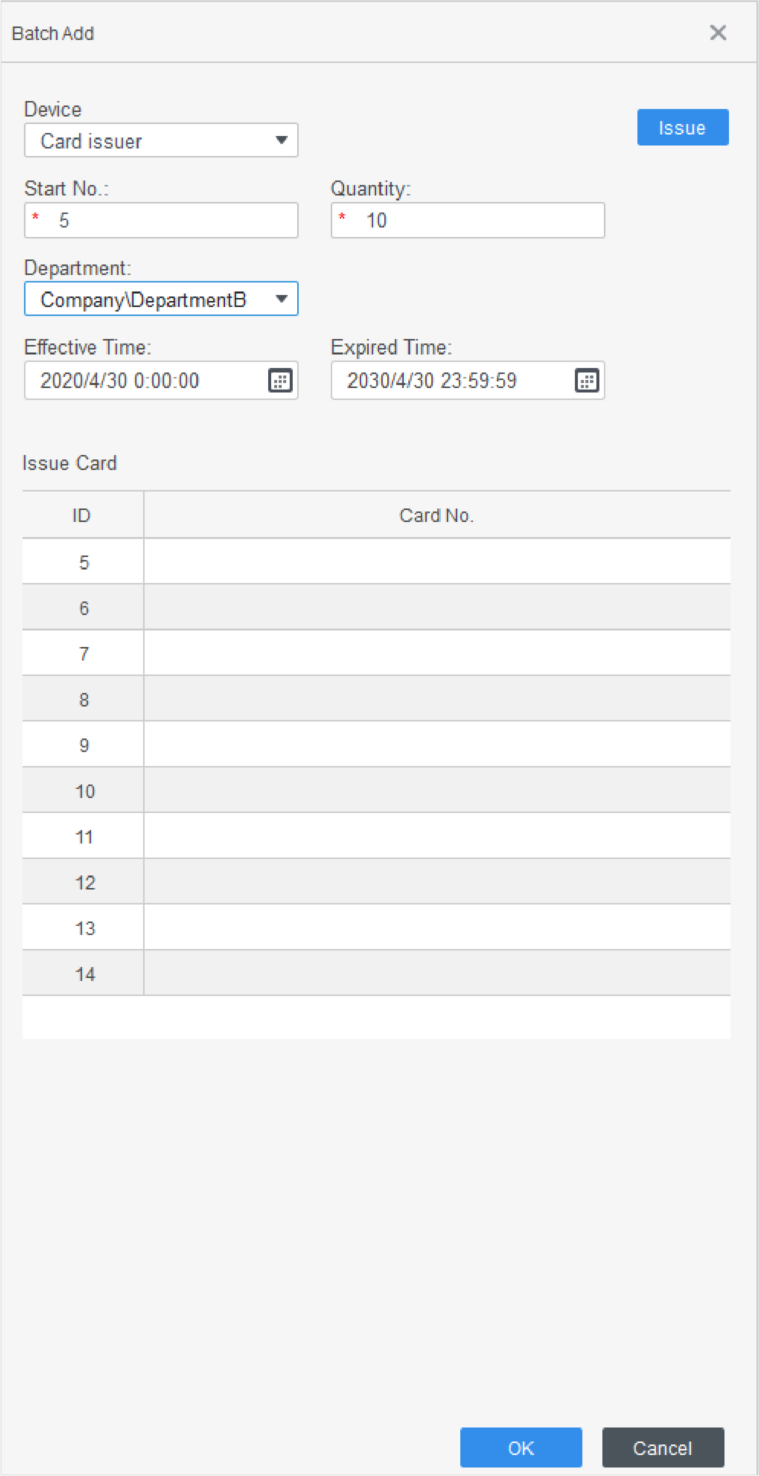
Step 3 Select card reader and the department of user. Set the start number, card quantity, effective time and expired time of card.

Step 4 Click **Issue** to start issuing cards**.**

The card number will be read automatically.

Step 5 Click **Stop** after issuing card, and then click **OK**.

Figure 4-9 Add user in batches



Batch Add

Device: Card issuer

Start No.: * 5

Quantity: * 10

Department: Company\DepartmentB

Effective Time: 2020/4/30 0:00:00

Expired Time: 2030/4/30 23:59:59

Issue Card

ID	Card No.
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	

Step 6 In the list of user, click ✎ to modify information or add details of users.

4.3.2.3 Extracting User from Devices

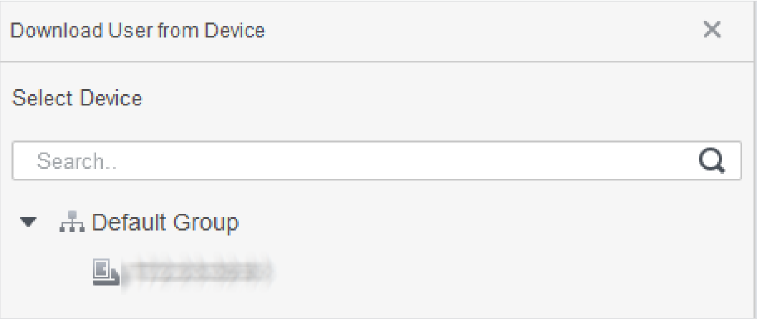
You can extract user information from devices.

Step 1 Log in to SmartPSS AC.

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

Step 3 Search and select the target device, and then click **OK**.

Figure 4-10 Devices with user information



Step 4 Select users as needed, and click **Extract**.

Step 5 In the list of user, click ✎ to modify information or add details of user.

4.3.2.4 Importing User

You can import users locally.

Step 1 Log in to SmartPSS AC.

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

Step 3 Import user information according to instructions.

4.3.3 Issuing Card in Batches

You can issue cards to user who have been added but have no card.

Step 1 Log in to SmartPSS AC.

Step 2 Select **Personnel Manager > User**.

Step 3 Select users as needed and then click **Batch Issue Card**.

Step 4 Issue card in batches. Card No. can be auto read by card reader or entered manually.

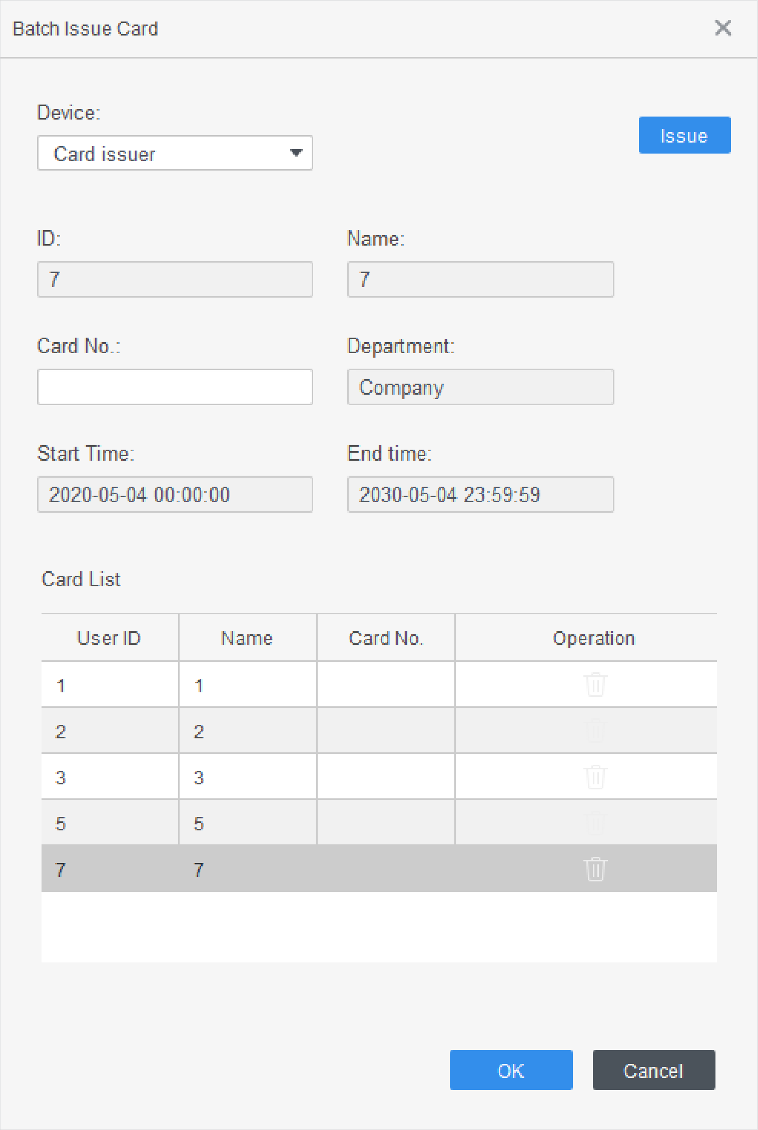
- Auto read

1) Select card reading device, and then click **Issue**.
2) According to the card list, put the cards of the corresponding user on card reader in sequence, and then the system will auto read the card number.
3) Modify user info, such as start time and end time for card validation.

- Enter manually

1) Select user in card list and enter the corresponding card number.
2) Modify user info, such as start time and end time for card validation.

Figure 4-11 Issue card in batches



Device: Card issuer

ID: 7

Name: 7

Card No.:

Department: Company

Start Time: 2020-05-04 00:00:00

End time: 2030-05-04 23:59:59

Card List

User ID	Name	Card No.	Operation
1	1		🗑
2	2		🗑
3	3		🗑
5	5		🗑
7	7		🗑

Step 5 Click **OK**.

4.3.4 Exporting User Information

You can export user information.

Step 1 Log in to SmartPSS AC.

Step 2 Select **Personnel Manager** > **User**.

Step 3 Select the user information which needs to be exported, and then click **Export** to export all user information to local.

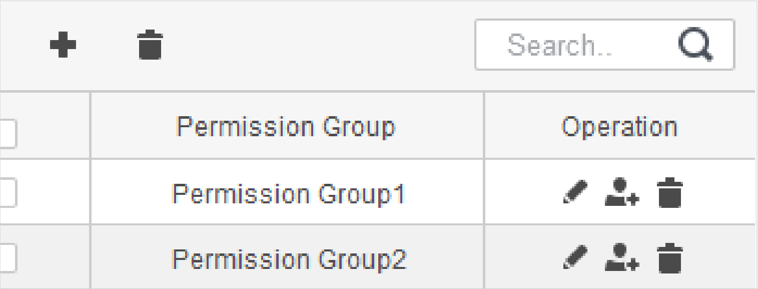
4.4 Permission Configuration

4.4.1 Adding Permission Group

Step 1 Log in to SmartPSS AC.

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

Figure 4-12 Permission group list



	Permission Group	Operation
□	Permission Group1	✎ 👤+ 🗑
□	Permission Group2	✎ 👤+ 🗑

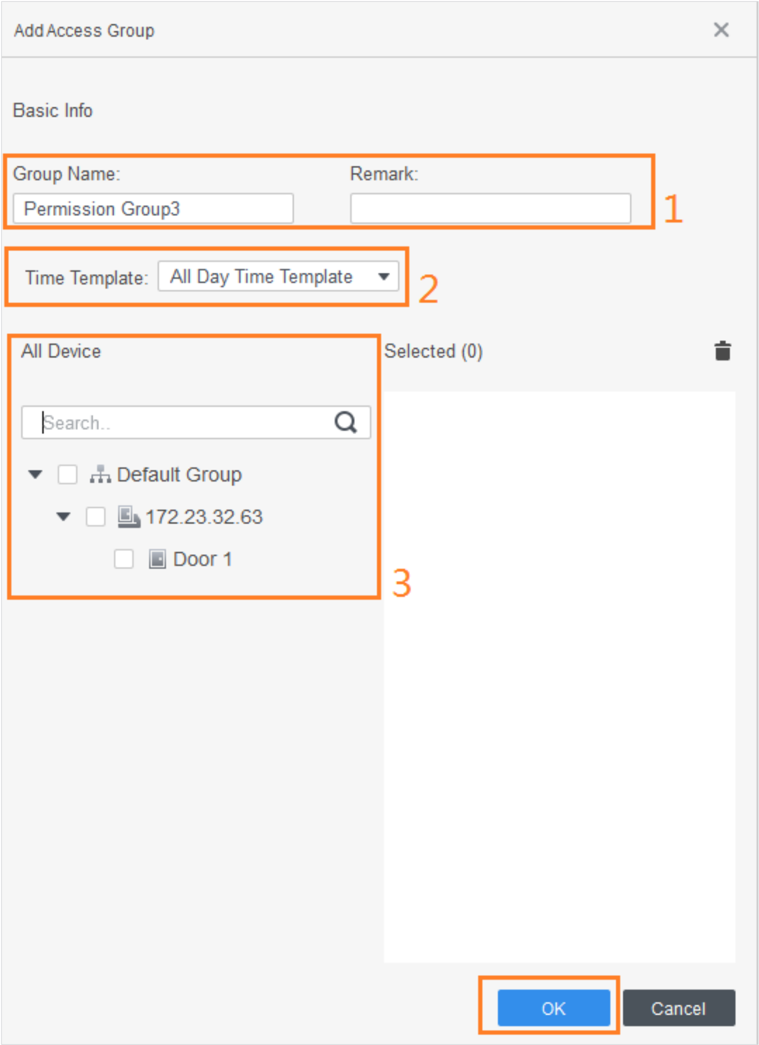
Step 3 Click ✚ to add a permission group.

Step 4 Set permission parameters.

1) Enter group name and remark.
2) Select the needed time template.

   For details of time template setting, see SmartPSS AC user manual.
3) Select the corresponding device, such as door 1.

Figure 4-13 Add permission group



Basic Info

Group Name: Permission Group3

Remark:

Time Template: All Day Time Template

All Device

- □ Default Group
  - □ 172.23.32.63
    - □ Door 1

Step 5 Click **OK**.

On the **Permission Group List** interface, you can do:

- Click 🗑 to delete group.
- Click ✎ to modify group info.
- Double-click permission group name to view group info.

4.4.2 Configuring Permission

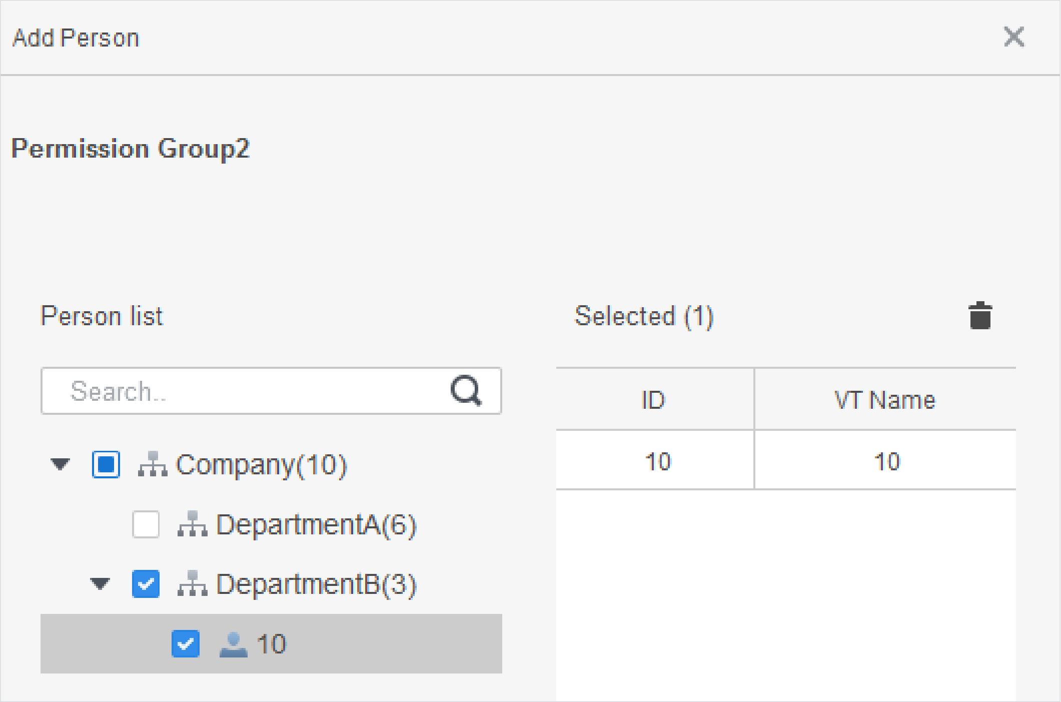
The method to configure permission for department and for users is similar. This section takes users as an example.

Step 1 Log in to SmartPSS AC.

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

Step 3 Select the target permission group, and then click 👤+.

Figure 4-14 Configure permission



Add Person ✕

Permission Group2

Person list

Search..

▾ ■ Company(10)
□ DepartmentA(6)
▾ ☑ DepartmentB(3)
☑ 10

Selected (1) 🗑

ID	VT Name
10	10

Step 4 Select the user need to be configured permission.

Step 5 Click **OK**.

4.5 Access Management

4.5.1 Remotely Opening and Closing Door

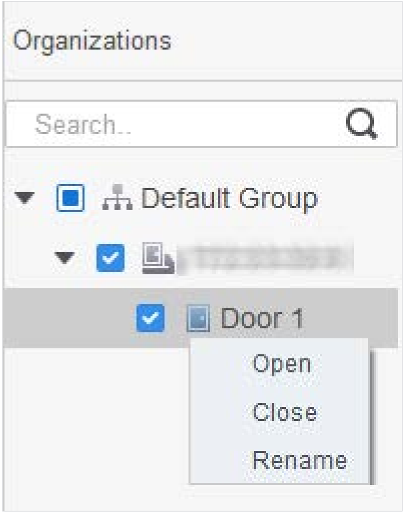
After access configuration, you can remotely control door through SmartPSS AC.

Step 1 Click **Access Manager** on the homepage. (Or click **Access Guide >**).

Step 2 Remotely control the door. There are two methods.

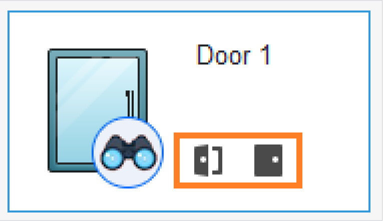
- Method 1: Select the door, right click and select **Open**.

Figure 4-15 Remotely control (method 1)



- Method 2: Click or to open or close the door.

Figure 4-16 Remotely control (method 2)



Step 3 View door status by **Event Info** list.

- Event filtering: Select the event type in the **Event Info**, and the event list displays events of the selected types. For example, select **Alarm**, and the event list only displays alarm events.
- Event refresh locking: Click to the right of **Event Info** to lock or unlock the event list, and then the real-time events cannot be viewed.
- Event deleting: Click to the right of **Event Info** to clear all events in the event list.

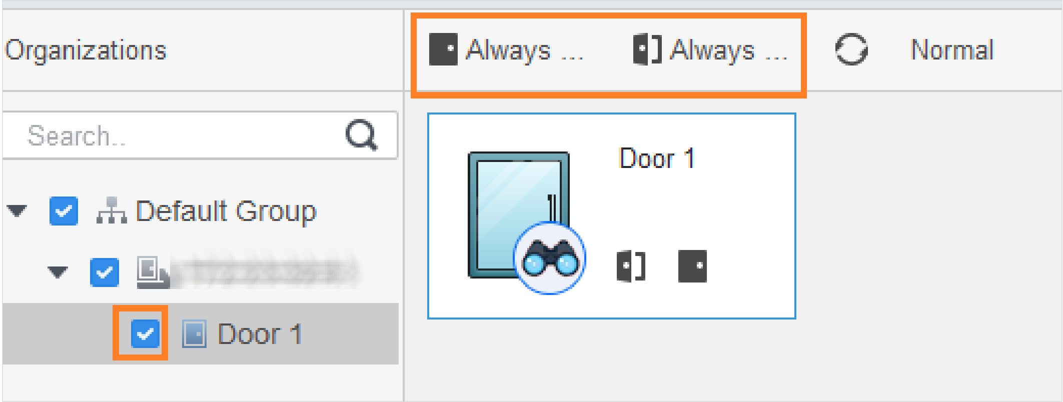
4.5.2 Setting Always Open and Always Close

After setting always open or always close, the door is open or closed all the time and cannot be controlled manually. If you want to manually control the door again, click **Normal** to reset the door status.

Step 1 Click **Access Manager** on the homepage. (Or click **Access Guide** >).

Step 2 Select the needed door, and then click **Always Open** or **Always Close**.

Figure 4-17 Set always open or always close



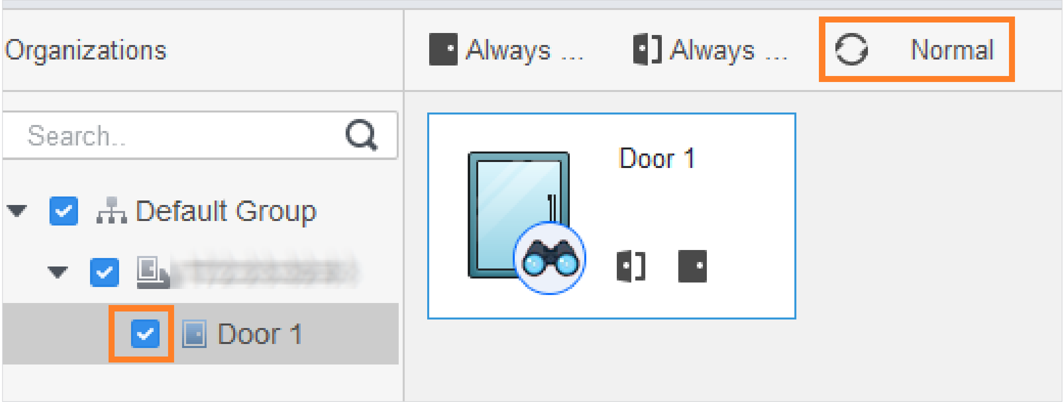
4.5.3 Resetting Door Status

Click **Normal** to reset the door status, if you want to manually control the door again when you have clicked **Always Open** or **Always Close**.

Step 1 Click **Access Manager** on the homepage. (Or click **Access Guide** >).

Step 2 Select the needed door, and then click **Normal**. And then follow the on-screen instructions to operate.

Figure 4-18 Reset door status



4.6 Attendance Management

You can set attendance time, add attendance shifts, personnel scheduling, process attendance, manage attendance statistics, search reports, add holidays, and configure attendance.

4.6.1 Report Search

You can view the normal attendance, attendance abnormality, overtime attendance and staff information here. And the statistics can be exported as reports.

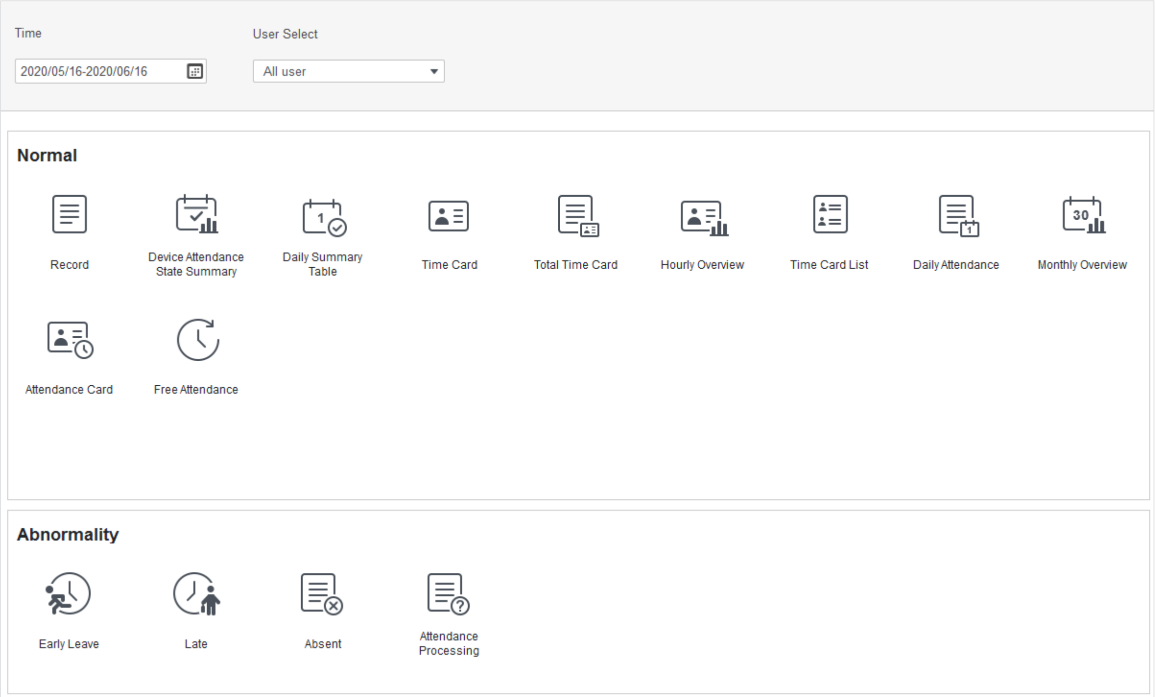
Step 1 Log in to SmartPSS AC.

Step 2 Click **Attendance Manager**.

Step 3 On the left menu bar, click .

Step 4 Select the time, department and statistic type, to view the corresponding reports.

Figure 4-19 Report search

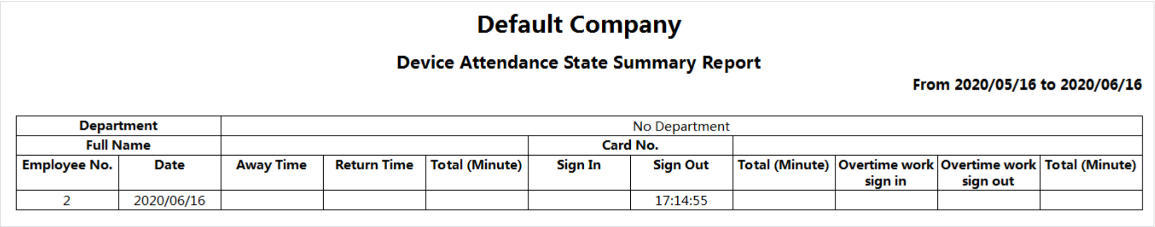


Time: 2020/05/16-2020/06/16

User Select: All user

After the device is added and authenticated on the SmartPSS AC platform, the corresponding attendance status will be reported to the platform, and the platform will generate the corresponding attendance status report.

Figure 4-20 Attendance status report of the device



Default Company

Device Attendance State Summary Report

From 2020/05/16 to 2020/06/16

Department		No Department								
Full Name					**Card No.**					
Employee No.	**Date**	**Away Time**	**Return Time**	**Total (Minute)**	**Sign In**	**Sign Out**	**Total (Minute)**	**Overtime work sign in**	**Overtime work sign out**	**Total (Minute)**
2	2020/06/16					17:14:55				

4.6.2 Other Configurations

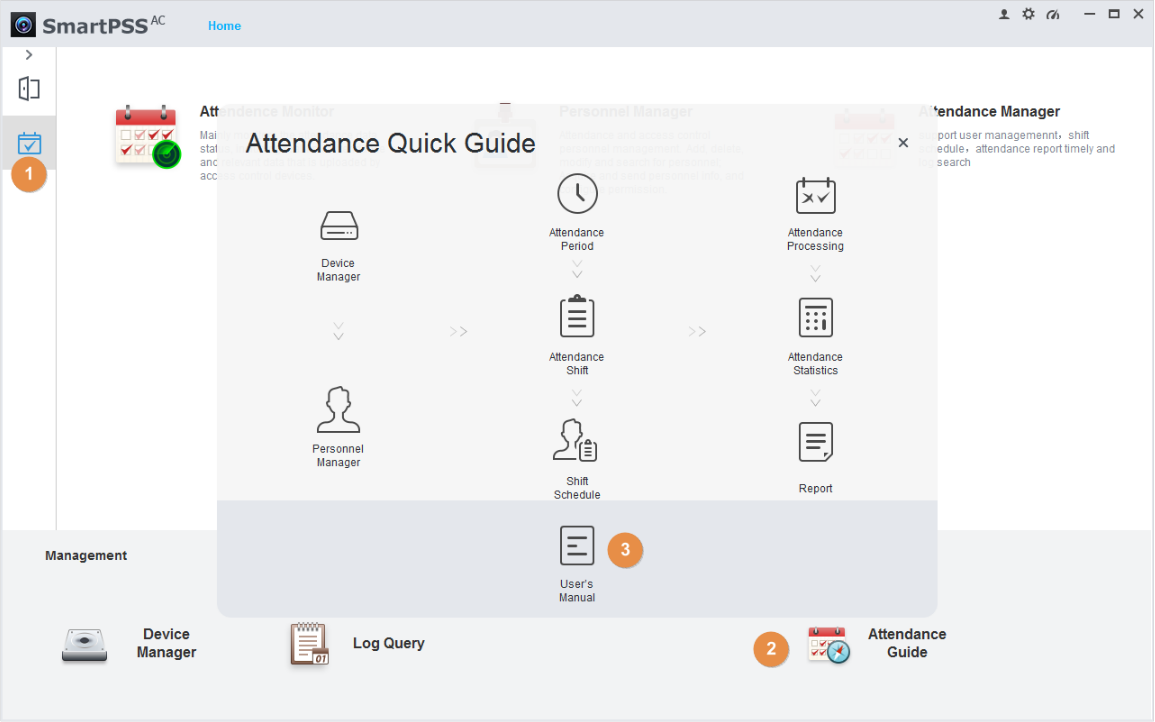
For other configurations such as attendance periods, attendance shifts, personnel scheduling, attendance processing and attendance statistics, adding holidays and attendance configurations, refer to the SmartPSS AC user's manual.

Step 1 Log in to SmartPSS AC.

Step 2 Click ☑ on the left menu.

Step 3 Click **Attendance Guide** at the lower-right corner.

Figure 4-21 View SmartPSS AC user's manual



5 FAQ

1 **The access controller fails to start after power-on.**

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

2 **Faces cannot be recognized after the access controller powers on.**

Make sure that **Face** is selected in the unlock mode. See "2.8.2 Unlock".

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

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

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

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

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

Check whether names of XML files and titles of tables were modified because the system will identify the files through their titles.

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

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

Appendix 1 Notes of Face Recording/Comparison

Before Registration

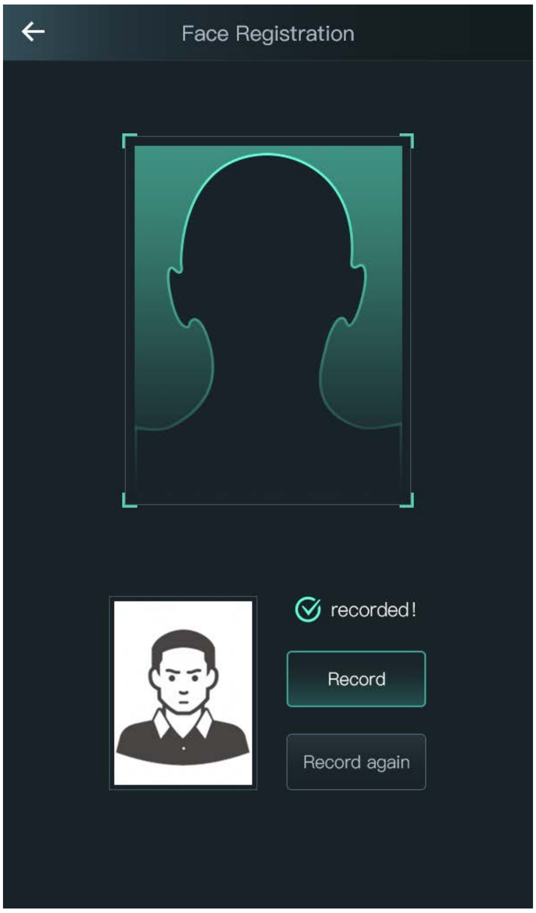
- Glasses, hats, and beards might influence face recognition performance.
- Do not cover your eyebrows when wearing hats.
- Do not change your beard style greatly if you will use the device; otherwise face recognition might fail.
- Keep your face clean.
- Keep the device at least two meters away from light source and at least three meters away from windows or doors; otherwise backlight and direct sunlight might influence face recognition performance of the device.

During Registration

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

Make your head center on the photo capture frame. A picture of your face will be captured automatically.

Appendix Figure 1-1 Registration



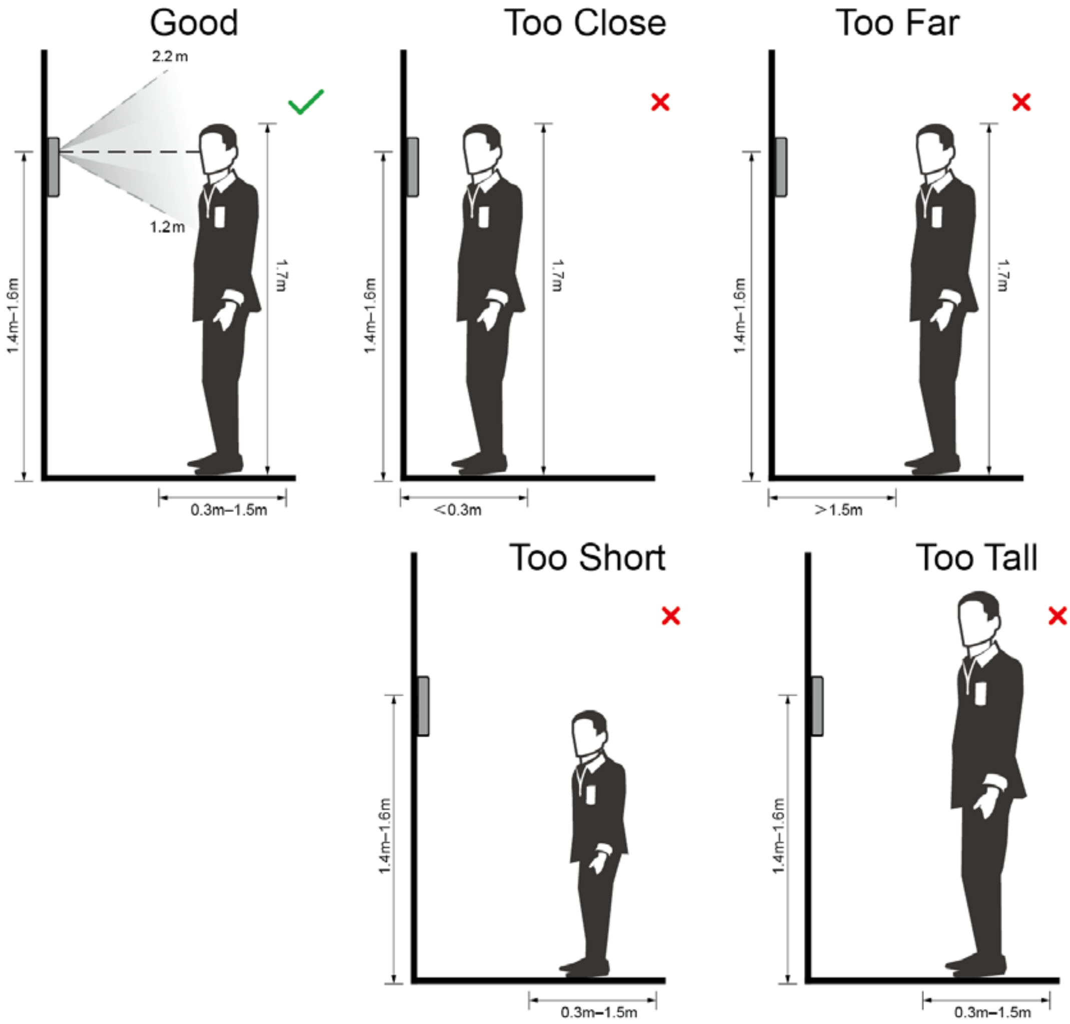
- Do not shake your head or body, otherwise the registration might fail.

- Avoid two faces appear in the capture frame at the same time.

Face Position

If your face is not at the appropriate position, face recognition effect might be influenced.

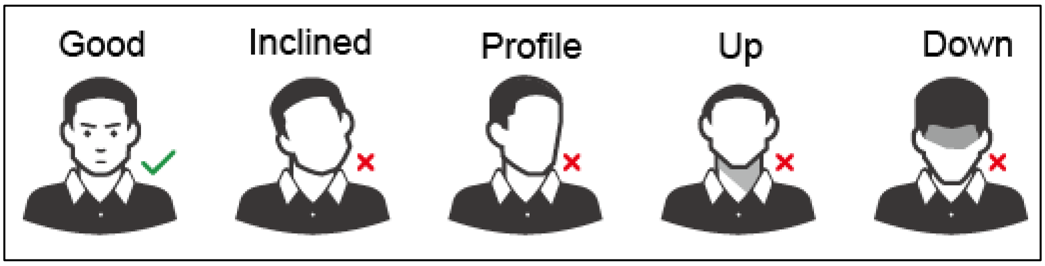
Appendix Figure 1-2 Appropriate face position



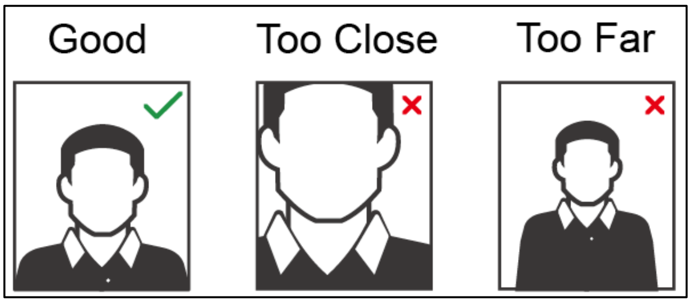
Requirements of Faces

- Make sure that the face is clean and forehead is not covered by hair.
- Do not wear glasses, hats, heavy beards, or other face ornaments that influence face image recording.
- With eyes open, without facial expressions, and make your face toward the center of camera.
- When recording your face or during face recognition, do not keep your face too close to or too far from the camera.

Appendix Figure 1-3 Head position



Appendix Figure 1-4 Face distance



- When importing face images through the management platform, make sure that image resolution is within 150 × 300 to 600 × 1200; image pixels are more than 500 × 500; image size is less than 75 KB, and image name and person ID are the same.
- Make sure that the face takes up more than 1/3 but no more than 2/3 of the whole image area, and the aspect ratio does not exceed 1:2.

Appendix 2 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.