Face Recognition Access Controller

User's Manual

V1.0.0

Foreword

General

This manual introduces the functions and operations of the Face Recognition Access Controller (hereinafter referred to as the "Access Controller"). Read carefully before using the device, and keep the manual safe for future reference.

Safety Instructions

The following signal words might appear in the manual.

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

Revision History

Version	Revision Content	Release Time
V1.0.0	First Release.	June 2022

Privacy Protection Notice

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

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.

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

Important Safeguards and Warnings

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

Transportation Requirement

Transport, use and store the Device under allowed humidity and temperature conditions.

Storage Requirement

Store the Device under allowed humidity and temperature conditions.

Installation Requirements

 **WARNING**

- Do not connect the power adapter to the Device while the adapter is powered on.
- Strictly comply with the local electric safety code and standards. Make sure the ambient voltage is stable and meets the power supply requirements of the Device.
- Do not connect the Device to two or more kinds of power supplies, to avoid damage to the Device.
- Improper use of the battery might result in a fire or explosion.
- Please follow the electrical requirements to power the Device.
  - Following are the requirements for selecting a power adapter.
    - The power supply must conform to the requirements of IEC 60950-1 and IEC 62368-1 standards.
    - The voltage must meet the SELV (Safety Extra Low Voltage) requirements and not exceed ES-1 standards.
    - When the power of the device does not exceed 100 W, the power supply must meet LPS requirements and be no higher than PS2.
  - We recommend using the power adapter provided with the Device.
  - When selecting the power adapter, the power supply requirements (such as rated voltage) are subject to the Device label.

- Personnel working at heights must take all necessary measures to ensure personal safety including wearing a helmet and safety belts.
- Do not place the Device in a place exposed to sunlight or near heat sources.
- Keep the Device away from dampness, dust, and soot.
- Install the Device on a stable surface to prevent it from falling.
- Install the Device in a well-ventilated place, and do not block its ventilation.

- Use an adapter or cabinet power supply provided by the manufacturer.
- Use the power cords that are recommended for the region and conform to the rated power specifications.
- The Device is a class I electrical appliance. Make sure that the power supply of the Device is connected to a power socket with protective earthing.

Operation Requirements

- Check whether the power supply is correct before use.
- Ground the device to protective ground before you power it on.
- Do not unplug the power cord on the side of the Device while the adapter is powered on.
- Operate the Device within the rated range of power input and output.
- Use the Device under allowed humidity and temperature conditions.
- Do not drop or splash liquid onto the Device, and make sure that there is no object filled with liquid on the Device to prevent liquid from flowing into it.
- Do not disassemble the Device without professional instruction.
- This product is professional equipment.
- The Device is not suitable for use in locations where children are likely to be present.

Table of Contents

1 Overview

1.1 Introduction

The access controller is an access control panel that supports unlock through faces, passwords, cards, fingerprint, QR code, and their combinations. Based on the deep-learning algorithm, it features faster recognition and higher accuracy. It can work with management platform which meets various needs of customers.

1.2 Features

- 7" LCD with a resolution of 600 × 1024.
- 2-MP dual-lens CMOS camera.
- Supports 50,000 users, 50,000 faces, 50,000 passwords, 100,000 cards, 50 administrators, and 300,000 records.
- Multiple unlock methods including face, IC card, password and QR code.
- Recognizes faces 0.3 m to 3.0 m away (0.98 ft–9.84 ft), and detects persons between the height of 0.9 m and 2.4 m (2.95 ft–7.87 ft).
- Powered by the face recognition deep learning algorithm, the device can accurately locate over 360 key points on the face of a target.
- Faces can be recognized within 0.2 seconds, without need for the person to touch the device.
- Features face mask detection and safety helmet detection.
- Plays advertisements in video and image format.
- Supports extension modules for fingerprint, QR code and fingerprint + QR code.
- Recognizes up to 6 faces at the same time.

1.3 Application

It is widely used in parks, communities, business centers and factories, and ideal for places such as office buildings, government buildings, schools and stadiums.

Figure 1-1 Networking

2 Local Operations

2.1 Basic Configuration Procedure

Figure 2-1 Basic configuration procedure

2.2 Common Icons

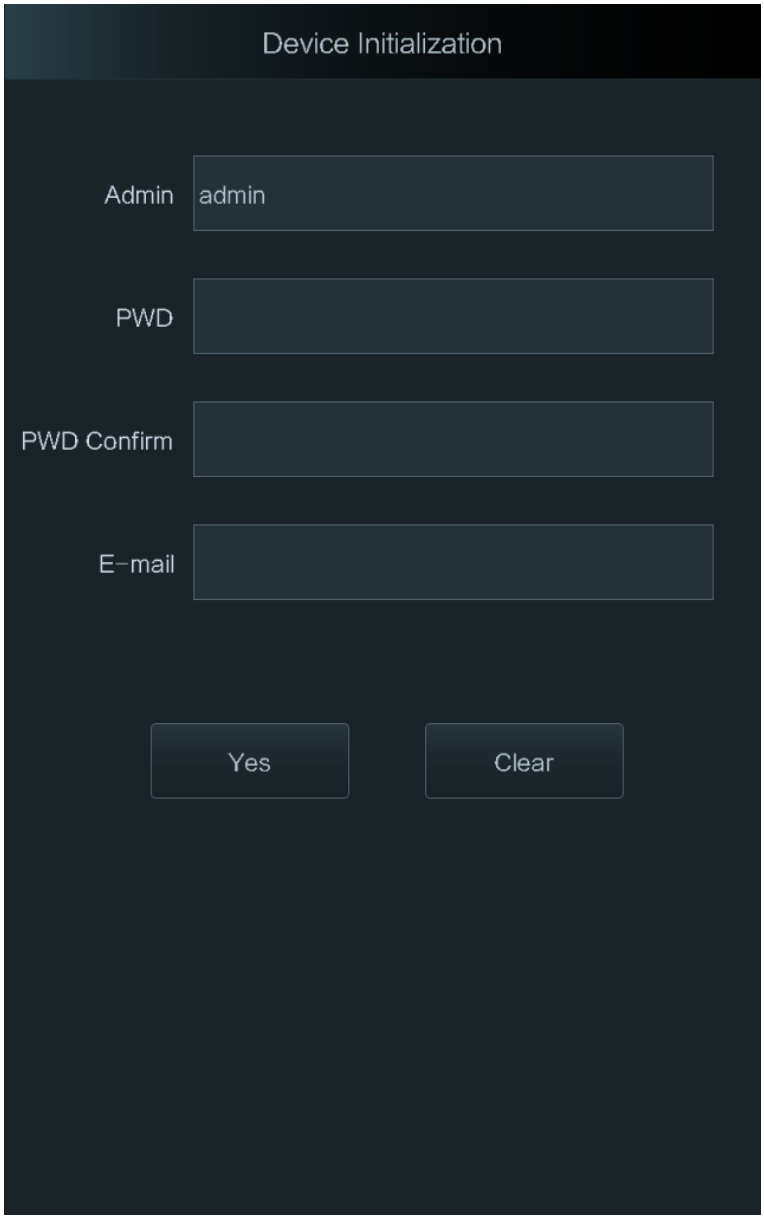
Table 2-1 Description of icons

Icon	Description
	Main menu icon.
	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.
	Turn on.
	Turn off.
	Delete
	Home screen
	Search

2.3 Initialization

For the first-time use or after restoring factory defaults, you need to set a password and email address for the admin account. You can use the admin account to log in to the main menu of the Access Controller and the webpage.

Figure 2-2 Initialization



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

You can unlock the door through faces, passwords, and QR code. You can also make calls through the intercom function.

- If there is no operation in 30 seconds, the access controller will go to the standby mode.
- This manual is for reference only. Slight differences might be found between the standby screen in this manual and the actual device.

Figure 2-3 Homepage

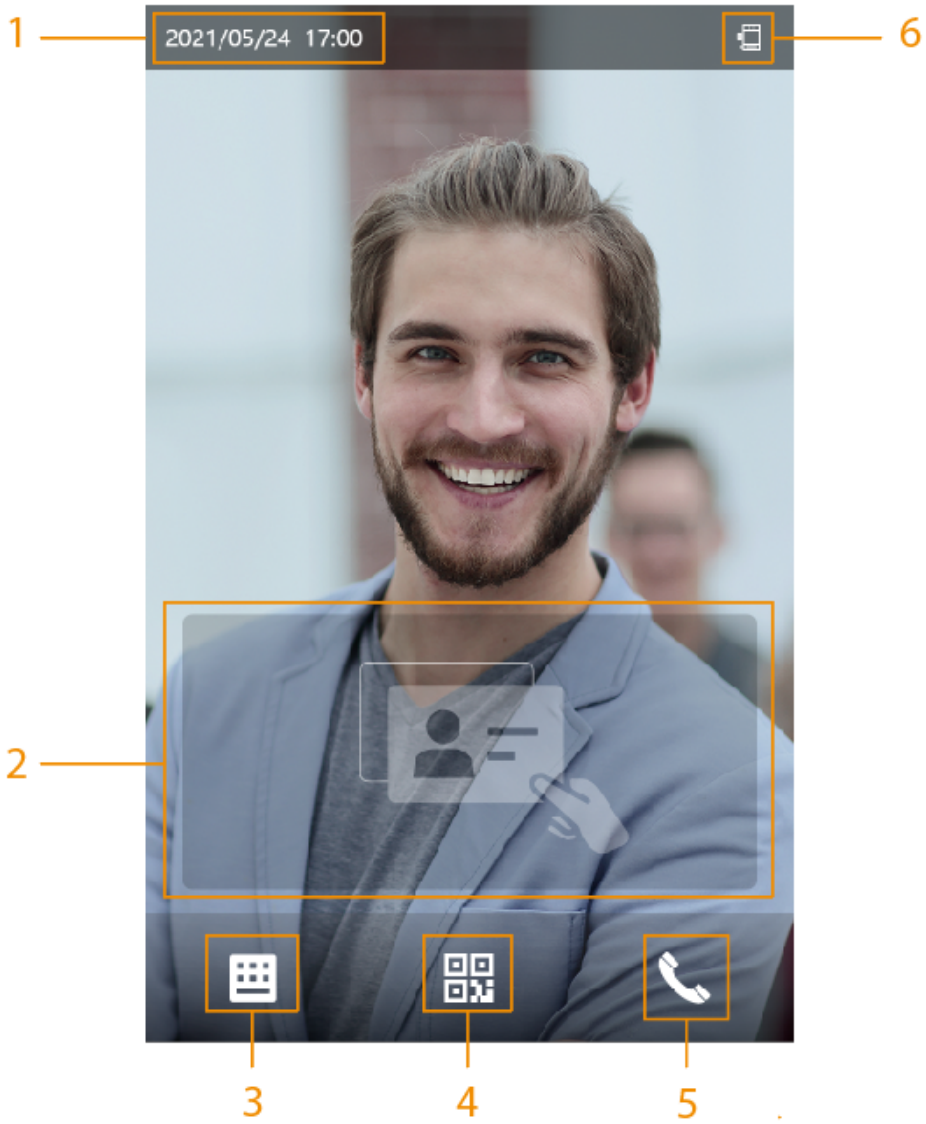


Table 2-2 Home screen description

No.	Name	Description
1	Date and time	Current date and time.
2	Card swiping area	Swipe card on this area.
3	Password	Enter user password or public password to unlock the door.
4	QR code	Tap the QR code icon and scan QR code to unlock the door. QR code icon is not available for the fingerprint model of Access Controller.

No.	Name	Description
5	Intercom	• When the Access Controller functions as a server, it can call the VTO and VTH. • When DSS functions as a server, The Access Controller can call the VTO, VTS and DSS. Tap the icon, enter the room number to call the home owner.
6	Status display	Displays status of Wi-Fi, network and USB.

2.5 Logging In

Log in to the main menu to configure the Access Controller. Only admin account and administrator account can enter the main menu of the Access Controller. For the first-time use, use the admin account to enter the main menu screen and then you can create the other administrator accounts.

Background Information

- admin account: Can log in to the main menu screen of the Access Controller, but has no door access permission.
- Administration account: Can log in to the main menu of the Access Controller and has door access permissions.

Procedure

Step 1 Press and hold the standby screen for 3 seconds, and then swipe left or right.

Step 2 select a verification method to enter the main menu.

- Face: Enter the main menu by face recognition.
- Fingerprint: Enter the main menu by using fingerprint.

  Fingerprint function is only available when the fingerprint module is mounted to the Access Controller.
- Card Punch: Enter the main menu by swiping card.
- PWD: Enter the user ID and password of the administrator account.
- admin: Enter the admin password to enter the main menu.

2.6 Network Communication

Configure the network, serial port and Wiegand port to connect the Access Controller to the network.

The serial port and the wiegand port might differ depending on models of Access Controller.

2.6.1 Configuring IP

Background Information

Set IP address for the Access Controller to connect it to the network. After that, you can log in to the webpage and the management platform to manage the Access Controller.

Procedure

Step 1 On the **Main Menu**, select **Connection** > **Network** > **IP Address**.

Step 2 Configure IP Address.

Figure 2-4 IP address configuration

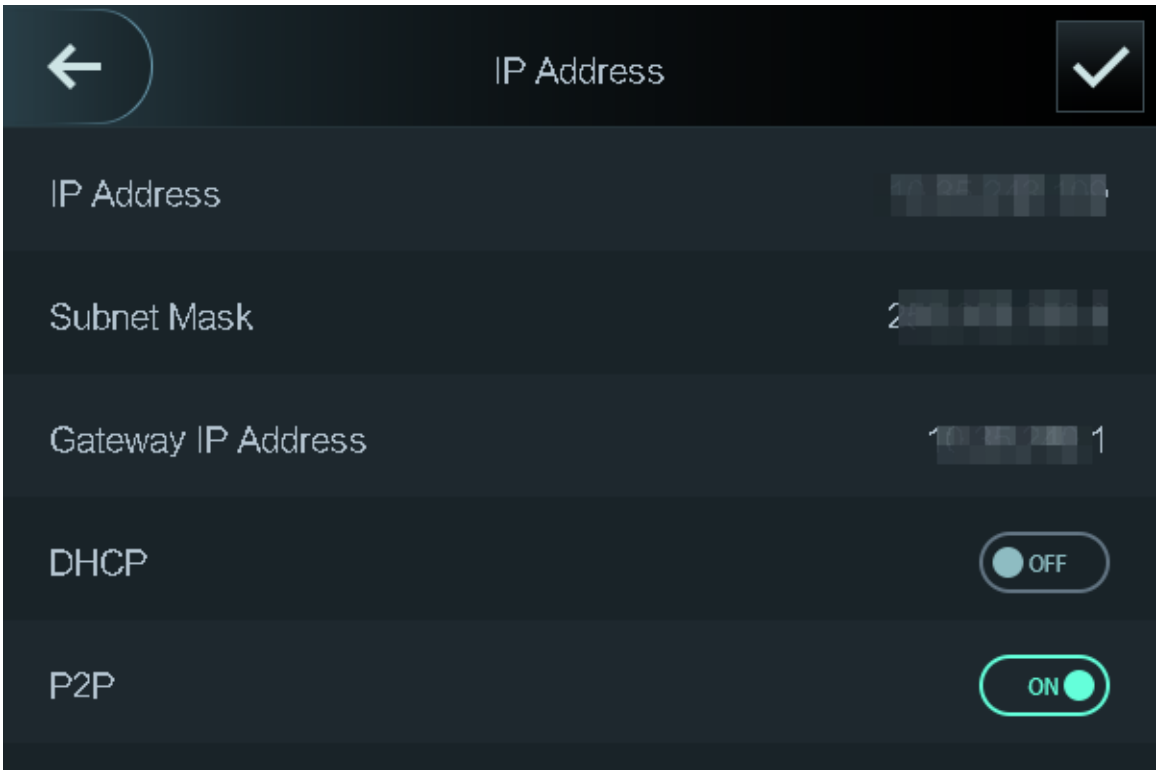


Table 2-3 IP configuration parameters

Parameter	Description
IP Address/Subnet Mask/Gateway Address	The IP address, subnet mask, and gateway IP address must be on the same network segment.
DHCP	It stands for Dynamic Host Configuration Protocol. When DHCP is turned on, the Access Controller will automatically be assigned with IP address, subnet mask, and gateway.
P2P	P2P (peer-to-peer) technology enables users to manage devices without applying for DDNS, setting port mapping or deploying transit server.

2.6.2 Active Register

Background Information

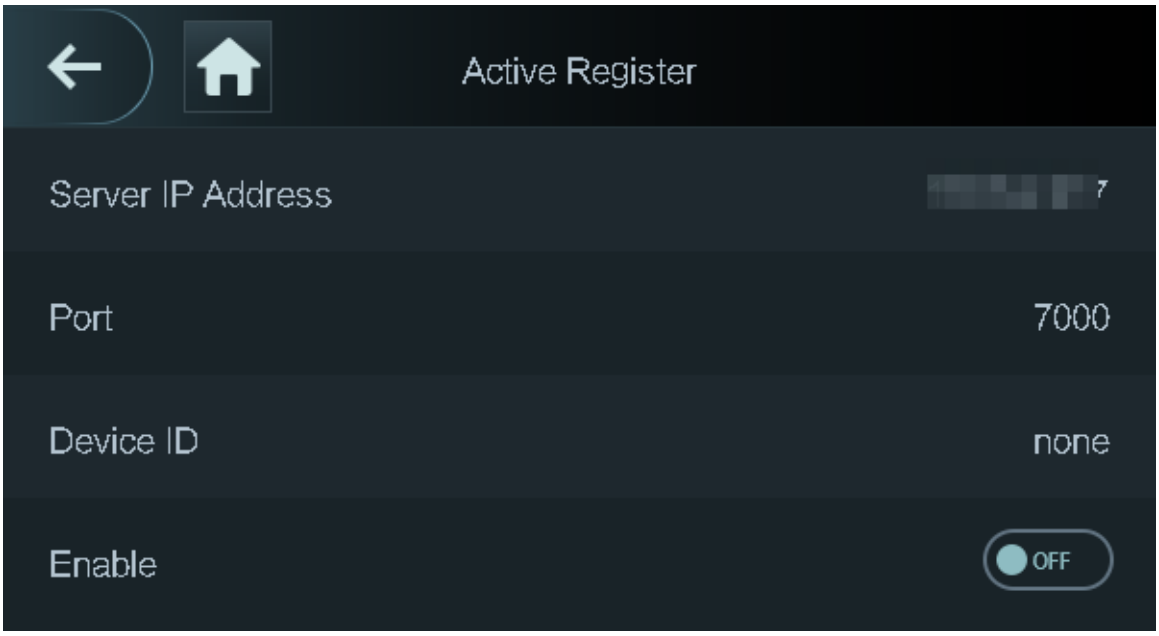
You can turn on the automatic registration function to access the Access Controller through the management platform.

The management platform can clear all personnel configurations and initialize the Access Controller. To avoid data loss, keep the management platform permissions properly.

Procedure

Step 1 On the **Main Menu**, select **Connection** > **Network** > **Active Register**.

Figure 2-5 Auto register



Step 2 Turn on the automatic registration function and set the parameters.

Table 2-4 Auto registration

Parameter	Description
Server Address	The IP address of the management platform.
Port	The port No. of the management platform.
Device ID	Enter the device ID (user defined). When you add the Access Controller to the management platform, the device ID on the management platform must conform to the defined device ID on the Access Controller.

Step 3 Enable the active register function.

2.6.3 Configuring Wi-Fi

Background Information

You can connect the Access Controller to the network through Wi-Fi network.

Wi-Fi function is only available for certain models of the Access Controller.

Procedure

Step 1 On the **Main Menu** , select **Connection Network** > **WiFi**.

Step 2 Turn on Wi-Fi.

Step 3 Tap to search available wireless networks.

Step 4 Select a wireless network and enter the password.

If no Wi-Fi is searched, tap **SSID** to enter the name of Wi-Fi.

Step 5 Tap

2.6.4 Configuring Serial Port

Procedure

Step 1 On the **Main Menu**, select **Connection** > **Serial Port**.

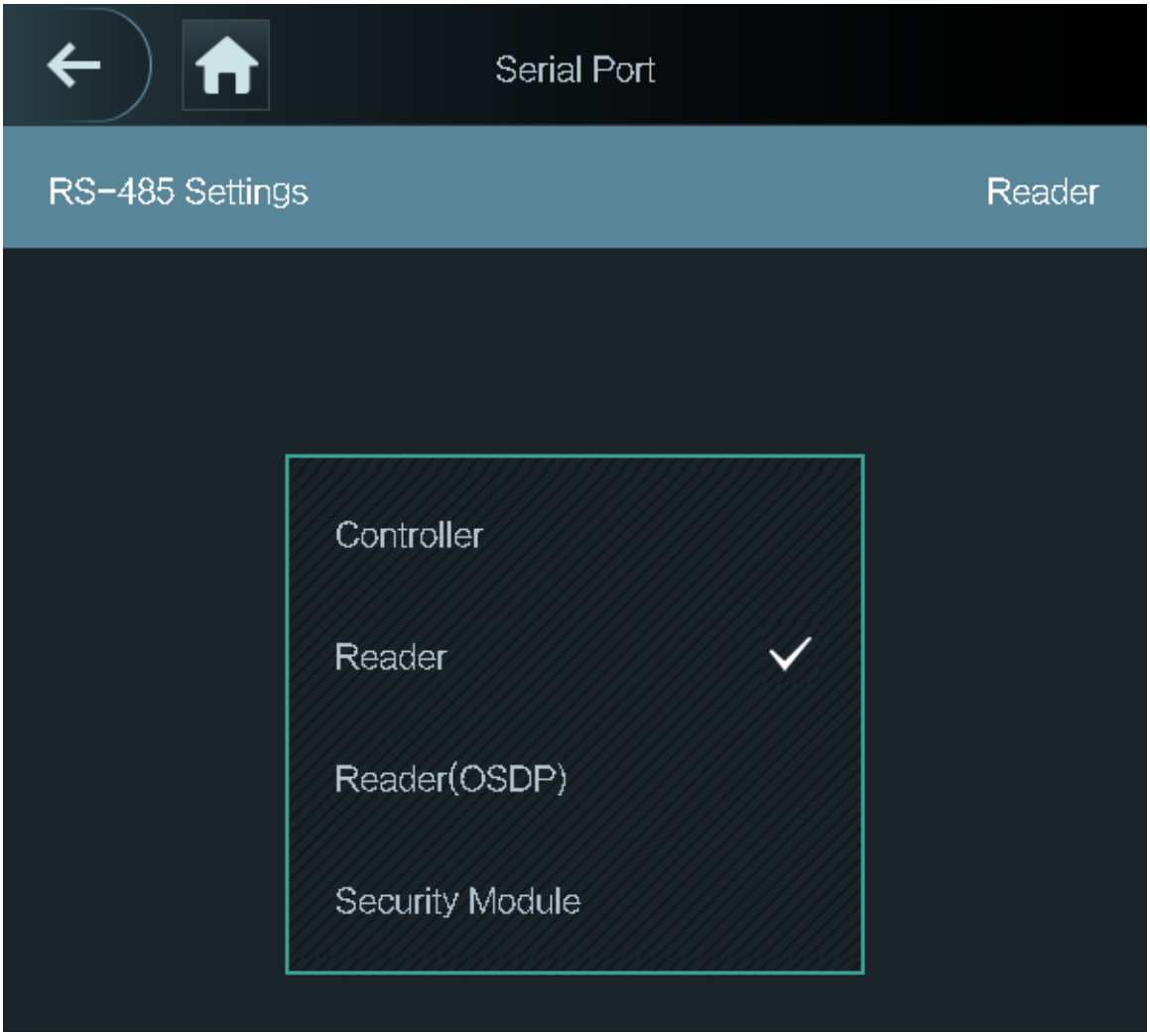
Step 2 Select a port type.

- Select **Reader** when the Access Controller connects to a card reader.
- Select **Controller** when the Access Controller functions as a card reader, and the Access Controller will send data to the Access Controller to control access.

  Output Data type:

  - Card: Outputs data based on card number when users swipe card to unlock door; outputs data based on user's first card number when they use other unlock methods.
  - No.: Outputs data based on the user ID.
- Select **Reader (OSDP)** when the Access Controller is connected to a card reader based on OSDP protocol.
- Security Module: When a security module is connected, the exit button, lock and fire alarm linkage will be not effective.

Figure 2-6 Serial port



2.6.5 Configuring Wiegand

Background Information

The access controller allows for both Wiegand input and Output mode.

Procedure

Step 1 On the **Main Menu**, select **Connection** > **Wiegand**.

Step 2 Select a Wiegand.

- Select **Wiegand Input** when you connect an external card reader to the Access Controller.
- Select **Wiegand Output** when the Access Controller functions as a card reader, and you need to connect it to a controller or another access terminal.

Figure 2-7 Wiegand output

Table 2-5 Description of Wiegand output

Parameter	Description
Wiegand Output Type	Select a Wiegand format to read card numbers or ID numbers. • **Wiegand26** : Reads three bytes or six digits. • **Wiegand34** : Reads four bytes or eight digits. • **Wiegand66** : Reads eight bytes or sixteen digits.
Pulse Width	Enter the pulse width and pulse interval of Wiegand output.
Pulse Interval	
Output Data Type	Select the type of output data. • **User ID** : Outputs data based on user ID. • **Card No.** : Outputs data based on user's first card number.

2.7 User Management

You can add new users, view user/admin list and edit user information.

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

2.7.1 Adding New Users

Procedure

Step 1 On the **Main Menu**, select **User** > **New User**.

Step 2 Configure the parameters on the interface.

Figure 2-8 New user

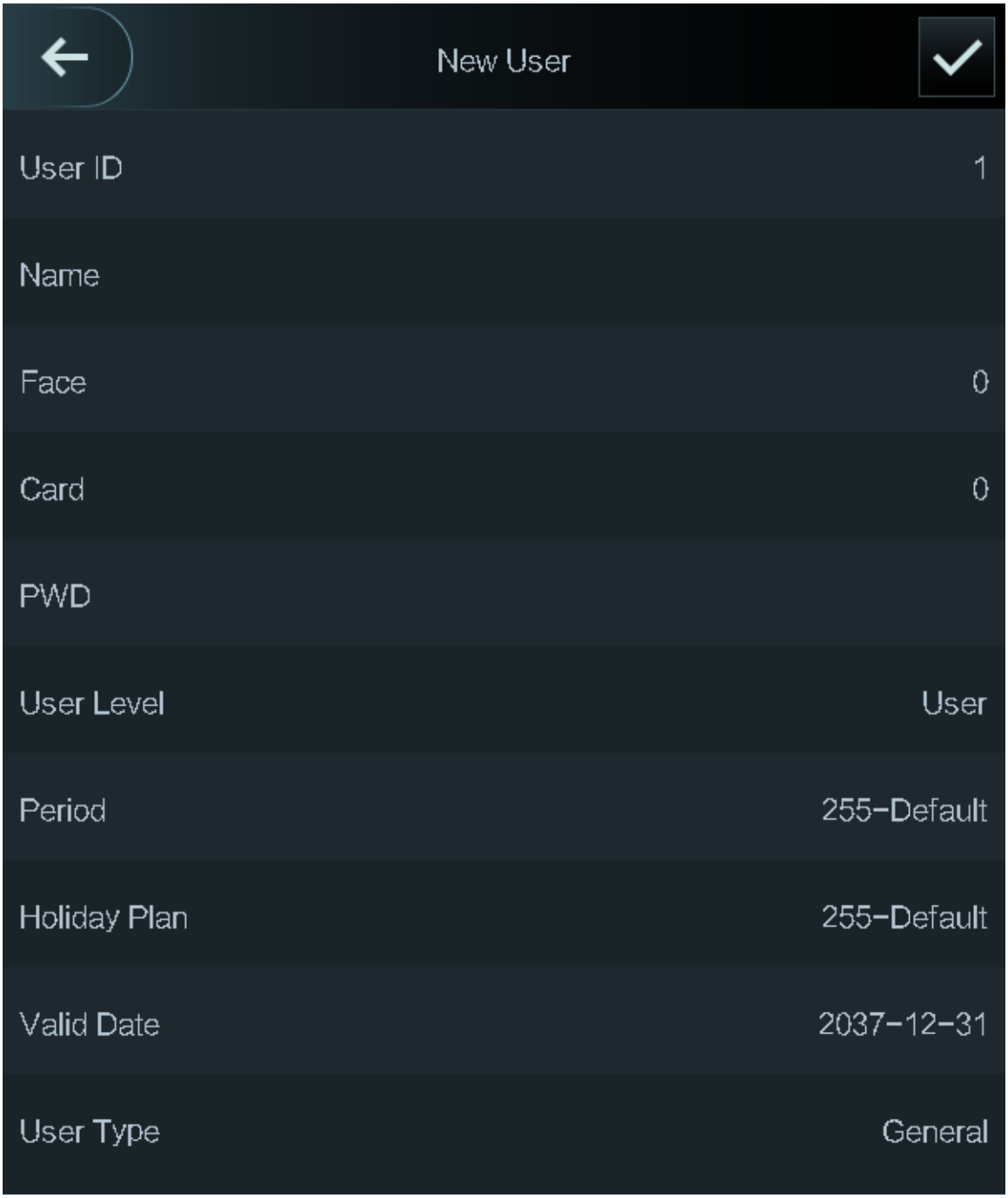


Table 2-6 Description of new user parameters

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 name with at most 32 characters (including numbers, symbols, and letters).

Parameter	Description
Face	Make sure that your face is centered on the image capturing frame, and an image of the face will be captured and analyzed automatically.
Card	A user can register five cards at most. 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. An alarm will be triggered if a duress card is used to unlock the door. Only certain models support card unlock.
PWD	Enter the user password. The maximum length of the password is 8 digits.
User Level	You can select a user level for new users. • **User** : Users only have door access permission. • **Admin** : Administrators can unlock the door and configure the access controller.
Period	People can unlock the door only during the defined period.
Holiday Plan	People can unlock the door only during the defined holiday plan.
Valid Date	Set a date on which the access permissions of the person will be expired.
User Type	• **General** : General users can unlock the door. • **Blocklist** : When users in the blocklist unlock the door, service personnel will receive a notification. • **Guest** : Guests can unlock the door within a defined period or for certain amount of times. After the defined period expires or the unlocking times runs out, they cannot unlock the door. • **Patrol** : Patrol users will have their attendance tracked, but they have no unlocking permissions. • **VIP** : When VIP unlock the door, service personnel will receive a notice. • **Others** : When they unlock the door, the door will stay unlocked for 5 more seconds. • Custom User 1/Custom User 2: Same with general users.

Step 3 Tap ☑ to save the configuration.

2.7.2 Viewing User Information

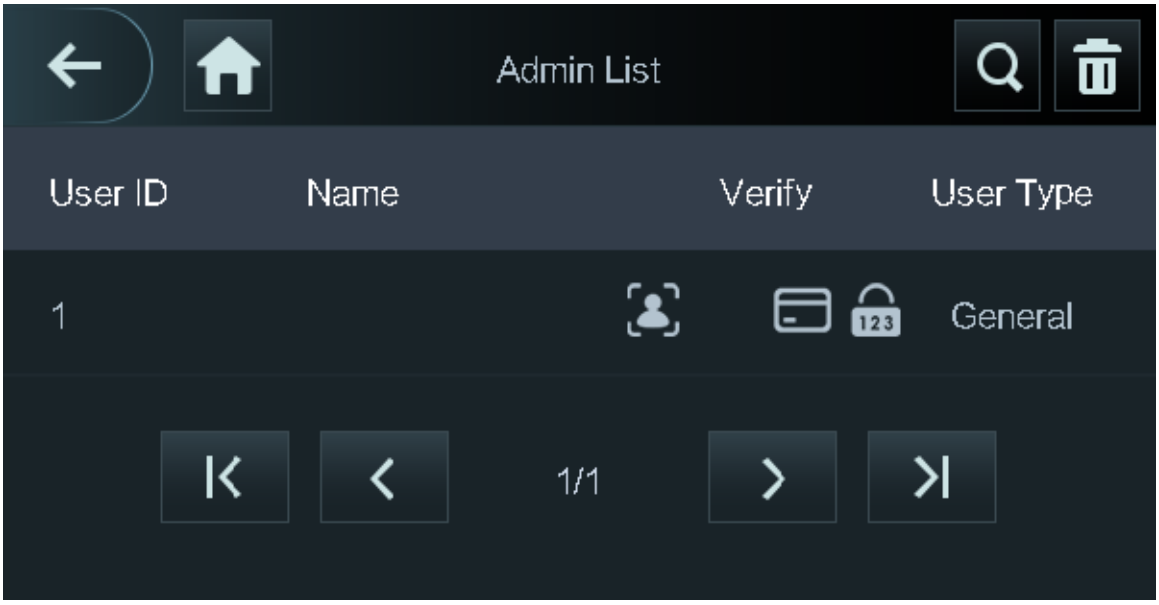
You can view user/admin list and edit user information.

Procedure

Step 1 On the **Main Menu**, select **User** > **User List**, or select **User** > **Admin List**.

Step 2 View all added users and admin accounts.

Figure 2-9 Admin list



- : Unlock through password.
- : Unlock through swiping card.
- : Unlock through face recognition.
- : Unlock through fingerprint.

Related Operations

On the **User** screen, you can manage the added users.

- Search for users: Tap and then enter the username.
- Edit users: Tap the user to edit user information.
- Delete users
  - Delete individually: Select a user, and then tap .
  - Delete in batches:
    - On the **User List** screen, tap to delete all users.
    - On the **Admin List** screen, tap to delete all admin users.

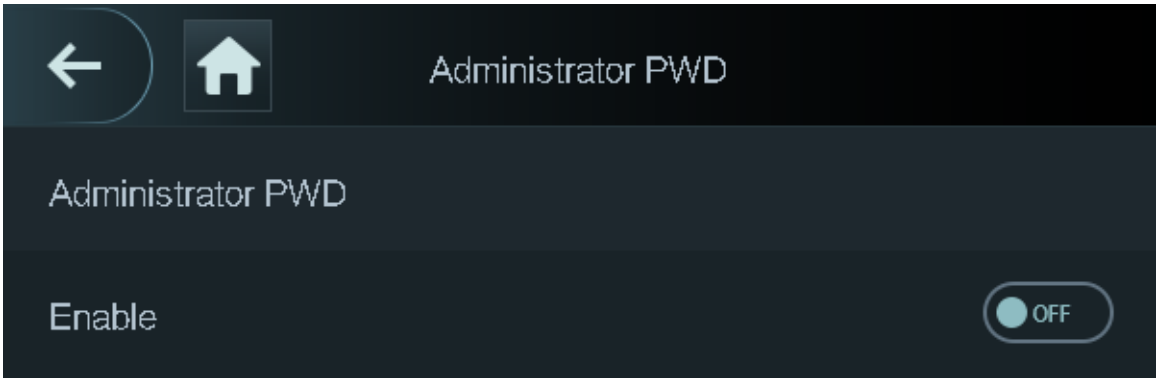
2.7.3 Configuring Administrator Password

You can unlock the door by only entering the admin password. Admin password is not limited by user types. Only one admin password is allowed for one device.

Procedure

Step 1 On the **Main Menu** screen, select **User** > **Administrator PWD**.

Figure 2-10 Set admin password



Step 2 Tap **Administrator PWD**, and then enter the administrator password.

Step 3 Tap ☑.

Step 4 Turn on the administrator function.

2.8 Access Management

You can configure door access parameters, such as unlocking modes, alarm linkage, door schedules. Unlock modes might differ depending on the actual product.

2.8.1 Configuring Unlock Combinations

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

Background Information

Fingerprint extension module must be mounted to the Access Controller if you want to unlock the door through fingerprint.

Procedure

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

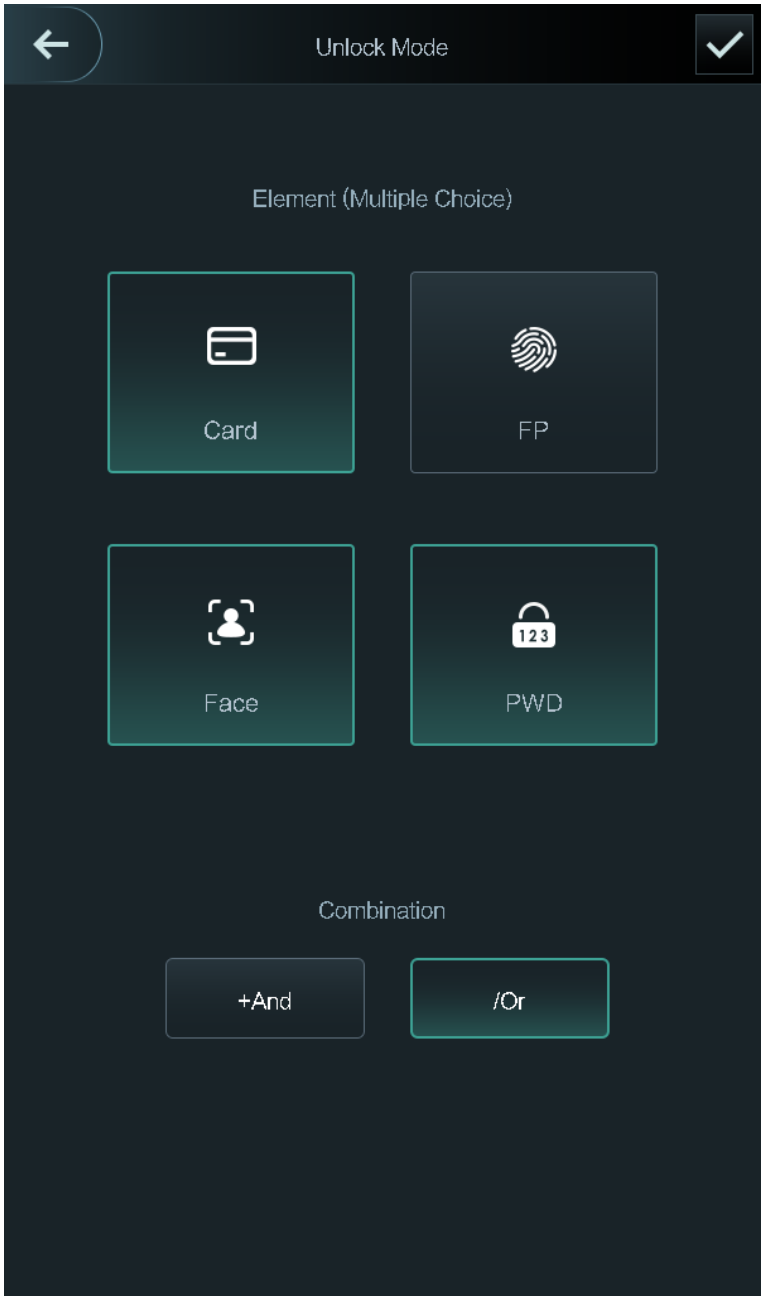
Step 2 Select unlocking methods.

To cancel your selection, tap the selected method again.

Step 3 Tap +**And** or **/Or** to configure combinations.

- **+And** : Verify all the selected unlocking methods to open the door.
- **/Or** : Verify one of the selected unlocking methods to open the door.

Figure 2-11 Element (multiple choice)



Step 4 Tap ☑ to save changes.

2.8.2 Configuring Alarm

Background Information

An alarm will be triggered when abnormal access events occur.

Procedure

Step 1 Select **Access** > **Alarm**.

Step 2 Enable the alarm type.

Figure 2-12 Alarm

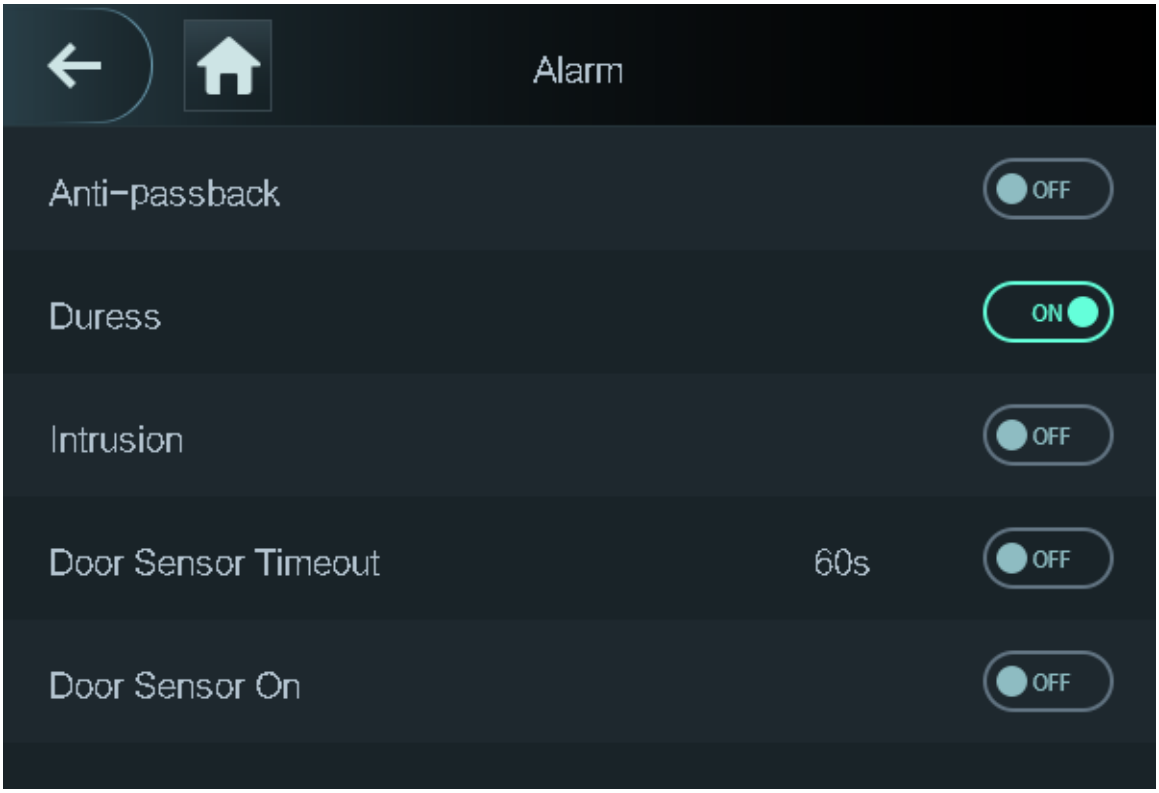


Table 2-7 Description of alarm parameters

Parameter	Description
Anti-passback	Users need to verify their identities both for entry and exit; otherwise an alarm will be triggered. It helps prevents a card holder from passing an access card back to another person so they gain entry. When anti-passback is enabled, the card holder must leave the secured area through an exit reader before system will grant another entry. • If a person enters after authorization and exits without authorization, an alarm will be triggered when they attempt to enter again, and access is denied at the same time. • If a person enters without authorization and exits after authorization, an alarm will be triggered when the they attempt to enter again, and access is denied at the same time.
Duress	An alarm will be triggered when a duress card, duress password or duress fingerprint is used to unlock the door.
Intrusion	When door sensor is enabled, an intrusion alarm will be triggered if the door is opened abnormally.
Door Sensor Timeout	A timeout alarm will be triggered if the door remains unlocked longer than the defined door sensor timeout, which ranges from 1 to 9999 seconds.

Parameter	Description
Door Sensor On	Intrusion and timeout alarms can be triggered only after door sensor is enabled.

2.8.3 Configuring Door Status

Procedure

Step 1 On the **Main Menu** screen, select **Access** > **Door Status**.

Step 2 Set door status.

- **NO** : The door remains unlocked all the time.
- **NC** : The door remains locked all the time.
- **Normal** : If **Normal** is selected, the door will be unlocked and locked according to your settings.

2.8.4 Configuring Lock Holding Time

Background Information

After a person is granted access, the door will remain unlocked for a defined time for them to pass through.

Procedure

Step 1 On the **Main Menu**, select **Access** > **Lock Holding Time.**

Step 2 Enter the unlock duration.

Step 3 Tap ☑ to save changes.

2.9 System

2.9.1 Configuring Time

Background Information

Configure system time, such as date, time, and NTP.

Procedure

Step 1 On the **Main Menu**, select **System** > **Time**.

Step 2 Configure system time.

Figure 2-13 Time

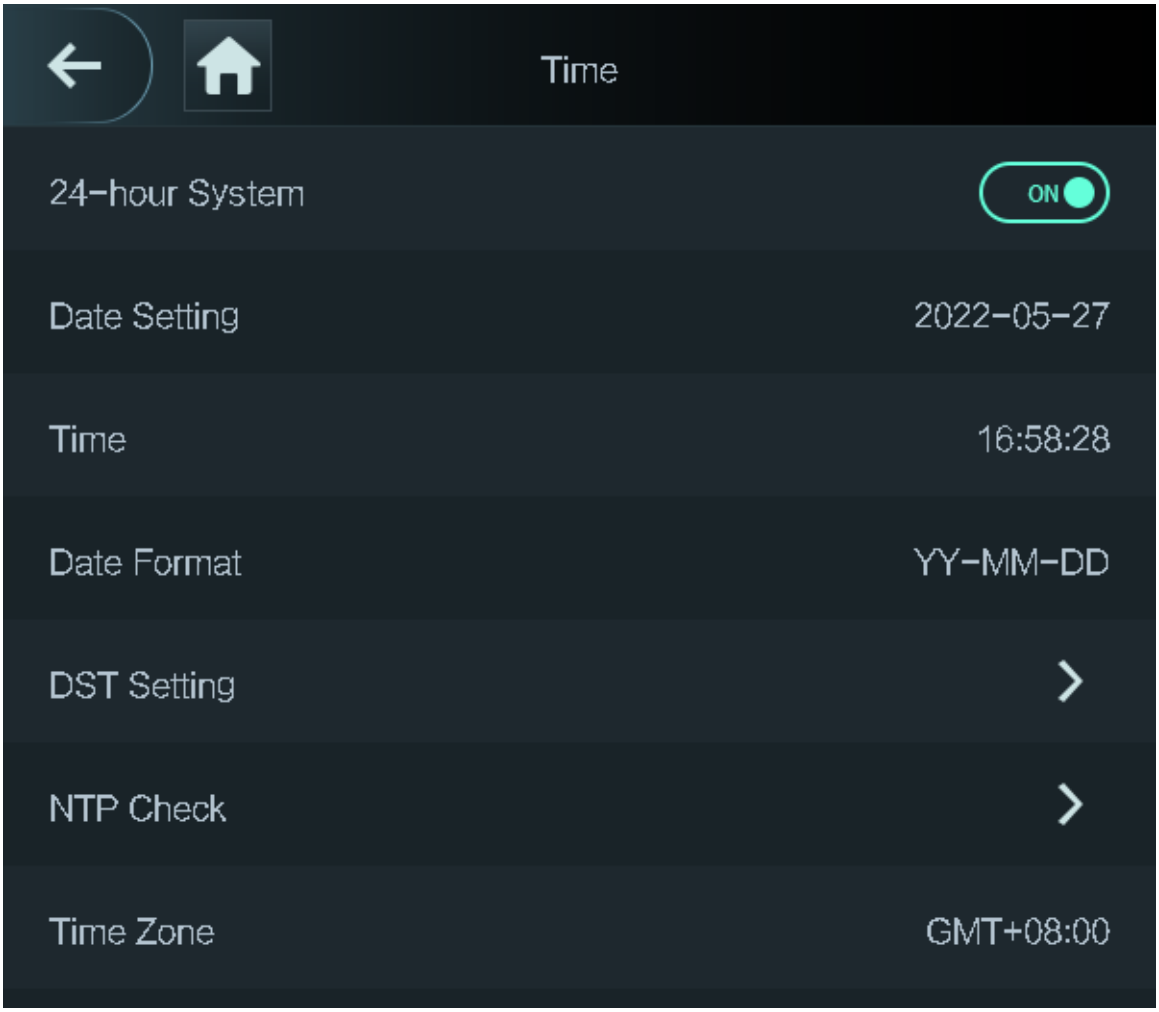


Table 2-8 Description of time parameters

Parameter	Description
24-hour System	The time is displayed in 24-hour format.
Date Setting	Set up the date.
Time	Set up the time.
Date Format	Select a date format.
DST Setting	1. Tap **DST Setting** 2. Enable DST. 3. Select **Date** or **Week** from the **DST** Type list. 4. Enter start time and end time. 5. tap ☑.

Parameter	Description
NTP Check	A network time protocol (NTP) server is a machine dedicated as the time sync server for all client computers. If your computer is set to sync with a time server on the network, your clock will show the same time as the server. When the administrator changes the time (for daylight savings), all client machines on the network will also update. 1. Tap **NTP Check**. 2. Turn on the NTP check function and configure parameters. • **Server IP Address** : Enter the IP address of the NTP server, and the Access Controller will automatically sync time with NTP server. • **Port** : Enter the port of the NTP server. • **Interval (min)** : Enter the time synchronization interval.
Time Zone	Select the time zone.

2.9.2 Configuring Face Parameters

Procedure

Step 1 On the main menu, select **System** > **Face Parameter**.

Step 2 Configure the face parameters, and then tap ☑.

Figure 2-14 Face parameter

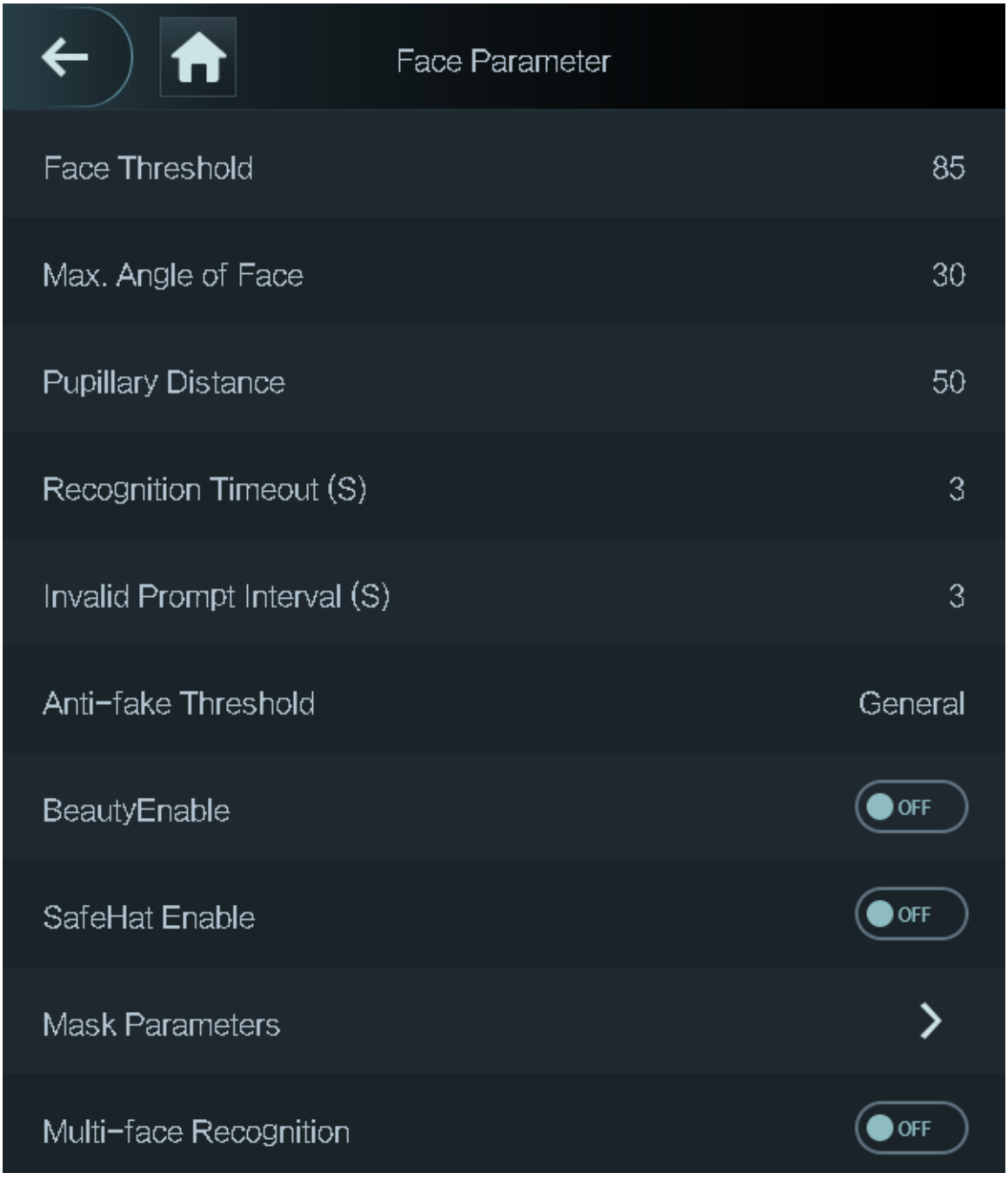


Table 2-9 Description of face parameters

Name	Description
Face Threshold	Adjust the face recognition accuracy. Higher threshold means higher accuracy.
Max. Angle of Face	Set the maximum face pose angle for face detection. Larger value means larger face angle range. If the face pose angle is out of the defined range, the face detection box will not appear.

Name	Description
Pupillary Distance	Face images require desired pixels between the eyes (called pupillary distance) for successful recognition. The default pixel is 45. The pixel changes according to the face size and the distance between faces and the lens. If an adult is 1.5 meters away from the lens, the pupillary distance can be 50 px-70 px.
Recognition Timeout (S)	If a person with access permission has their face successfully recognized, the Access Controller will prompt face recognition success. You can enter the prompt interval time.
Invalid Face Prompt Interval (S)	If a person without access permission attempts to unlock the door for several times in the defined interval, the Access Controller will prompt face recognition failure. You can enter the prompt interval time.
Anti-fake Threshold	Avoid false face recognition by using a photo, video, mask or a different substitute for an authorized person's face. ● Close: Turns off this function. ● General: Normal level of anti-spoofing detection means higher door access rate for people with face masks. ● High: Higher level of anti-spoofing detection means higher accuracy and security. ● Extremely High: Extremely high level of anti-spoofing detection means extremely high accuracy and security.
BeautyEnable	Beautify captured face images.
SafeHat Enable	Detects whether people wear safe hats.
Mask Parameters	● Mask mode: ◇ **No detect** : Mask is not detected during face recognition. ◇ **Mask reminder** : Mask is detected during face recognition. If the person is not wearing a mask, the system will remind them to wear masks, and access is allowed. ◇ **Mask intercept** : Mask is detected during face recognition. If a person is not wearing a mask, the system will remind them to wear masks, and access is denied. ● Mask Recognition Threshold: Higher threshold means higher mask detection accuracy.
Multi-face Recognition	Supports detecting 6 face images at the same time, and the unlock combinations mode become invalid. The door is unlocked after any one of them gain access.

2.9.3 Configuring Image Mode

Configure the image mode based on the installation site.

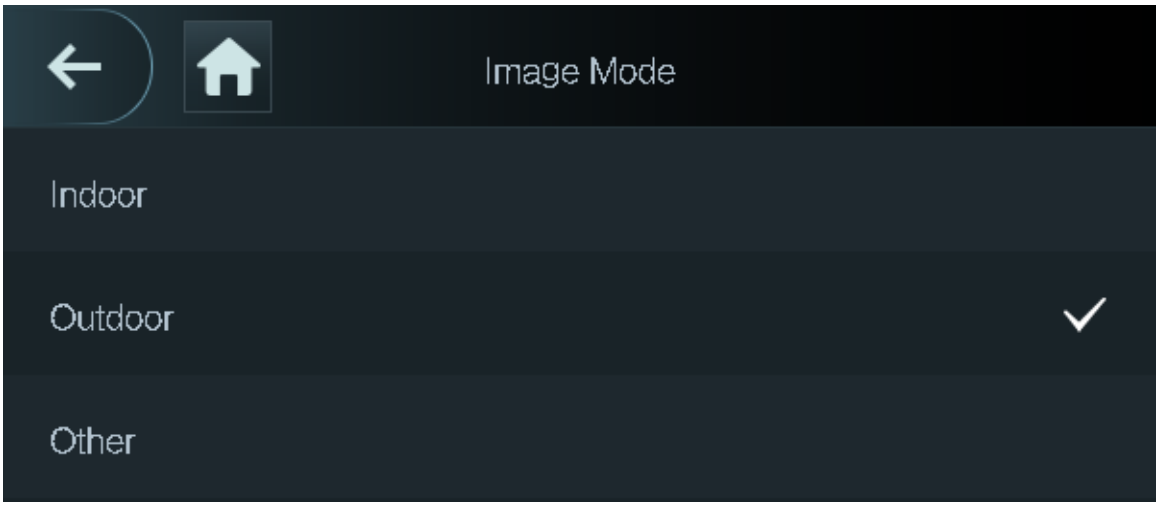
Procedure

Step 1 On the **Main Menu**, select **System** > **Image Mode**.

Step 2 Select image mode according to the installation location.

- Indoor: The Access Controller is usually installed indoor such as offices. The artificial light is even across the room and there is no daylight.
- Outdoor: The Access Controller is usually installed outdoor and the daylight is bright and even.
- Other: When human face is in back-lighting which makes the face dim, we recommend you select other mode to make it easier for the Access Controller to detect.

Figure 2-15 Image mode



2.9.4 Setting Volume

Background Information

You can adjust the volume.

Procedure

Step 1 On the **Main Menu**, select **System** > **Volume**.

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

Step 3 Tap + or − to adjust the volume.

2.9.5 (Optional) Configuring Fingerprint Parameters

Configure fingerprint detection accuracy. Higher value means that higher threshold of similarity and higher accuracy.

Background Information

This function is only available on Access Controller with fingerprint extension module.

Procedure

Step 1 On the **Main Menu**, select **System** > **Fingerprint**.

Step 2 Tap + or − to adjust the value.

2.9.6 Screen Settings

Configure screen off time and logout time.

Procedure

Step 1 On the **Main Menu**, select **System** > **Screen settings**.

Step 2 Tap **Logout Time** or **Screen Off Timeout**, and then tap + or − to adjust the time.

2.9.7 Restoring Factory Defaults

Procedure

Step 1 On the **Main Menu**, select **System** > **Restore Factory**.

Step 2 Restore factory defaults if necessary.

- **Restore Factory** : Resets all configurations except for configurations of IP and the type of extension module.
- **Restore Factory (Save user & log)** : Resets configurations except for user information and logs and IP configurations.

2.9.8 Restart the Device

On the **Main Menu**, select **System** > **Reboot**, and the Access Controller will be restarted.

2.10 USB Management

You can use a USB to update the Access Controller, and export or import user information through USB.

- Make sure that a USB is inserted to the Access Controller before you export data or update the system. To avoid failure, do not pull out the USB or perform any operation of the Access Controller during the process.
- You have to use a USB to export the information from an Access Controller to other devices. Face images are not allowed to be imported through USB.

2.10.1 Exporting to USB

Background Information

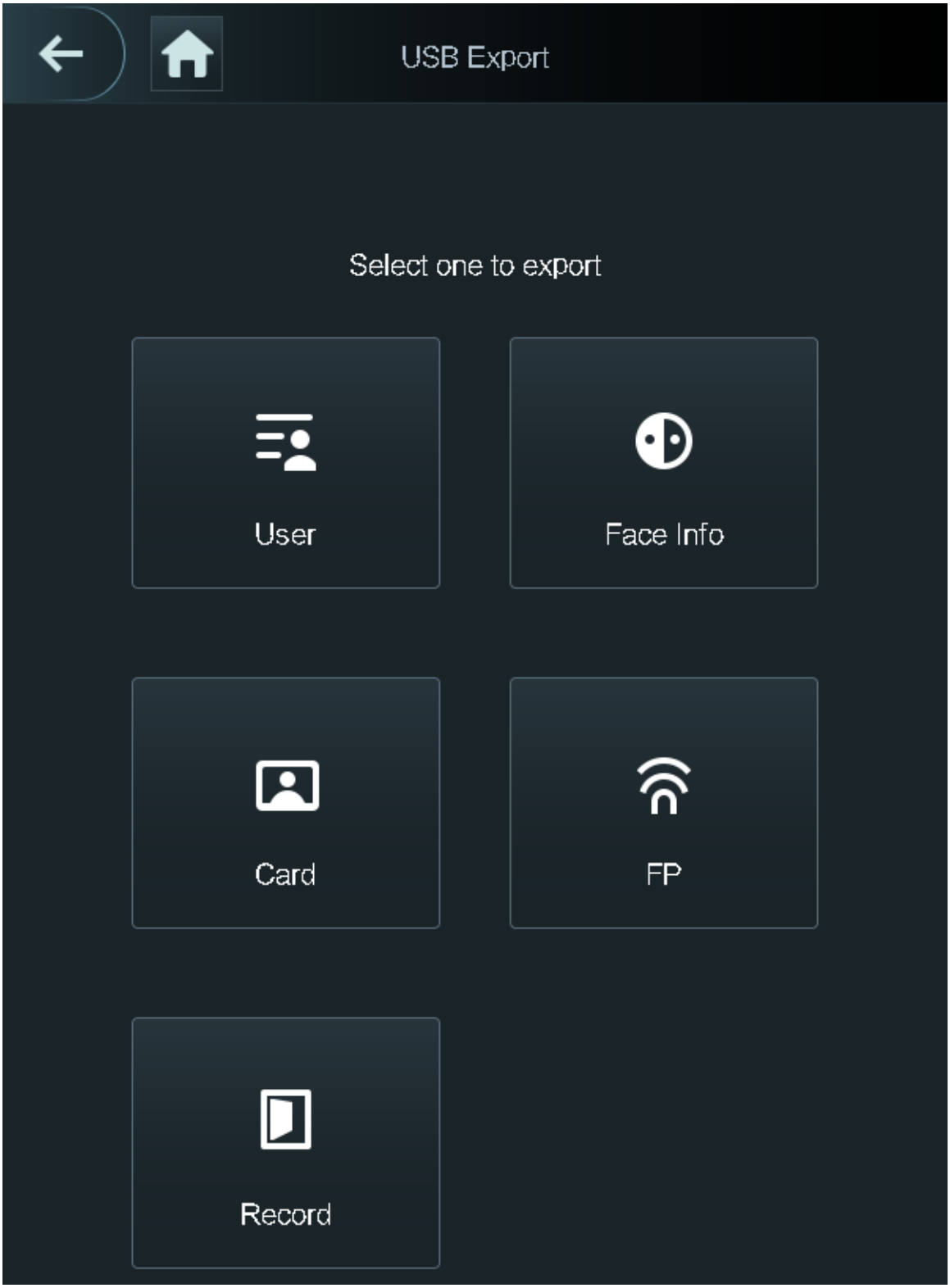
You can export data from the Access Controller to a USB. The exported data is encrypted and cannot be edited.

Procedure

Step 1 On the **Main Menu**, select **USB** > **USB Export**.

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

Figure 2-16 USB export



2.10.2 Importing From USB

Background Information

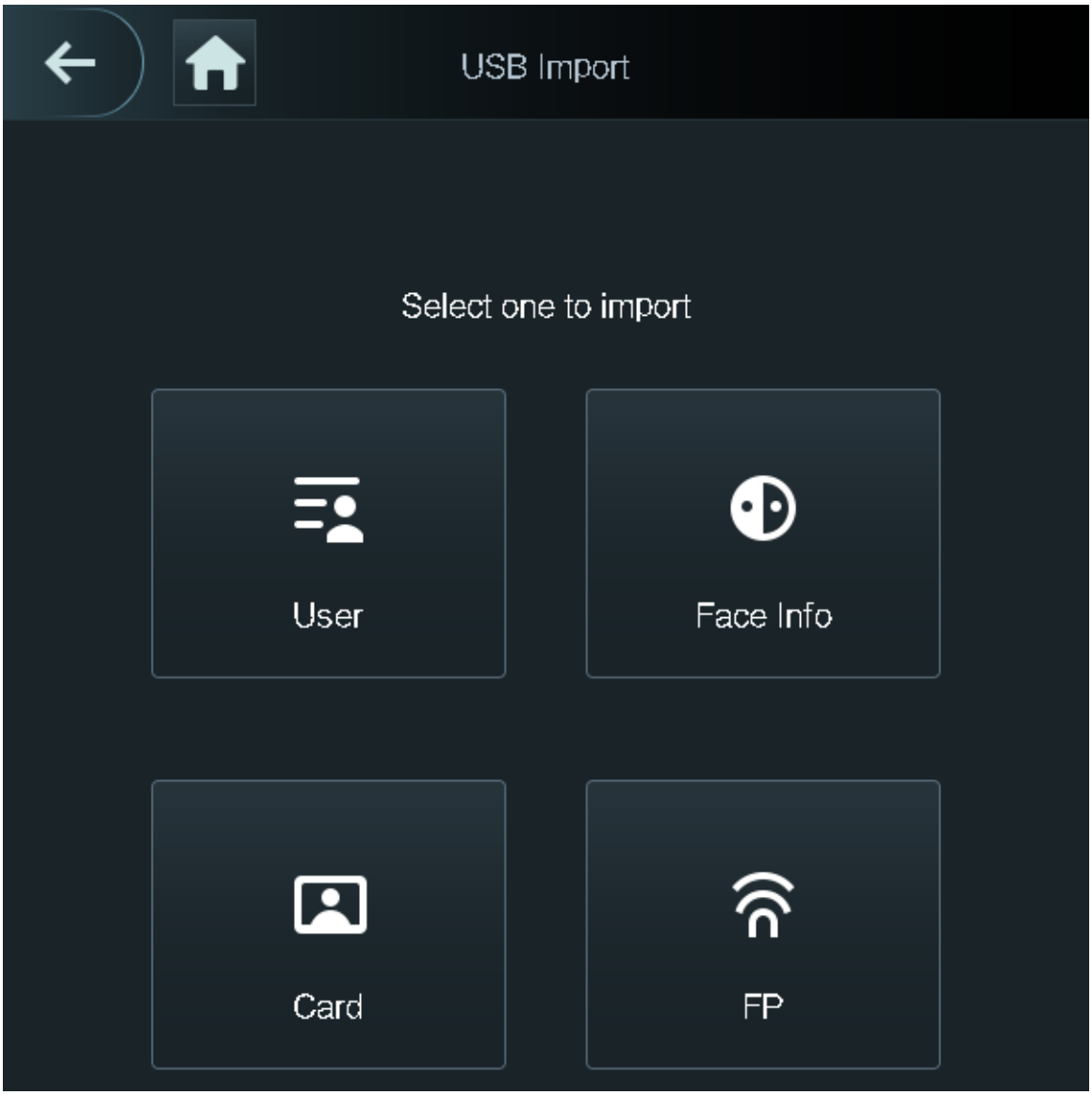
You can import data from USB to the Access Controller.

Procedure

Step 1 On the **Main Menu**, select **USB** > **USB Import**.

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

Figure 2-17 USB import



2.10.3 Updating System

Background Information

Use a USB to update the system of the Access Controller.

Procedure

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

Step 2 On the **Main Menu**, select **USB** > **USB Update**.

Step 3 Tap **OK**.

The Access Controller will restart when the updating completes.

2.11 Configuring Features

On the **Main Menu** interface, select **Features** > **Privacy Setting**.

Figure 2-18 Privacy setting

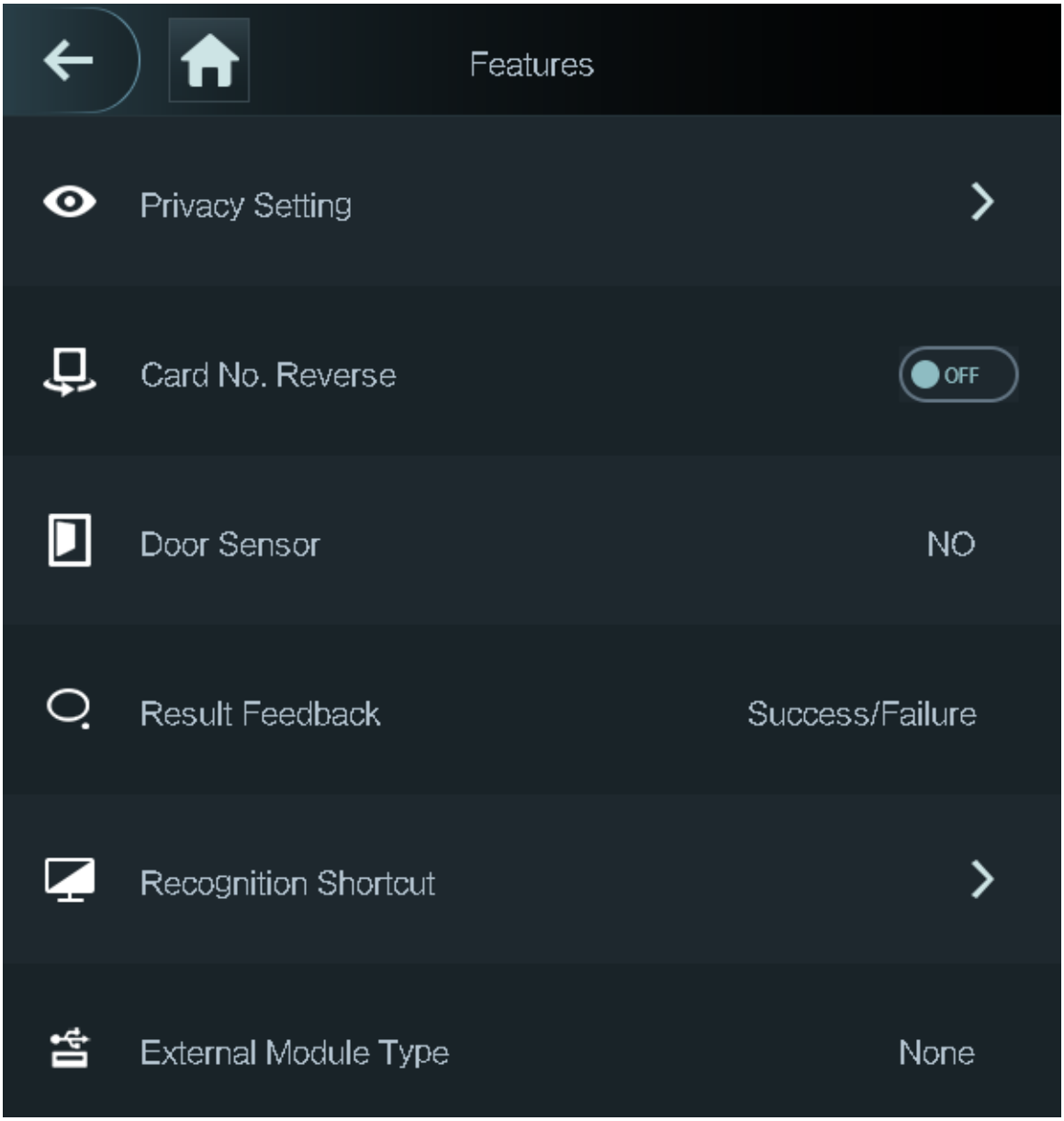


Table 2-10 Description of features

Parameter	Description
Private Setting	• PWD Reset Enable: You can enable this function to reset 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. The CG I is enabled by default. • SSH: Secure Shell (SSH) is a cryptographic network protocol for operating network services securely over an unsecured network. • Capture Photos: Face images will be captured automatically when people unlock the door. The function is enabled by default.
Card No. Reverse	When the Access Terminal connects to a third-party device through Wiegand input, and the card number read by the Access Terminal is in the reserve order from the actual card number, you need to turn on the **Card No. Reverse** function.
Door Sensor	NC: When the door opens, the circuit of the door sensor circuit is closed. NO: When the door opens, the circuit of the door sensor circuit is open. Intrusion and overtime alarms are triggered only after door detector is turned on.

Parameter	Description
Result Feedback	• Success/Failure: Only displays success or failure on the standby screen. • Only Name: Displays user ID, name and authorization time after access granted; displays not authorized message and authorization time after access denied. • Photo&Name: Displays user's registered face image, user ID, name and authorization time after access granted; displays not authorized message and authorization time after access denied. • Photos&Name: Displays the captured face image and a registered face image of a user, user ID, name and authorization time after access granted; displays not authorized message and authorization time after access denied.
Recognition shortcut	Select identity verification methods on the standby screen. • Password: The icon of the password unlock method is displayed on the standby screen. • QR code: The the icon of the QR code unlock method is displayed on the standby screen. • Call: The icon of call function is displayed on the standby screen. • Call Type: ◇ Call Room: Tap the call icon on the standby mode and enter the room number to make calls. ◇ Call Management Center: Tap the call icon on the standby mode, and then call the management center. ◇ Custom call room: Tap the call icon to call the defined room number. You need to define the number of room first on the **Recognition shortcut** screen.
External Module Type	1. Select an external module. • FP • QR Code • FP+QR Code: 2. Tap **Yes**. The Access Controller restarts. is displayed on the standby screen, which indicates connection success. If is displayed, it indicates that selected module type and the actual module mounted to the Access Controller do not match. External extension modules do not support hot swapping. External module type configurations will not be restored to factory defaults.

2.12 Unlocking the Door

You can unlock the door through faces, passwords, cards, and more. The default unlock methods are card/face/password.

If a fingerprint extension module is mounted to the Access Controller, the default unlock methods change to card/face/password/fingerprint by default after the Access Controller is restored to factory defaults.

If the Access Controller is not restored to factory defaults after an extension module is mounted to it, the default unlock methods are still card/face/password.

2.12.1 Unlocking by Cards

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

2.12.2 Unlocking by Face

Verify the identity of an individual by detecting their faces. Make sure that your face is centered on the face detection frame.

2.12.3 Unlocking by User Password

Background Information

Enter the user ID and password to unlock the door.

Procedure

Step 1 Tap on the standby screen.

Step 2 tap **PWD Unlock**, and then enter the user ID and password.

Step 3 Tap **Yes**.

2.12.4 Unlocking by Administrator Password

Enter only the administrator password to unlock the door. The access controller only allows for one administrator password. Using administrator password to unlock the door without being subject to user levels, unlock modes, periods, holiday plans, and anti-passback except for normally closed door. One device allows for only one admin password.

Prerequisites

The administrator password was configured. For details, see "2.7.3 Configuring Administrator Password".

Background Information

Administrator password cannot be used to unlock the door status is set to NC.

Procedure

Step 1 Tap on the standby screen.

Step 2 Tap **Admin PWD**, and then enter the admin password.

Step 3 Tap ☑.

2.12.5 Unlocking by QR code

Procedure

Step 1 On the standby screen, tap .

Step 2 Place your QR code in front of the lens.

You can also place the QR code in front of the lens directly without tapping .

If a QR code extension module is mounted to the Access Controller, will not be displayed on the standby screen. Place the QR code in front of the lens of the Access Controller or the lens of the extension module.

2.12.6 Unlocking by Fingerprint

Place you finger on the fingerprint scanner. This function is only available when a fingerprint extension module is mounted to the Access Controller.

2.13 System Information

You can view data capacity and device version.

2.13.1 Viewing Data Capacity

Background Information

On the **Main Menu**, select **System Info** > **Data Capacity**, you can view storage capacity of each data type.

2.13.2 Viewing Device Version

Background Information

On the **Main Menu**, select **System Info** > **Data Capacity**, you can view the device version, such as serial No., software version and more.

3 Web Operations

On the webpage, you can also configure and update the Access Controller.

Web configurations differ depending on models of the Access Controller.

3.1 Initialization

Initialize the Access Controller when you log in to the webpage for the first time or after the Access Controller is restored to the factory defaults.

Prerequisites

Make sure that the computer used to log in to the webpage is on the same LAN as the Access Controller.

Background Information

Set a password and an email address before logging in to the webpage for the first time.

Procedure

Step 1 Open a browser, go to the IP address (the default address is 192.168.1.108) of the Access Controller.

We recommend you use the latest version of Chrome or Firefox.

Step 2 Set the password and email address according to the screen instructions.

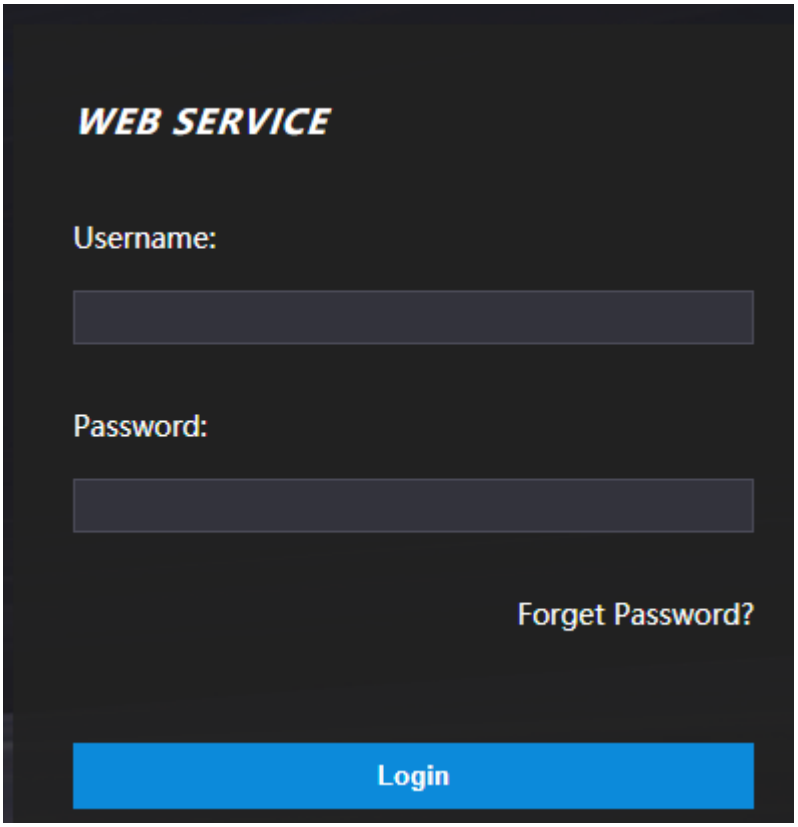
- The password must consist of 8 to 32 non-blank characters and contain at least two types of the following characters: upper case, lower case, numbers, and special characters (excluding ' " ; : &). Set a high-security password by following the password strength prompt.
- Keep the password safe after initialization and change the password regularly to improve security.

3.2 Logging In

Procedure

Step 1 Open a browser, enter the IP address of the Access Controller in the **Address** bar, and press the Enter key.

Figure 3-1 Login



Step 2 Enter the user name and password.

- The default administrator name is admin, and the password is the one you set up during initialization. We recommend you change the administrator password regularly to increase security.
- If you forget the administrator login password, you can click **Forget password?** For details, see "3.3 Resetting the Password".

Step 3 Click **Login**.

3.3 Resetting the Password

Background Information

Reset the password through the linked e-mail when you forget the admin password.

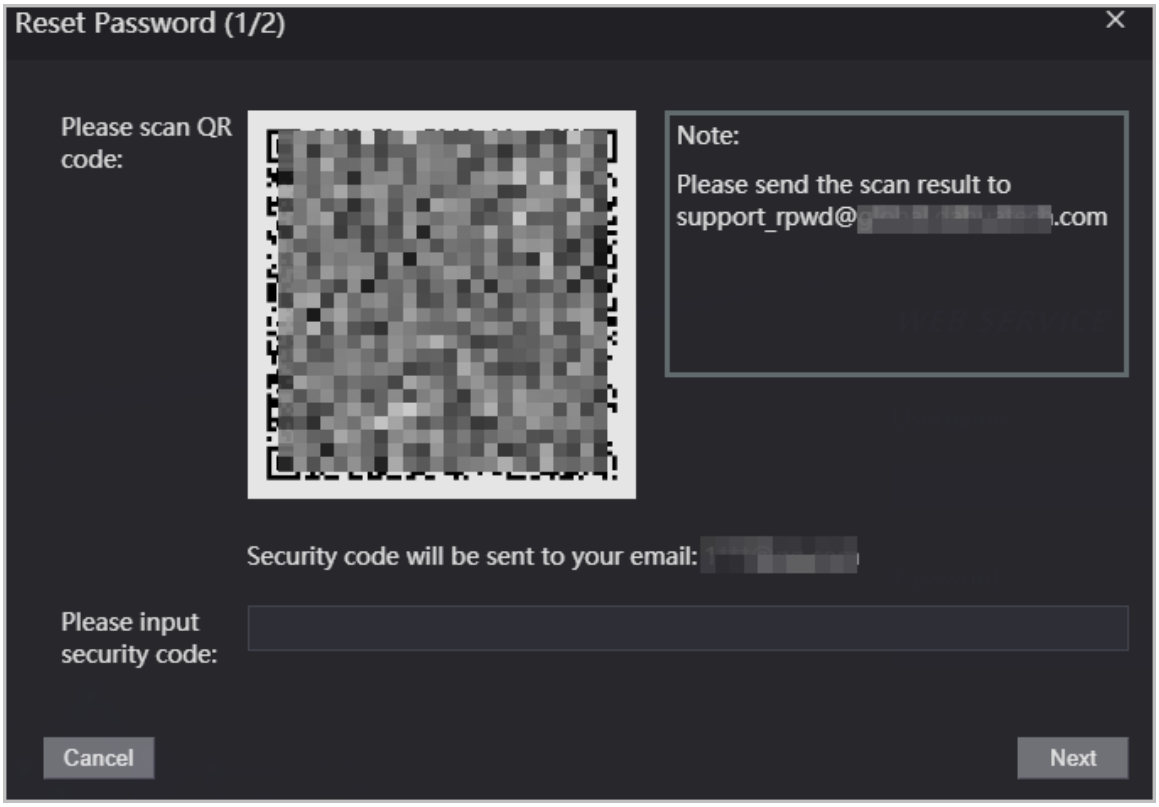
Procedure

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

Step 2 Read the on-screen prompt carefully, and then click **OK**.

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

Figure 3-2 Reset password



- Up to two security codes will be generated when the same QR code is scanned. If the security code becomes invalid, refresh the QR code and scan again.
- After you scan the QR code, you will receive a security code in your linked e-mail address. Use the security code within 24 hours after you receive it. Otherwise, it will become invalid.
- If the wrong security code is entered in a row, the administrator account will be frozen for 5 minutes.

Step 4 Enter the security code.

Step 5 Click **Next**.

Step 6 Reset and confirm the new password.

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

Step 7 Click **OK**.

3.4 Configuring Door Parameter

Background Information

Configure the access control parameters.

Procedure

Step 1 Log in to the webpage.

Step 2 Select **Door Parameter**.

Figure 3-3 Door parameter

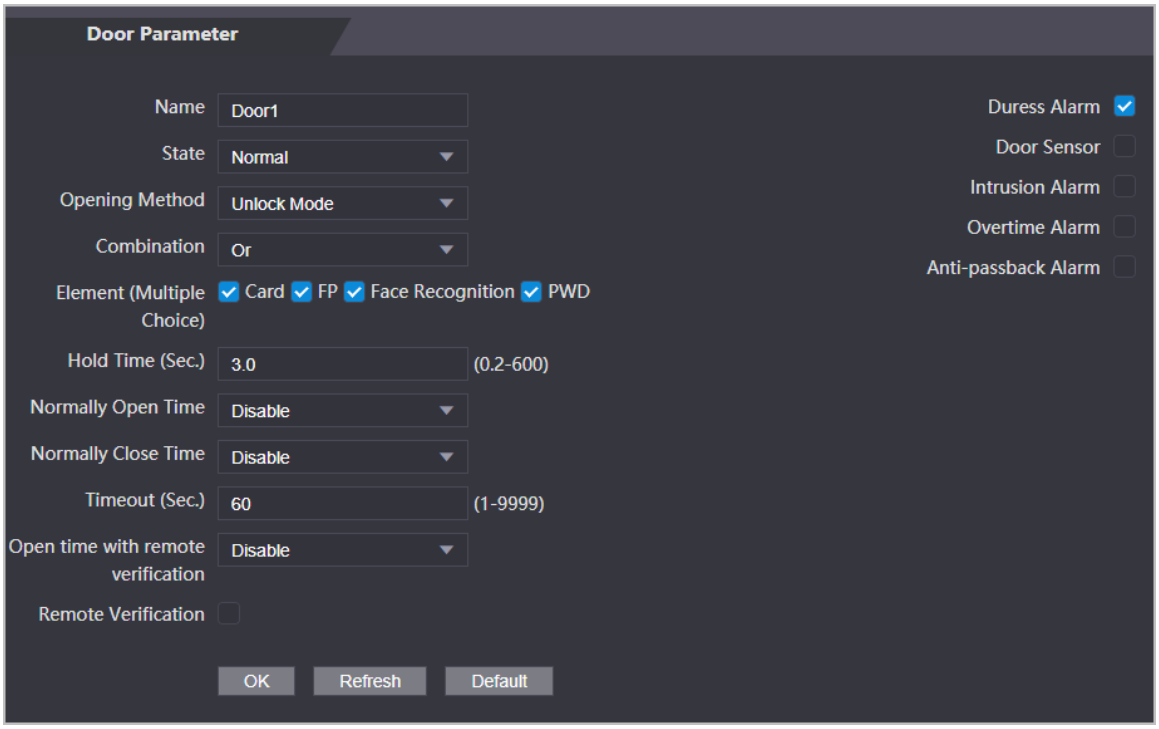


Table 3-1 Description of door parameters

Parameter	Description
Name	Enter a name of the door.
State	Set the door status. • **NO** : The door remains unlocked all the time. • **NC** : The door remains locked all the time. • **Normal** : If **Normal** is selected, the door will be unlocked and locked according to your settings.
Opening Method	• Unlock by Period: Set different unlock methods for different periods. • Group Combination: The user can unlock the door only after defined users or user groups grant access. • Unlock Mode: Set unlock combinations.
Hold Time (Sec.)	After a person is granted access, the door will remain unlocked for a defined time for them to pass through. It ranges from 0.2 s to 600 s.
Normally Open Time	The door remains open or closed during the defined period.
Normally Close Time	
Timeout (Sec.)	A timeout alarm will be triggered if the door remains unlocked for longer time than this value.
Open with remote verification	Set the remote verification door opening period. After users gain access on the Access Controller, they must also be granted access from the management platform before the door unlocks.

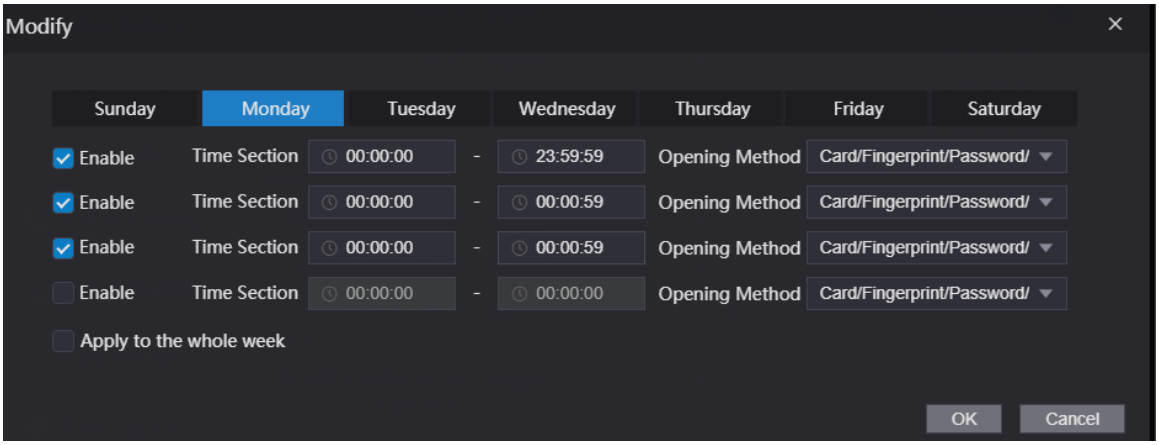
Parameter	Description
Duress Alarm	An alarm will be triggered when a duress card or duress password is used to unlock the door.
Door Sensor	Intrusion and overtime alarms can be triggered only after **Door Sensor** is enabled.
Intrusion Alarm	When **Door Sensor** is enabled, an intrusion alarm will be triggered if the door is opened abnormally.
Overtime Alarm	A timeout alarm will be triggered if the door remains unlocked for longer time than the **Timeout (Sec)**.
Anti-passback Alarm	Users need to verify their identities both for entry and exit; otherwise an alarm will be triggered. It help prevents a card holder from passing an access card back to another person so they gain entry. When anti-passback is enabled, the card holder must leave the secured area through an exit reader before system will grant another entry. ● If a person enters after authorization and exits without authorization, an alarm will be triggered when they attempt to enter again, and access is denied at the same time. ● If a person enters without authorization and exits after authorization, an alarm will be triggered when the they attempt to enter again, and access is denied at the same time.

Step 3 Configure the opening method.

- Unlock by Period

1. In the **Opening Method** list, select **Unlock by Period**, and then click .

Figure 3-4 Time section parameter



2. Configure the time and the opening method for a time section. You can configure up to four time sections for a single day.
3. Select **Apply to the whole week** to copy the defined time to the rest of days.

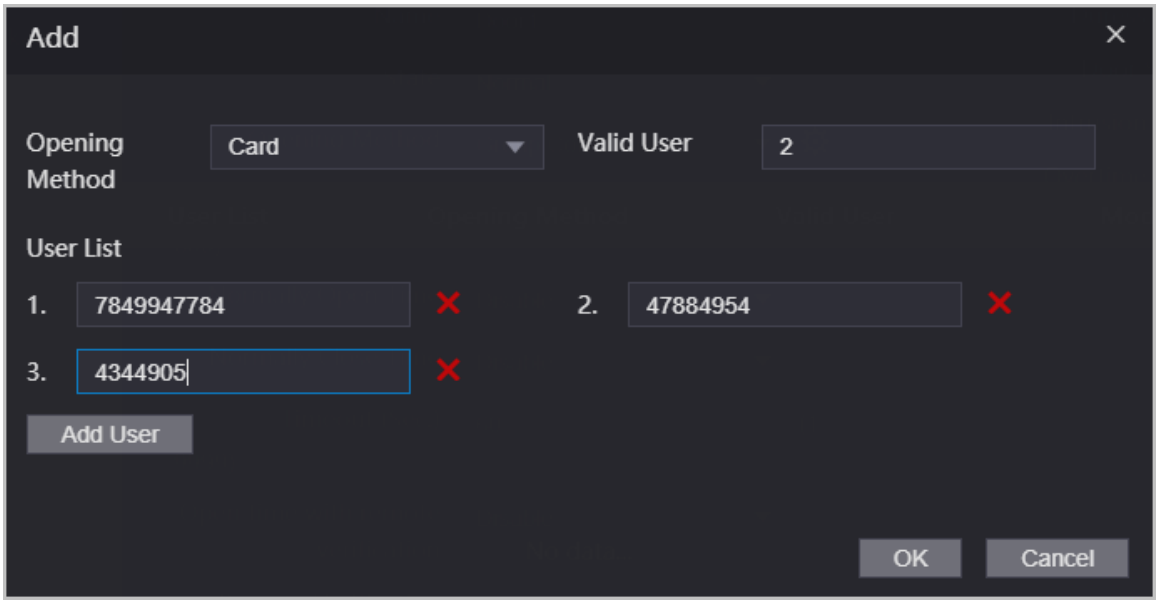
- Group Combination

1. In the **Opening Method** list, select **Group Combination**, and then click .
2. Click **Add**.

3. Select an unlocking method in the **Opening Method** list., and enter the number of valid users.

   If the number of valid users is 2, and there are 3 users in the defined user list. Two users in the list are required to grant access.

Figure 3-5 Group Combination



4. In the **User List** area, click **Add User**, enter the user ID of existing users.

   - VIP, patrol, and blocklist users cannot be added.
   - Valid users in all groups must verify their identities to grant access in the group order.

5. Click **OK**.

- Unlock mode

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

Step 4 Configure other parameters.

Step 5 Click **OK**.

3.5 Configuring Alarm Linkage

3.5.1 Setting Alarm Linkage

Background Information

Configure alarm linkage to trigger alarms when abnormal access events occur.

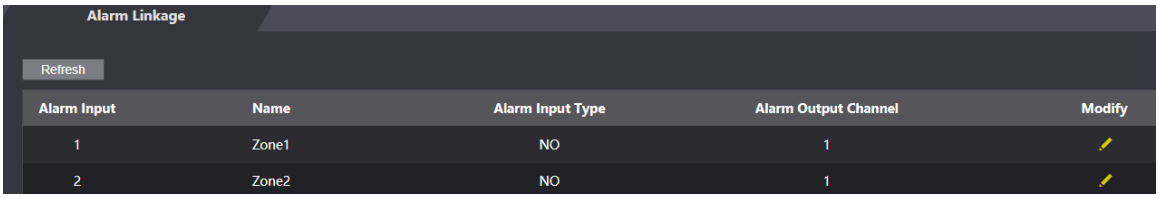
The configurations on the webpage will be synchronized with the configurations on the management platform if the Access Controller is added to it.

Procedure

Step 1 Log in to the webpage.

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

Figure 3-6 Alarm linkage



Step 3 Click , and then you can modify alarm linkage parameters.

Figure 3-7 Modify alarm linkage parameters

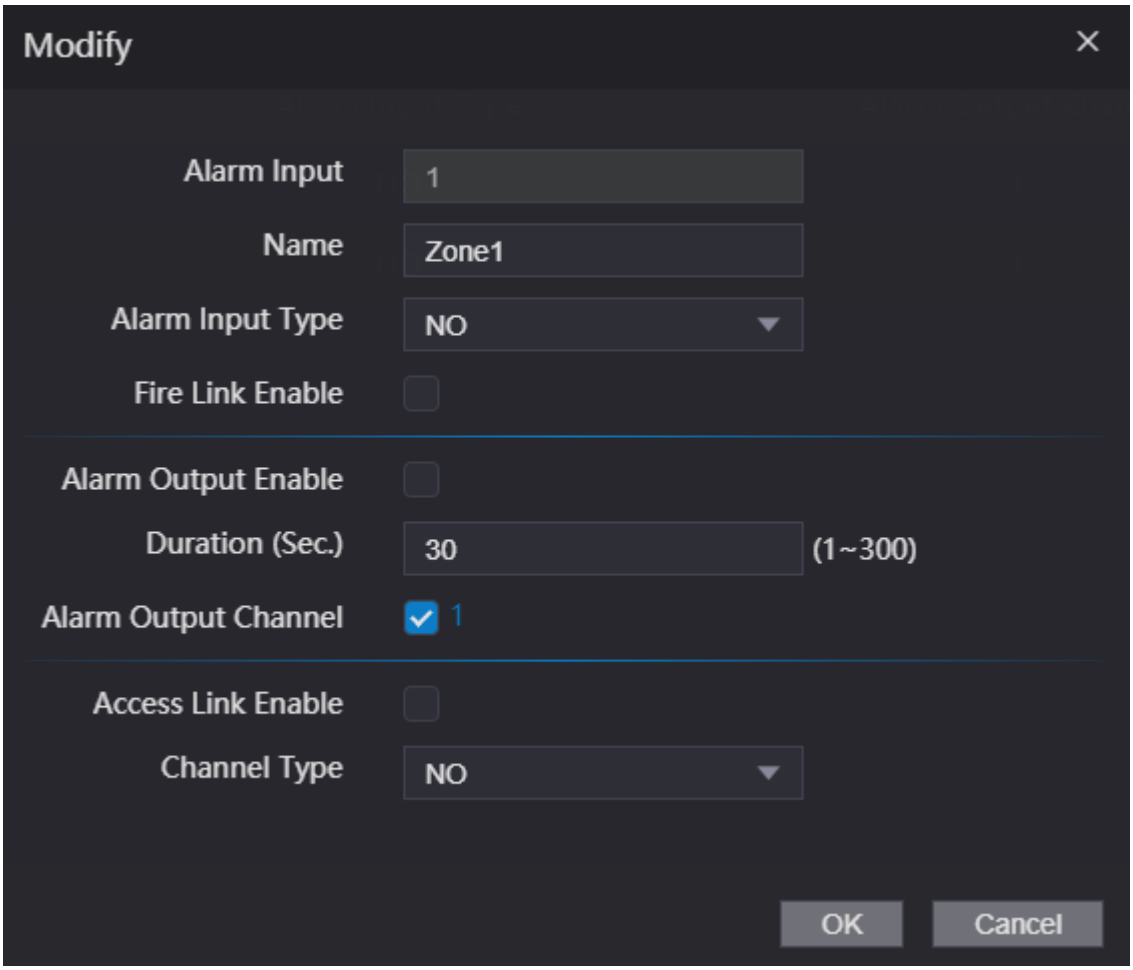


Table 3-2 Description of alarm linkage parameters

Parameter	Description
Alarm Input	The number of the alarm input which cannot be modified.
Name	Enter the name of the alarm.

Parameter	Description
Alarm Input Type	Select the input type according to the alarm device. • **NO** : The circuit of the alarm device is normally open, and it closes when an alarm is triggered. • **NC** : The circuit of the alarm device is normally closed, and it opens when an alarm is triggered.
Fire Link Enable	If fire linkage is enabled, fire alarms will be triggered fire events occur, and alarm outputs and door access will be linkaged. If fire linkage is turned on, alarm output is turned on by default, and the door access will be normally open when fire events occur by default.
Alarm Output Enable	If alarm output is turned on, the relay will generate alarm messages.
Duration (Sec.)	Alarm duration. It ranges from 1 s through 300 s.
Alarm Output Channel	Select the alarm output channel according to your alarm device.
Access Link Enable	After the access control linkage is turned on, the door will be normally open or normally closed when there are input alarm signals. • NO: The door is normally open when there are input alarm signals. • NC: The door is normally closed when there are input alarm signals.
Channel Type	

Step 4 Click **OK**.

3.5.2 Viewing Alarm Logs

Procedure

Step 1 Log in to the webpage.

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

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

3.6 Intercom Configuration

The Access Controller can function as a door station to realize video intercom function.

3.6.1 Configuring SIP Server

When connected to the same SIP server, all VTOs and VTHs can call each other. You can use the Access Controller or other VTOs or the management platform as the SIP server.

Background Information

When the Access Controller functions as the SIP server, it can connect up to 500 access control devices and VTHs.

Procedure

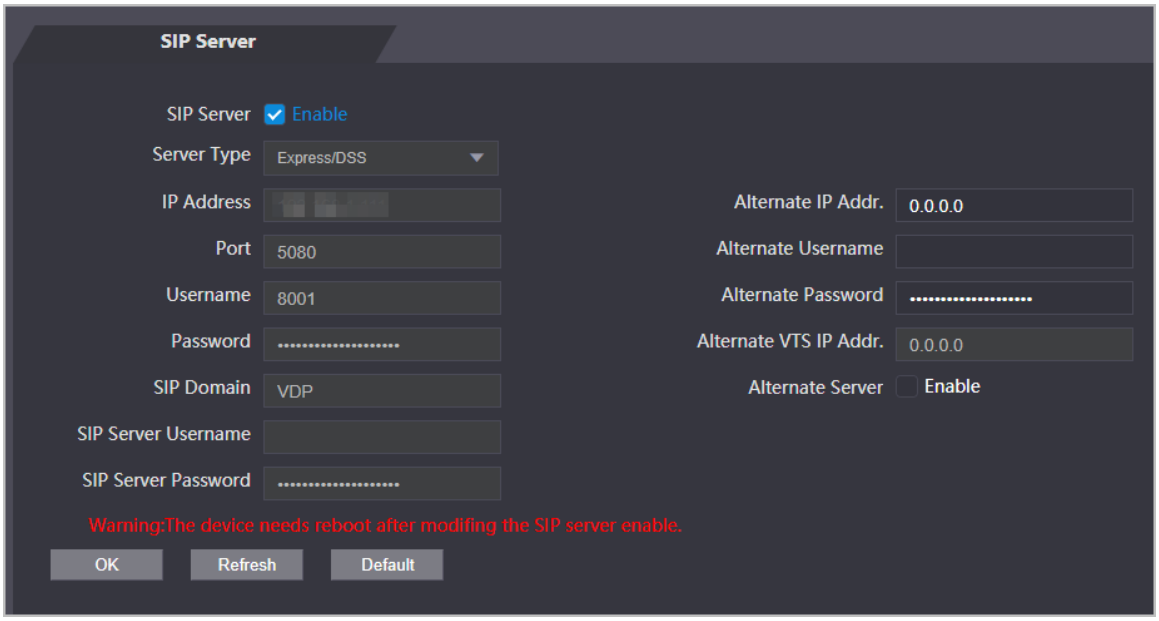
Step 1 Select **Intercom** > **SIP Server**.

Step 2 Select a server type.

- Use the Access Controller as the SIP server.

  Turn on **SIP Server** and keep other parameters as default.

  Figure 3-8 Use the Access Controller as the SIP server



- Use another VTO as the SIP server:

  1. Do not enable **SIP server** . Select **VTO** from the **Server Type**.
  2. Configure the parameters, and then click **OK**.

Figure 3-9 Use VTO as the SIP server

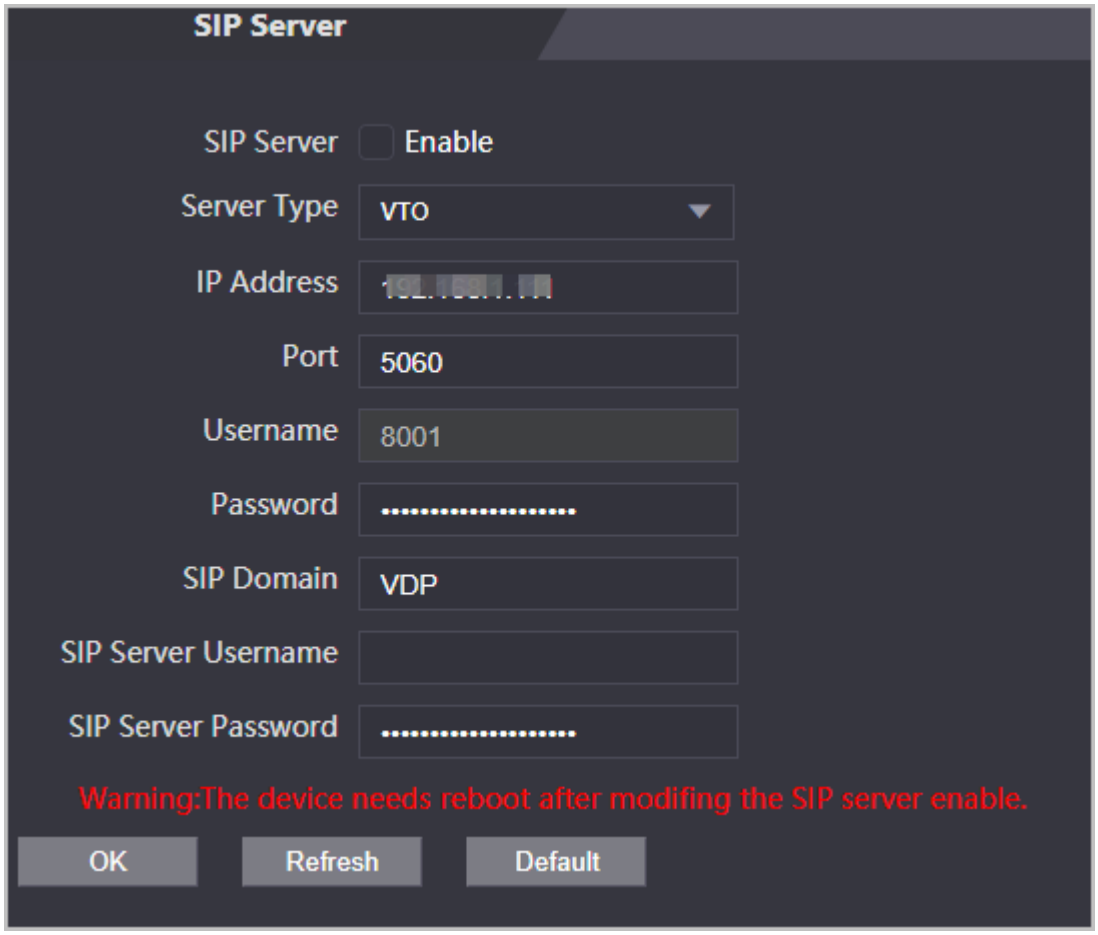


Table 3-3 SIP server configuration

Parameter	Description
IP Address	IP address of the platform.
Port	◇ 5060 by default when VTO works as SIP server. ◇ 5080 by default when the platform works as SIP server.
Username	Leave them as default.
Password	
SIP Domain	VDP.
SIP Server Username	The login username and password of the SIP server.
SIP Server Password	

- Use the DSS Express or DSS Pro as the SIP server.

  Do not enable **SIP server** . Select **Express/DSS** from the **Server Type**.

Figure 3-10 Use DSS Express or DSS Pro as the SIP server

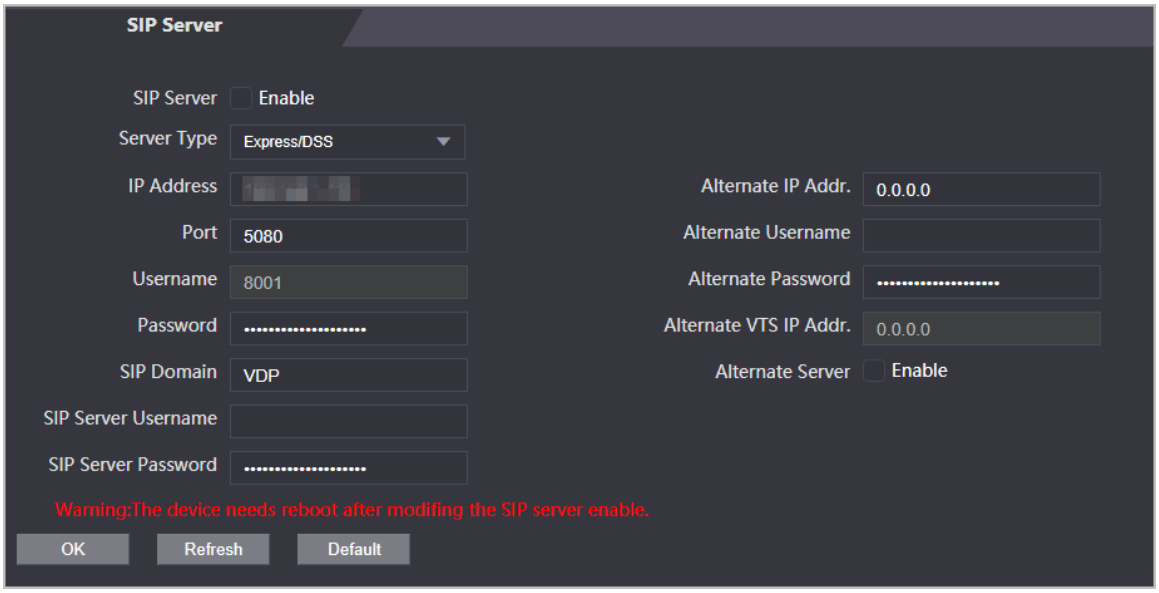


Table 3-4 SIP server configuration

Parameter	Description
IP Address	IP address of the platform.
Port	◇ 5060 by default when VTO work as SIP server. ◇ 5080 by default when the platform works as SIP server.
Username	Leave them as default.
Password	
SIP Domain	Leave it as default.
SIP Server Username	The login username and password of the platform.
SIP Server Password	
Alternate IP Addr.	The alternate server will be used as the SIP server when DSS Express or DSS Pro does not respond. We recommend you configure the alternate IP address. ◇ If you turn on the **Alternate Server** function, you will set the Access Controllers the alternate server. ◇ If you want another VTO to function as the alternate server, you need to enter the IP address, username, password of the VTO. Do not enable **Alternate Server** in this case. ◇ We recommend you set the main VTO as the alternate server.
Alternate Username	Used to log in to the alternate server.
Alternate Password	
Alternate VTS IP Addr.	Enter the IP address of the alternate VTS. When the management platform does not respond, the alternate VTS will be activated to make sure VTO, VTH and VTS can still realize video intercom function.

Step 3 Click **OK**.

3.6.2 Configuring Basic Parameters

Configure the basic information of VTO, such as device type and device number.

Procedure

Step 1 Select **Talkback** > **Local**.

Step 2 Configure the parameters.

- Use the Access Controller as the SIP server.

Figure 3-11 Basic parameter

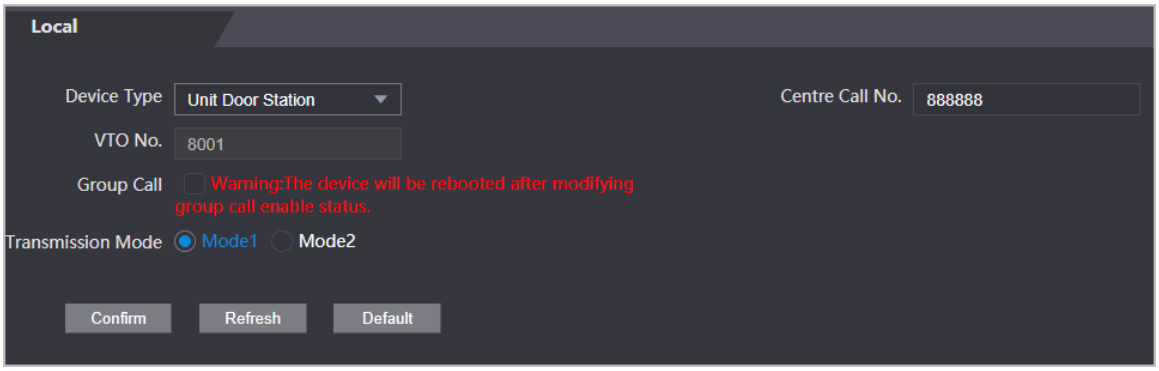


Table 3-5 Basic parameter description

Parameter	Description
Device Type	Select **Unit Door Station**.
VTO No.	The number of the VTO, which cannot be configured.
Group Call	When you turn on the group call function, the VTO calls the main VTH and the extensions at the same time.
Centre Call No.	The default phone number is 888888+VTS No. when the VTO calls the VTS. You can check the number of the VTS from the **Device** screen of VTS.
Transmission Mode	Mode 1 is selected by default.

- Use other VTO as the SIP server.

Figure 3-12 Basic parameter

Table 3-6 Basic parameter description

Parameter	Description
Device Type	Select **Unit Door Station**.
VTO No.	The number of the VTO. ◇ The number must have four digits. The first two digits are 80, and the last two digits start from 01. For example, 8001. ◇ If multiple VTOs exist in one unit, the VTO No. cannot be repeated.
Centre Call No.	The default phone number for the management center is 888888. Keep it as default.
Transmission Mode	Mode 1 is selected by default.

- Use the Platform (DSS Express or DSS Pro) as the SIP Server.

Figure 3-13 Basic parameter

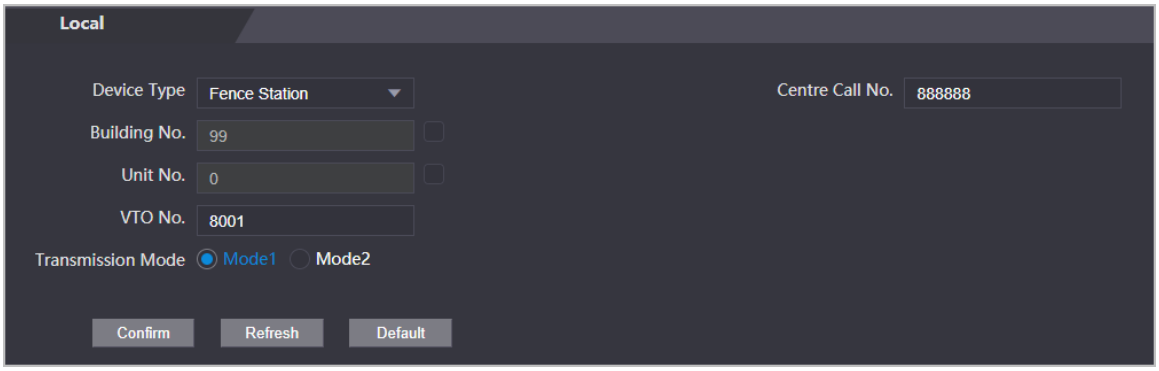


Table 3-7 Basic parameter description

Parameter	Description	
Device Type	Select the device type based on the installation position.	
Building No.	Select the checkbox and then enter the number of the building where the unit door station is installed.	If building and unit are enabled on DSS, enter the building number and unit number on the webpage. The building number, unit number and VTO number must conform to the configured parameters on DSS. Take room 1001, unit 2, and building 1 as an example. If building number is enabled on the DSS and the unit is not enabled, the room number is "1#1001". If building and unit are both enabled, the room number is "1#2#1001". If building is not enabled, and unit is not enabled either, the room number is "1001". For details, see the user manual of DSS.
Unit No.	Select the checkbox and then enter the number of the unit where the unit door station is installed.	
VTO No.	The number of the unit door station. If multiple VTOs exist in one unit, the VTO No. cannot be repeated.	
Centre Call No.	The default phone number is 888888 when the VTO calls the VTS. Keep it as default.	

Parameter	Description
Transmission Mode	Mode 1 is selected by default.

Step 3 Click **Confirm**.

3.6.3 Adding the VTO

When the Access Controller functions as the SIP Server and you have other VTOs, you need to add other VTOs to the SIP server to make sure they can call each other.

Procedure

Step 1 On the webpage of the Access Controller, select **Talkback setting** > **VTO No. Management**.

Step 2 Click **Add**, and then configure the VTO.

Figure 3-14 Add VTO

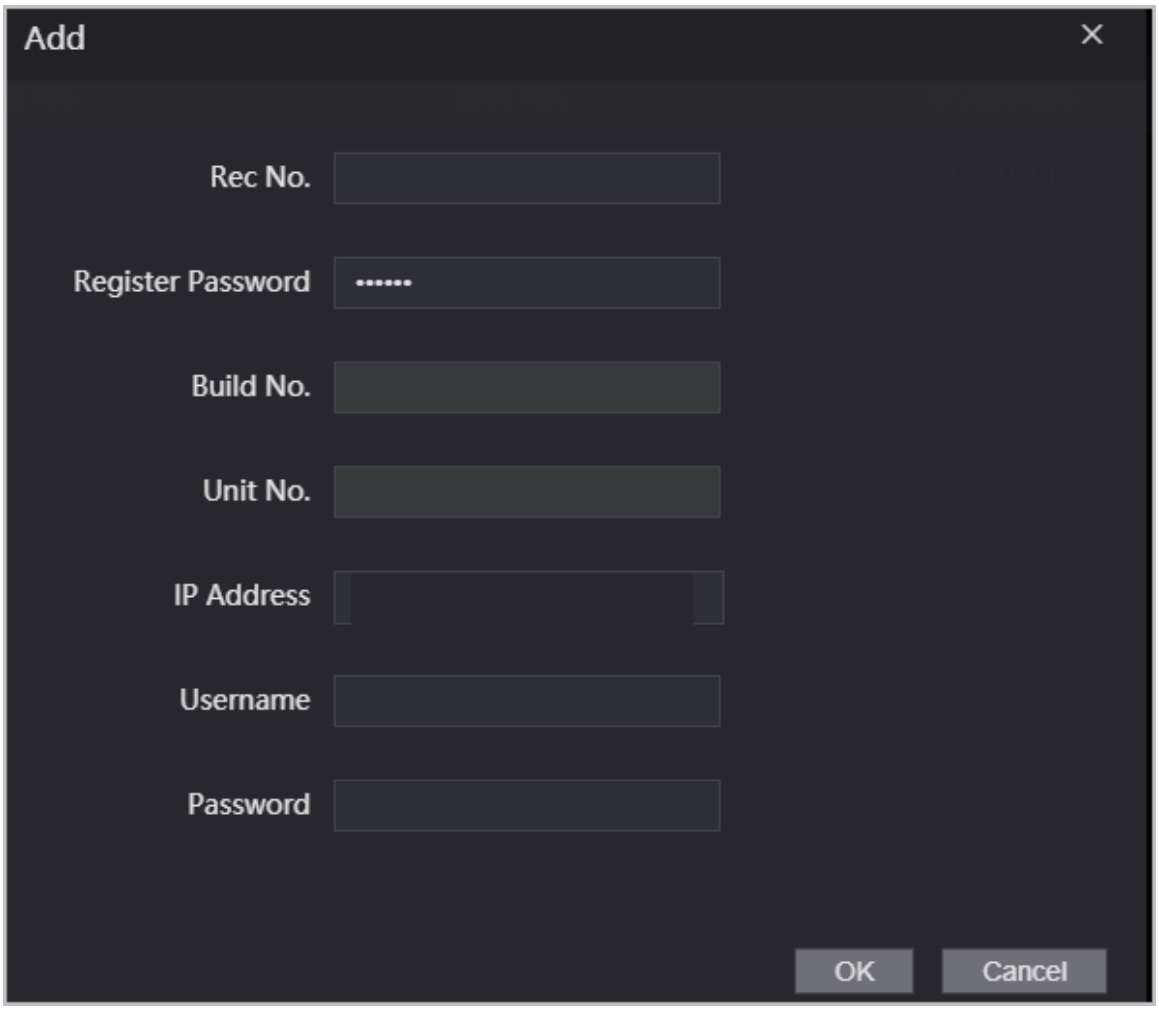


Table 3-8 Add VTO configuration

Parameter	Description
Rec No.	The number of the added VTO. You can check the number from the **Device** page on the webpage of the VTO.

Parameter	Description
Registration Password	Keep it default.
Build No.	Cannot be configured.
Unit No.	
IP Address	The IP address of the added VTO.
Username	The username and password used to log in to the webpage of the added VTO.
Password	

Step 3 Click **OK**.

3.6.4 Adding the VTH

When the Access Controller functions as the SIP Server, you can add all VTHs in the same unit to the SIP server to make sure they can call each other.

Background Information

- When there are main VTH and extension, you need to turn on the group call function first and then add main VTH and extension on the **VTH Management** page. For how to turn on the group call function, refer to "3.6.2 Configuring Basic Parameters".
- Extension cannot be added when the main VTHs are not added.

Procedure

Step 1 On the home page, select **Talkback setting** > **Room No. Management**.

Step 2 Add the VTH.

- Add individually
  1. Click **Add**.
  2. Configure parameters, and then click **OK**.

Figure 3-15 Add individually

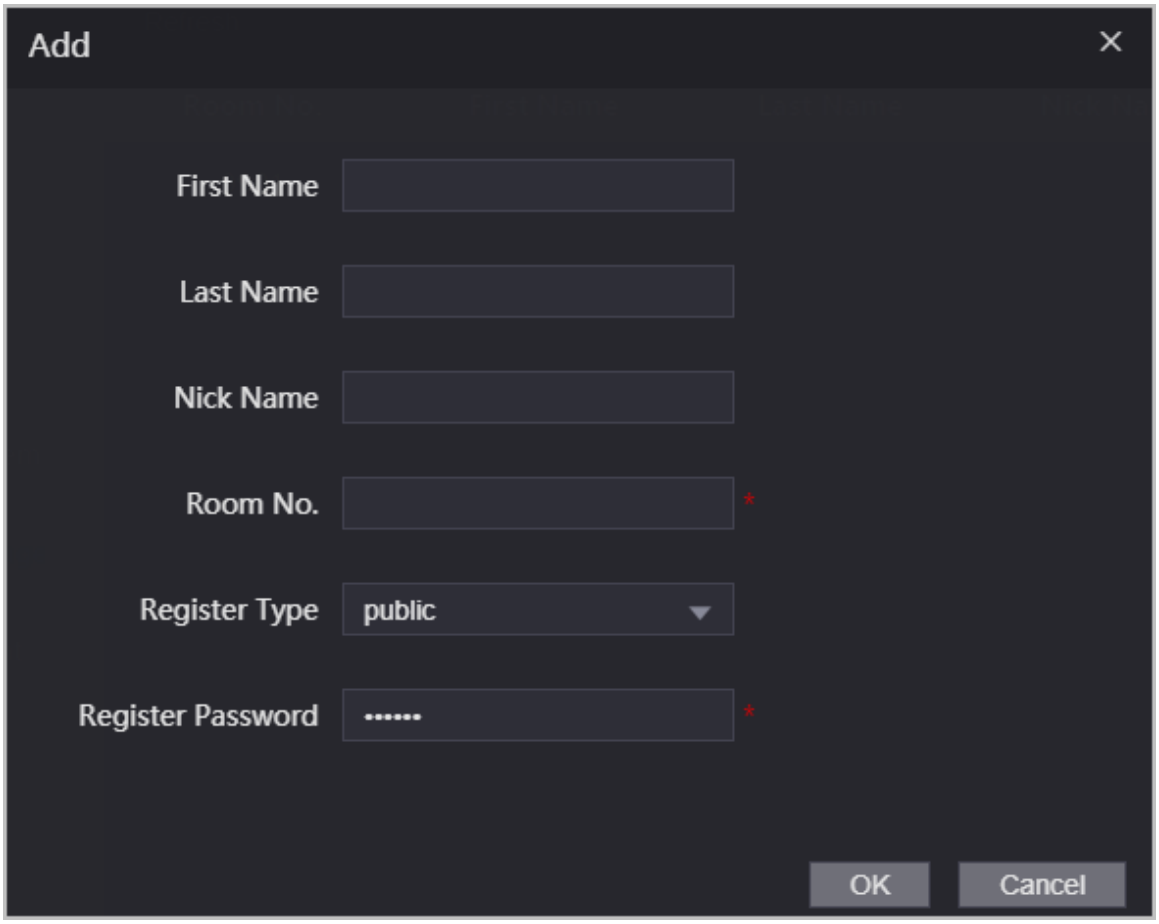


Table 3-9 Room information

Parameter	Description
Room No.	Enter the room number of the VTH. ◇ The room number consists of 1-5 digits, and must conform to the configured room number on the VTH. ◇ When there are main VTH and extensions, the room number of main VTH ends with -0 and the room number of extension ends with -1, -2 or -3. For example, the main VTH is 101-0, and the room number of the extension is 101-1, 101-2... ◇ If the group call function is not turned on, room number in the format of 9901-xx cannot be set.
First Name	Enter the name of the VTH to help you differentiate VTHs.
Last Name	
Nick Name	
Register Type	Keep them as defaults.
Registered Password	

- Add in batches

1. Click **Batch Add**

2. Configure the parameters.

Figure 3-16 Batch add

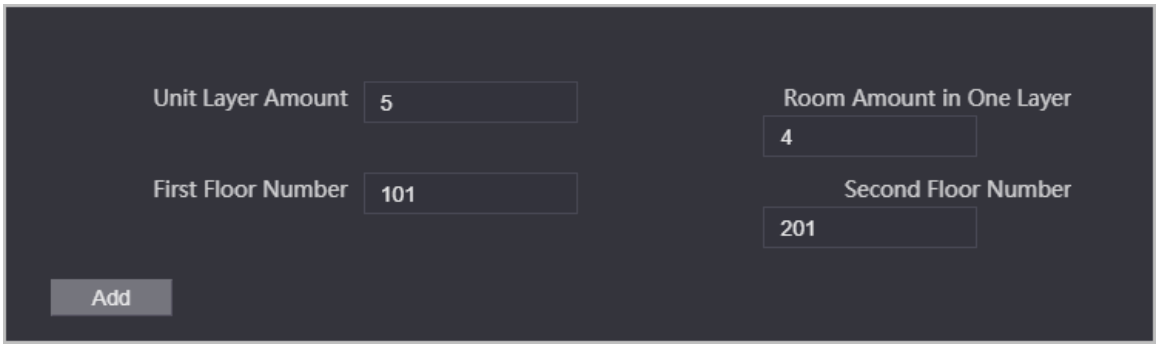


Table 3-10 Batch add

Parameter	Description
Unit Layer Amount	The number of floors of the building (ranging from 1 to 99).
Room Amount in One Layer	The number of rooms on each floor, which ranges from 1 to 99.
First Floor Number	The first room on the first floor.
Second Floor Number	The first room on the second floor, which equals the first room on the first floor plus the number of rooms on each floor.

3.6.5 Adding the VTS

When the Access Controller functions as the SIP Server, you can add VTSs to the SIP server to make sure they can call each other.

Procedure

Step 1 On the Homepage, select **Talkback setting** > **VTS Management**.

Step 2 Click **Add** and set parameters.

Figure 3-17 VTS management

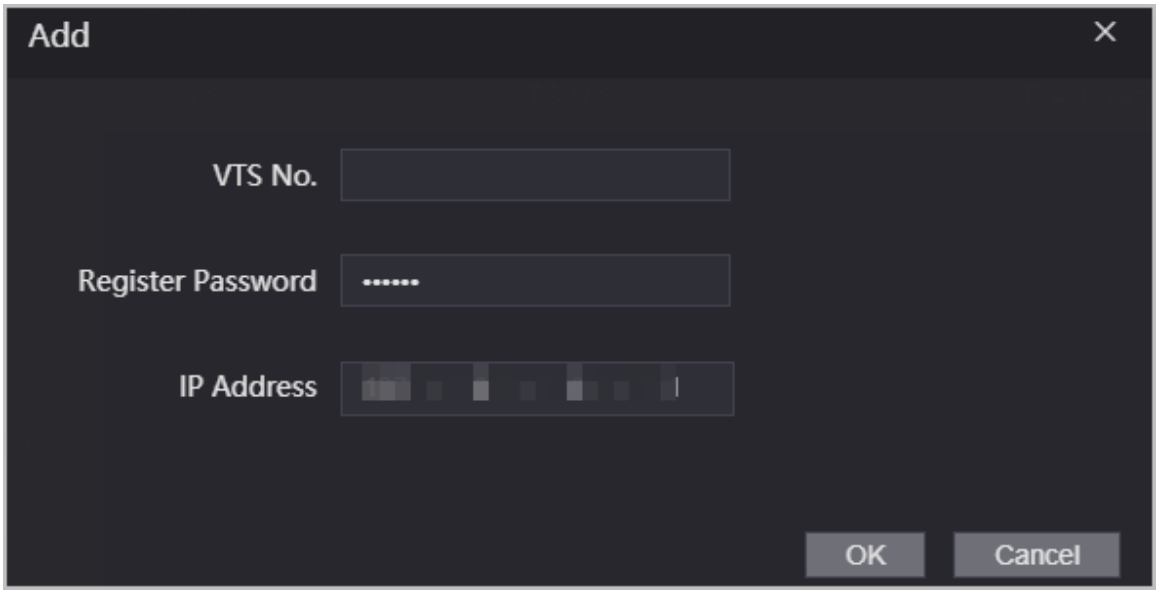


Table 3-11 VTS parameters

Parameter	Description
VTS No.	The number of the VTS, which can have up to 9 digits.
Registration Password	Registration password is the login password of the VTS. We recommend you keep it as default.
IP Address	The IP address of the VTS.

Step 3 Click **OK**.

3.6.6 Viewing Device Status

When the Access Controller works as the SIP Server, you can view the status of devices that are connected the SIP server.

Background Information

On the Homepage, select **Talkback setting** > **Status**.

3.6.7 Viewing Call Logs

View all the record of outgoing calls and incoming calls.

Background Information

On the Homepage, select **Talkback setting** > **Call**.

3.7 Personalization

Configure themes and add video or image resources to the Access Controller.

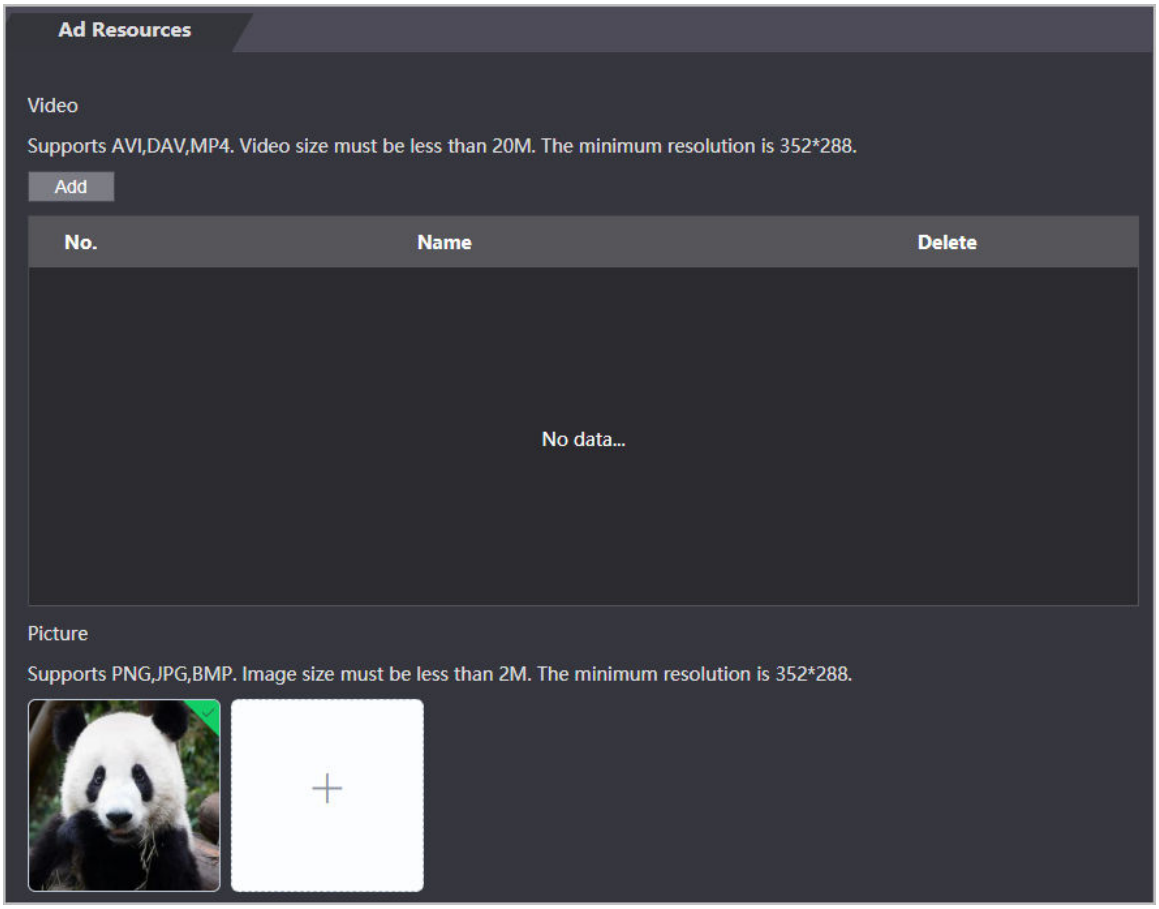
3.7.1 Adding Resources

Add images or videos to be displayed on the standby screen of the Access Terminal.

Procedure

Step 1 On the home page, select **Personalization** > **Ad Resources**.

Figure 3-18 Add resources



Step 2 Add videos or images.

- Add videos.
  1. Click **Add**.
  2. Click **Browse** , select the video file, and then click **Next**.

     ◇ You can upload up to 5 video files.
     ◇ Supports FLV, AVI, ASF, DAV, PS, TS, MP4. Video size must be less than 20 M.
     ◇ Only supports FireFox and the latest version of Chrome to upload video files.
  3. Click **OK**.
- Add images
  1. Click +.

2. Select image from the local and upload it.

   - You can upload up to 10 images.
   - Supports PNG, JPG, BMP. Image size must be less than 2 M.

Related Operations

- Click to delete uploaded images or videos.

  Videos and images in use cannot be deleted.
- Click to preview the uploaded image.

3.7.2 Configuring Theme

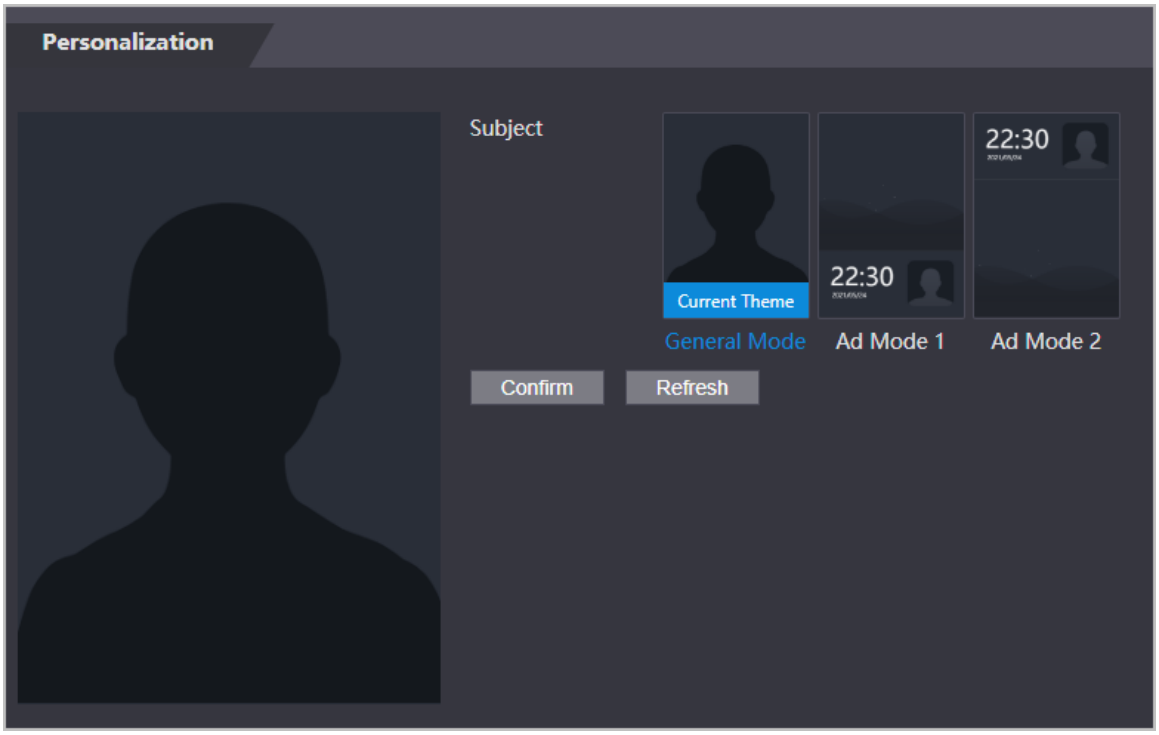
Procedure

Step 1 On the homepage, select **Personalization** > **Personalization**.

Step 2 Select the theme.

- General Mode: Displays the face image in full screen.
- Ad Mode 1: The upper area displays the advertisements, and the lower area displays the time and the face detection box.
- Ad Mode 2: The upper area displays the time and the face detection box., and the lower area displays the advertisements.

Figure 3-19 Theme

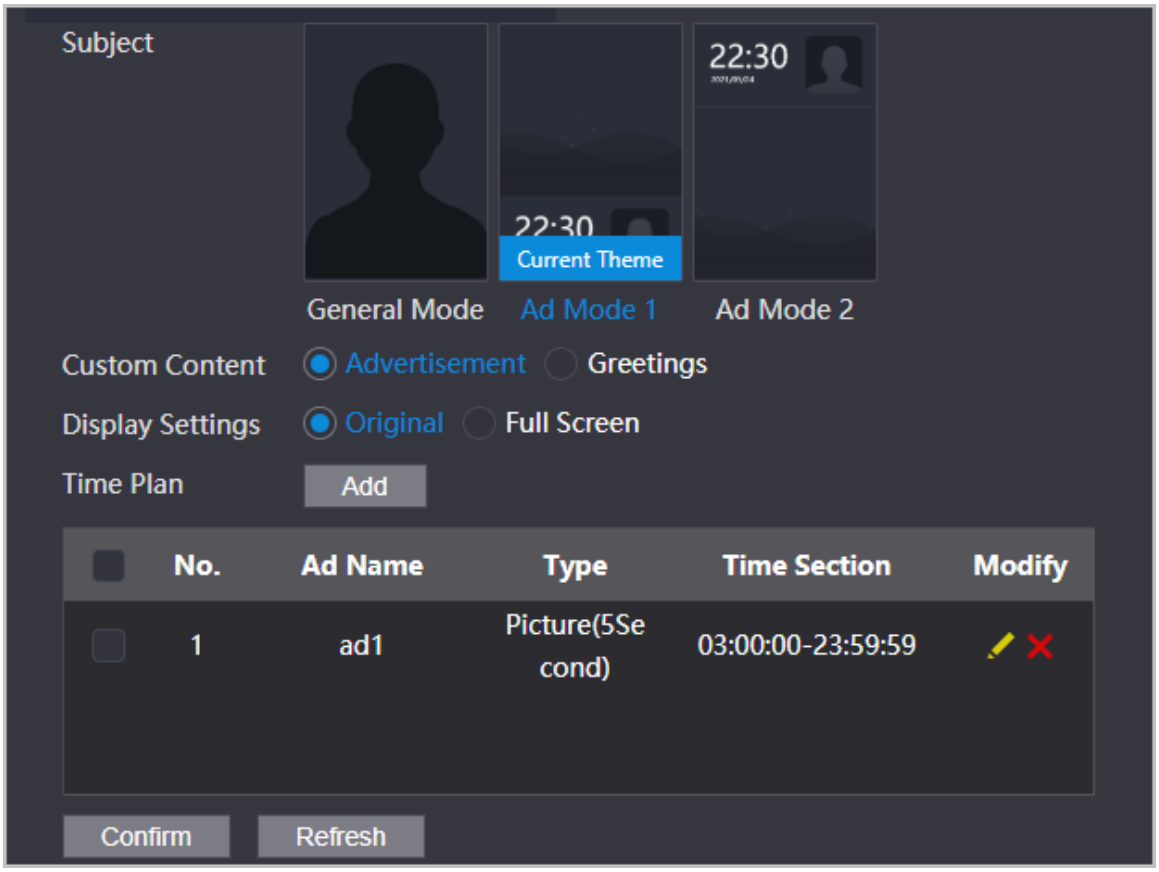


Step 3 Select the voice prompt for successful identity verification.

Step 4 Set advertisement display.

1. Select Ad mode 1 or Ad mode 2, and then select **Advertisement**.

Figure 3-20 Ad mode

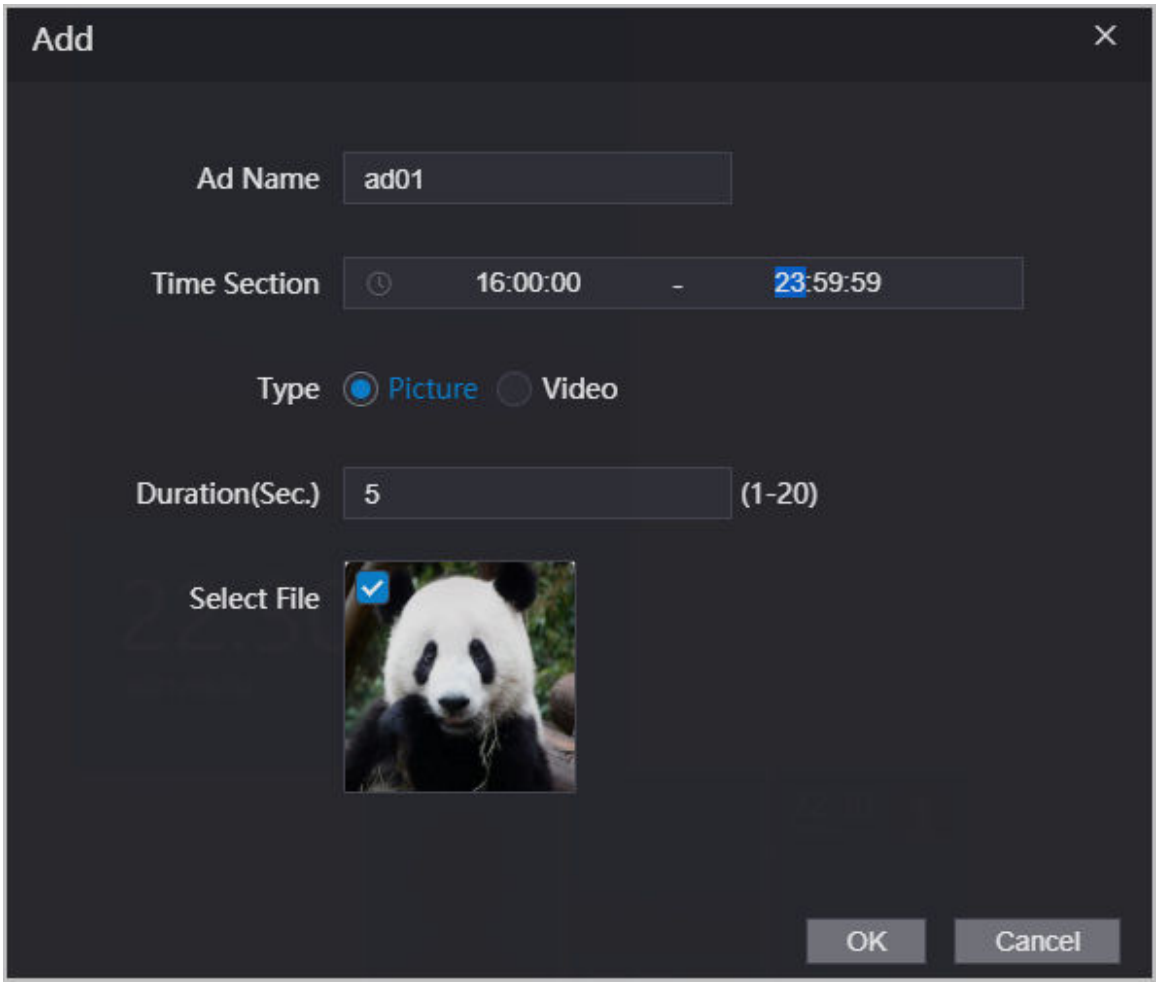


2. Select the display mode.
   - Original: Plays the image and video in the original size.
   - Full Screen: Plays the image and video in full screen.
3. Click **Add** to add time schedules.

   You can add up to 10 schedules.
4. Enter the name of the advertisement,
5. Select the time section, type and file.
6. Enter the duration, and then click **OK**.

   Set the duration for a single picture when pictures are played in a loop. The duration ranges from 1 s to 20 s and it is 5 s by default.
7. Select the type and the file.

Figure 3-21 Add time schedules

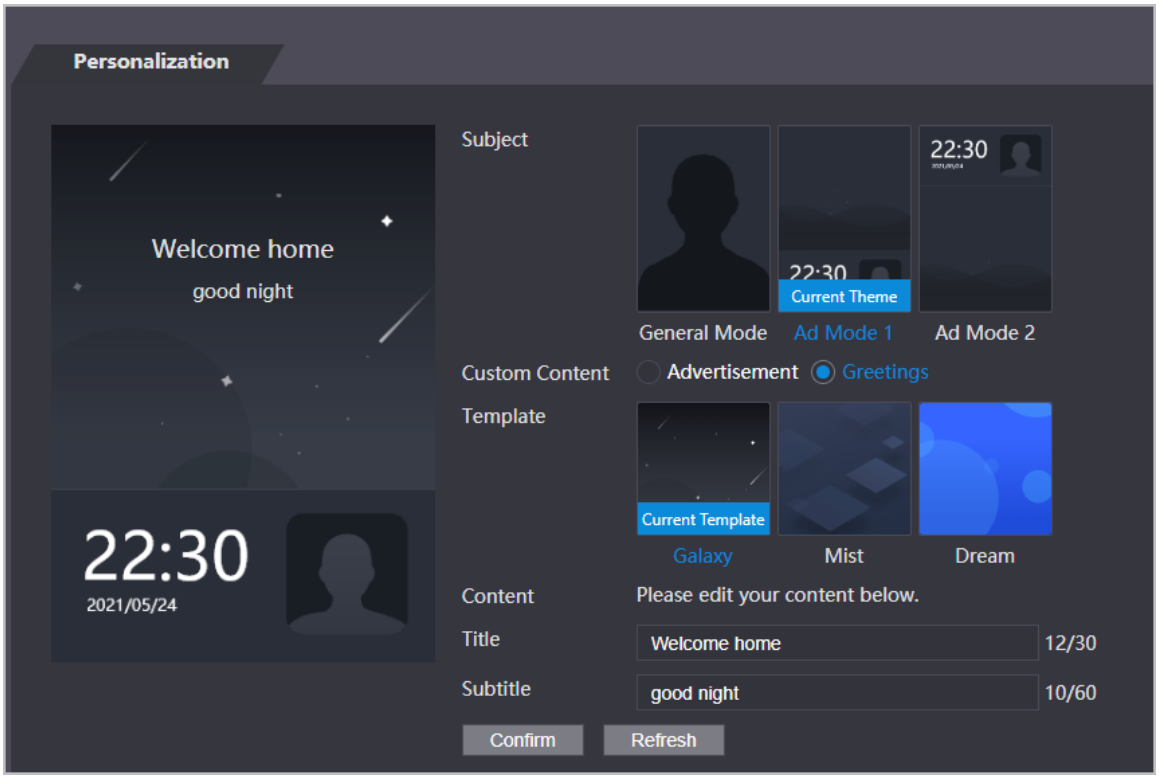


8. Select the added time schedule, and then click **OK**.

Step 5 Configure greetings.

1. Select **Greetings** from the **Custom Content**.
2. Select the template.
3. Enter the title and subtitle.

Figure 3-22 Greetings



4. Click **Confirm**.

3.8 Configuring Time

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

3.8.1 Configuring Time Sections

Background Information

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

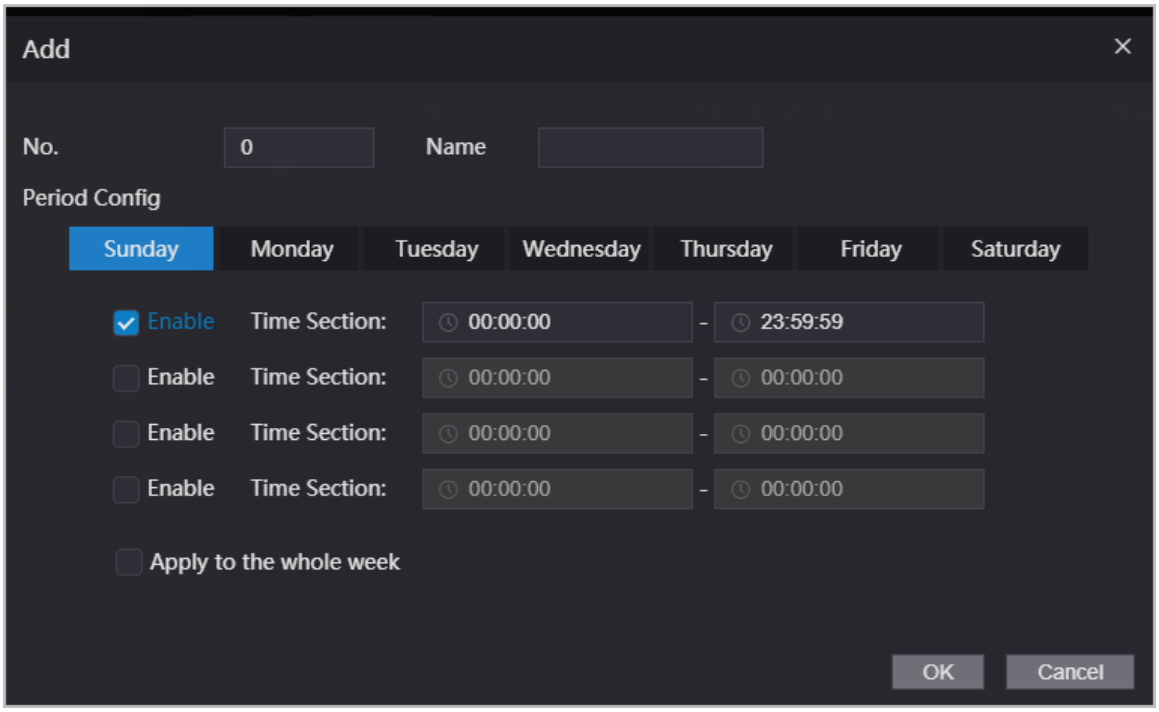
Procedure

Step 1 Log in to the webpage.

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

Step 3 Click **Add**.

Figure 3-23 Time section parameters



Step 4 Enter No. and name for the time section.

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

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

Step 5 Configure time sections for each day.

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

Step 7 Click **OK**.

3.8.2 Configuring Holiday Groups

Background Information

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

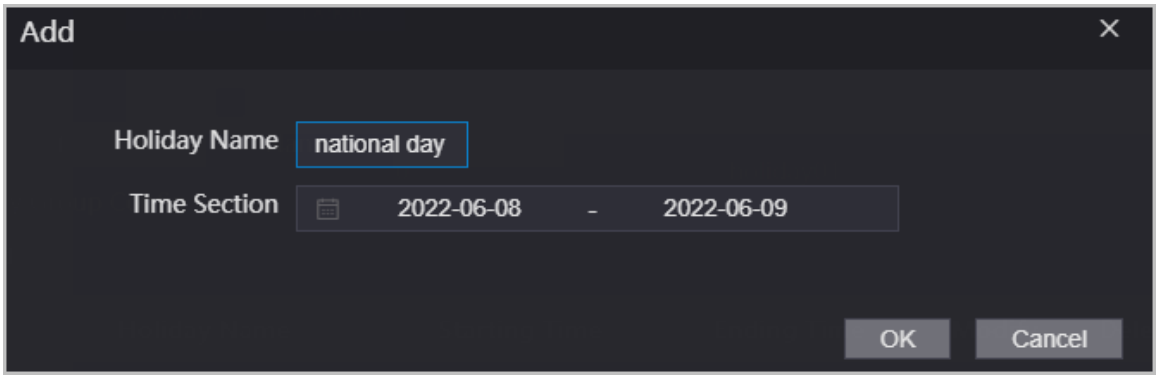
Procedure

Step 1 Log in to the webpage.

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

Step 3 Click **Add**.

Figure 3-24 Add a holiday group



Step 4 Set the name and the time for the holiday group.

- **Holiday Name** : Enter the name of the holiday group. Enter a name for each time section. You can enter a maximum of 32 characters (contain numbers, special characters and English characters).
- **Time Section** : Select the start time and end time of the holiday.

Step 5 Click **OK**.

You can add multiple holidays in a holiday group.

Step 6 Click **OK**.

3.8.3 Configuring Holiday Plans

Background Information

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

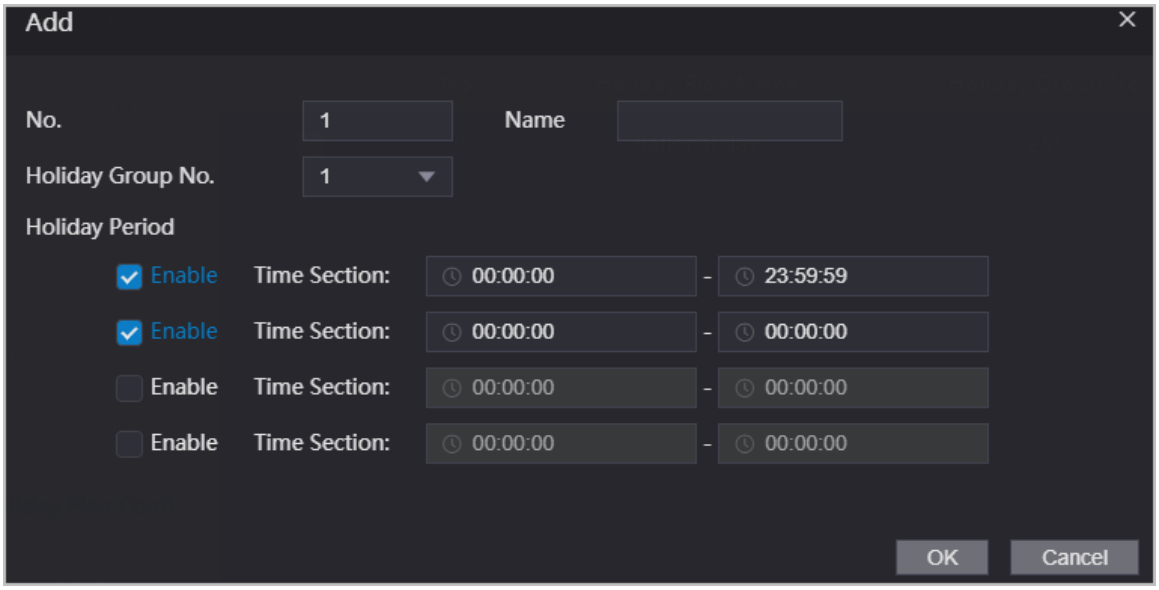
Procedure

Step 1 Log in to the webpage.

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

Step 3 Click **Add**.

Figure 3-25 Add holiday plan



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

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

Step 5 In the **Holiday Group No.** list, select the number of the defined holiday group.

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

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

Step 7 Click **OK**.

3.9 Data Capacity

You can see how many users, cards and face images that the Access Controller can store.

Log in to the webpage and select **Data Capacity**.

Figure 3-26 Data capacity

3.10 Configuring Video and Image

Configure video and image parameters, such as stream and brightness.

Background Information

We recommend you use the default parameters in this section.

3.10.1 Configuring Video

On the home page, select **Video Setting**, and then configure the video stream, status, image and exposure.

Background Information

- Video Standard: Select **NTSC**.
- Channel Id: Channel 1 is for configurations of visible light image. Channel 2 is for configurations of infrared light image.
- Default: Restore to defaults settings.
- Capture: Take a snapshot of the current image.

PAL video standard is 25 fps and the NTSC video standard is 30 fps.

3.10.1.1 Configuring Channel 1

Procedure

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

Step 2 Select **1** from the **Channel No.** list.

Step 3 Configure the date rate.

Figure 3-27 Date rate

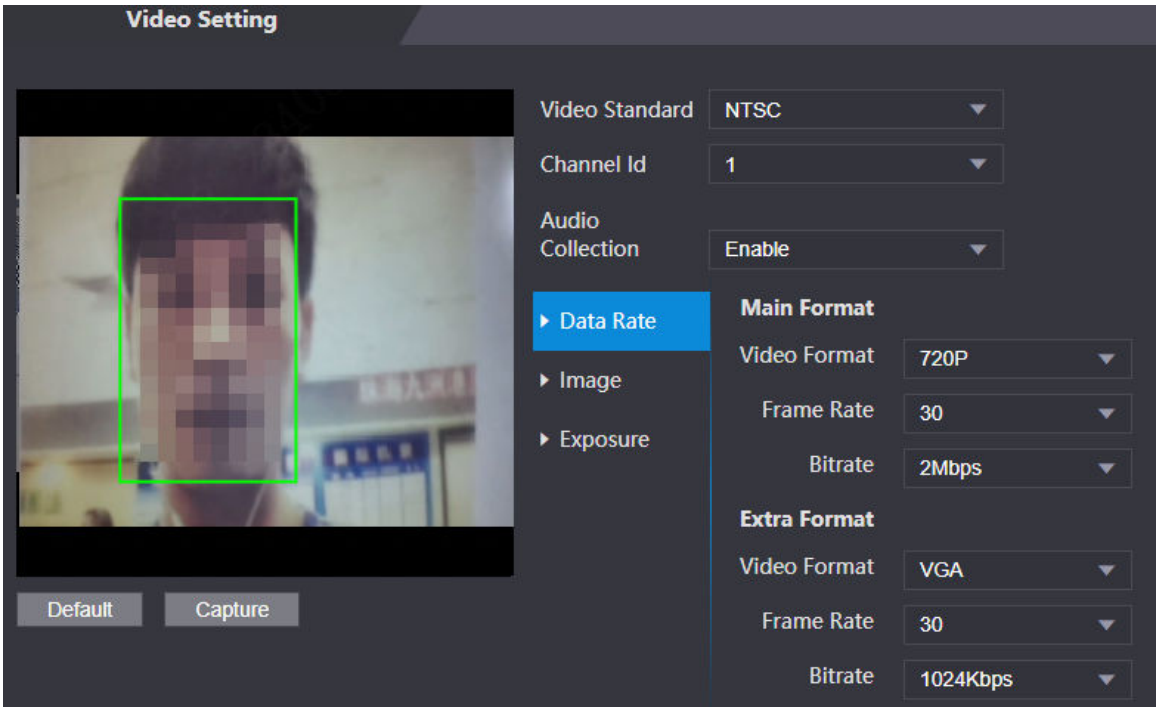


Table 3-12 Date rate description

Parameter		Description
Main Format	Video Format	When the Access Controller functions as the a VTO and connects the VTH, the acquired stream limit of VTH is 720p.When resolution is changed to 1080p, the call and monitor function might be affected.
	Frame Rate	The number of frames (or images) per second. The frame rate range is 1–25 fps.
	Bitrate	It indicates the amount of data transmitted over an internet connection in a given amount of time. Select a proper bandwidth based on your network speed.
Extra Stream	Video Format	The sub-stream supports D1, VGA and QVGA.
	Frame Rate	The number of frames (or images) per second. The frame rate range is 1–25 fps.
	Bitrate	It indicates the amount of data transmitted over an internet connection in a given amount of time.

Step 4 Configure the image.

Figure 3-28 Image

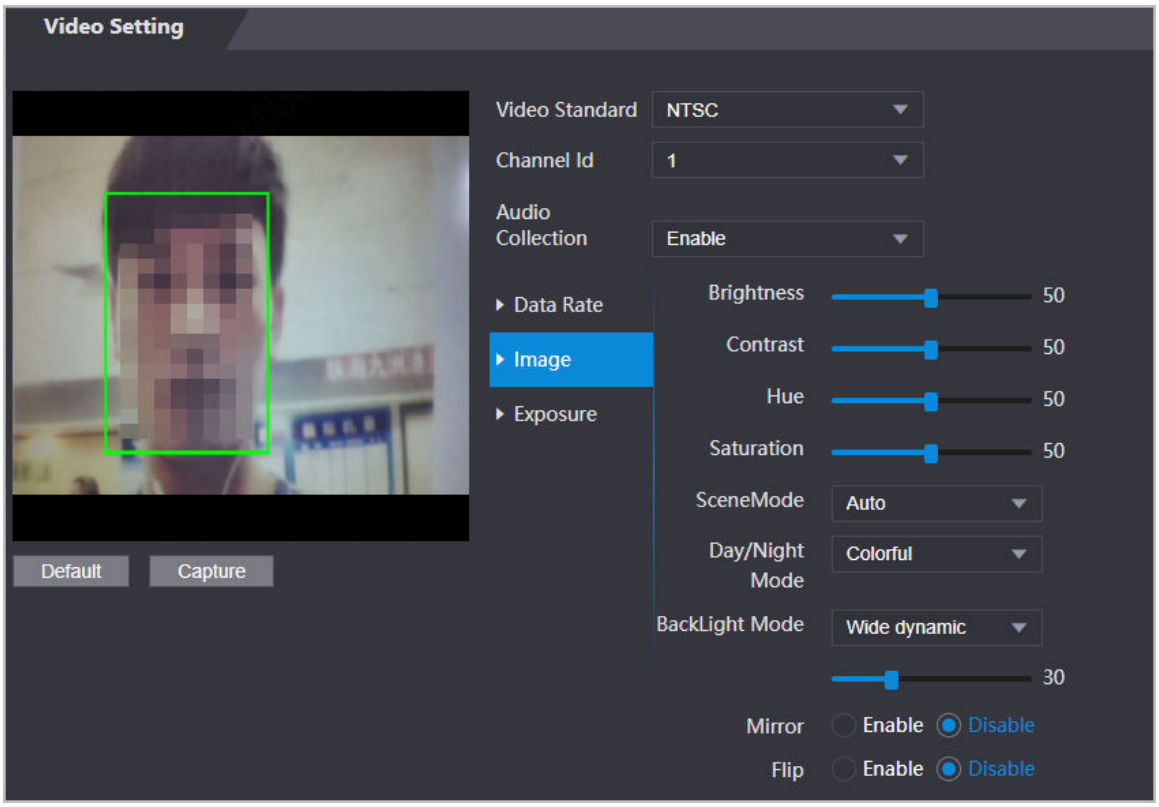


Table 3-13 Image description

Parameter	Description
Brightness	Brightness is the relative lightness or darkness of a particular color. The larger the value is, the brighter the image will be.
Contrast	Contrast is the difference in the luminance or color that makes an object distinguishable. The larger the contrast value is, the greater the color contrast will be.
Hue	Refers to the strength or saturation of a color. It describes the color intensity, or how pure it is.
Saturation	Color saturation indicates the intensity of color in an image. As the saturation increases, the color appears stronger, for example being more red or more blue. The saturation value does not change image brightness.
Scene Mode	The image hue is different in different scene mode. • **Close** : Scene mode function is turned off. • **Auto** : The system automatically adjusts the scene mode based on the photographic sensitivity. • **Sunny** : In this mode, image hue will be reduced. • **Night** : In this mode, image hue will be increased.
Day/Night	Day/Night mode affects light compensation in different situations. • **Auto** : The system automatically adjusts the day/night mode based on the photographic sensitivity. • **Colorful** : In this mode, images are colorful. • **Black and white** : In this mode, images are in black and white.
Backlight Mode	• **Close** : Backlight compensation is turned off. • **Backlight** : Backlight compensation automatically brings more light to darker areas of an image when bright light shining from behind obscures it. • **Wide dynamic** : The system dims bright areas and compensates for dark areas to create a balance to improve the overall image quality. • **Inhibition** : Highlight compensation (HLC) is a technology used in CCTV/IP security cameras to deal with images that are exposed to lights like headlights or spotlights. The image sensor of the camera detects strong lights in the video and reduces exposure in these spots to enhance the overall quality of the image.
Mirror	When the function is turned on, images will be displayed with the left and right side reversed.
Flip	When this function is turned on, images can be flipped over.

Step 5 Configure the exposure parameters.

Figure 3-29 Exposure

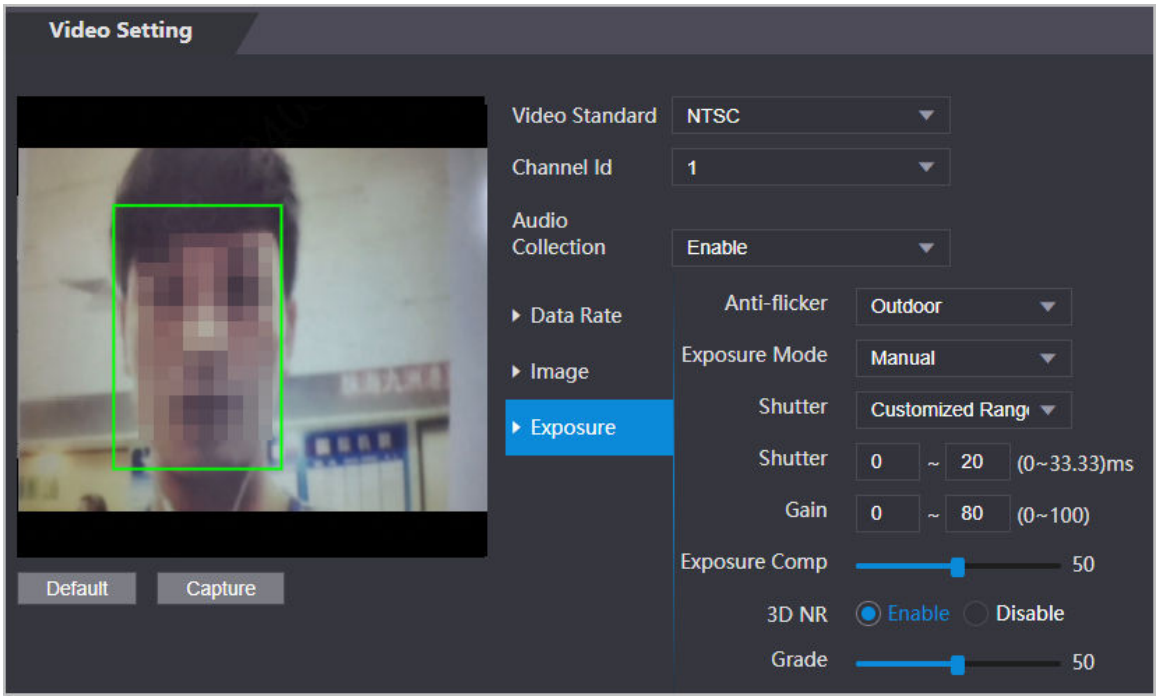


Table 3-14 Exposure parameter description

Parameter	Description
Anti-flicker	Set anti-flicker to reduce flicker and reduce uneven colors or exposure. ● **50Hz** : When the mains power supply is 50 Hz, the exposure is automatically adjusted to prevent the appearance of horizontal lines. ● **60Hz** : When the mains power supply is 60 Hz, the exposure is automatically adjusted to reduce the appearance of horizontal lines. ● **Outdoor** : When **Outdoor** is selected, the exposure mode can be switched.
Exposure Mode	You can set the exposure to adjust image brightness. ● **Auto** : The Access Controller automatically adjusts the brightness of images. ● **Shutter Priority** : The Access Terminal will adjust image brightness according to shutter exposure range. If the image brightness is not enough and the shutter value has reached its upper or lower limit, the Access Controller will adjust the gain value automatically for ideal brightness level. ● **Manual** : You can configure gain and shutter value manually to adjust image brightness. ◇ When you select **Outdoor** from the **Anti-flicker** list, you can select **Shutter Priority** as the exposure mode. ◇ Exposure mode might differ depending on different models of Access Controller.

Parameter	Description
Shutter	Shutter is a component that allows light to pass for a determined period. The higher the shutter speed, the shorter the exposure time, and the darker the image.
Gain	When the gain value range is set, video quality will be improved.
Exposure Compensation	You can make a photo brighter or darker by adjusting exposure compensation value.
3D NR	When 3D Noise Reduction (RD) is turned on, video noise can be reduced to ensure high definition videos. You can set its grade when this function is turned on.
Grade	

3.10.1.2 Configuring Channel 2

Procedure

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

Step 2 Select 2 from the **Channel No.**.

Step 3 Configure the video status.

We recommend you turn on the WDR function when the face is in back-lighting.

Figure 3-30 Image

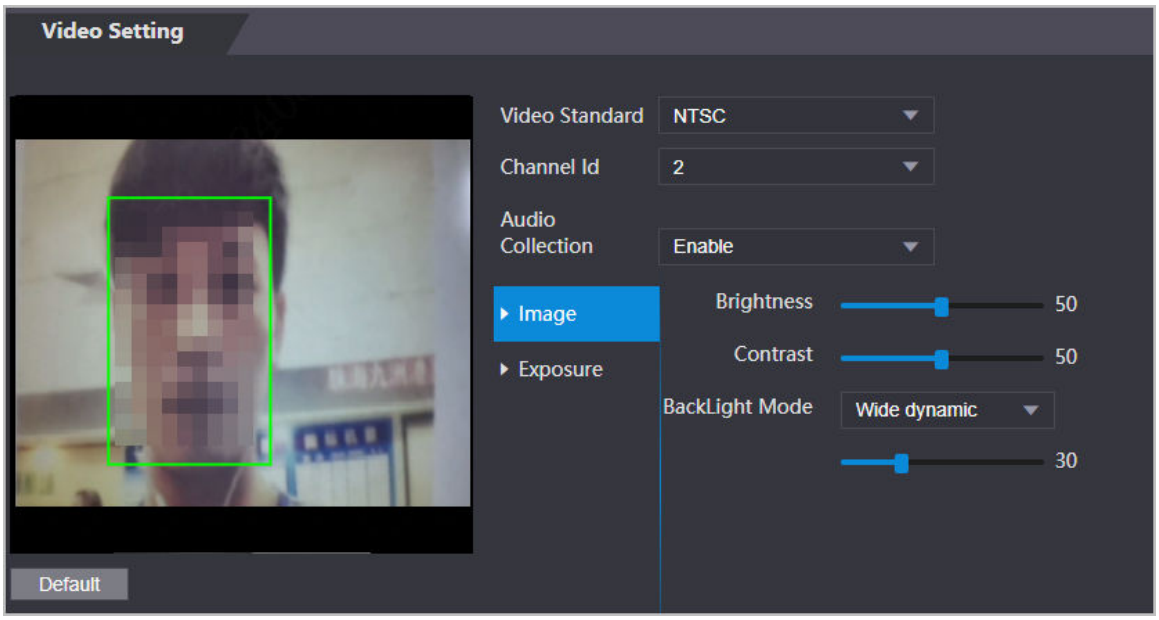


Table 3-15 Image description

Parameter	Description
Brightness	Brightness is the relative lightness or darkness of a particular color. The larger the value is, the brighter the image will be.

Parameter	Description
Contrast	Contrast is the difference in the luminance or color that makes an object distinguishable. The larger the contrast value is, the greater the color contrast will be.
Backlight Mode	• **Close** : Back-light compensation is turned off. • **Backlight** : Black-light compensation automatically brings more light to darker areas of an image when bright light shining from behind obscures it. • **Wide dynamic** : The system dims bright areas and compensates for dark areas to ensure to create a balance to improve the overall image quality. • **Inhibition** : Highlight compensation (HLC) is a technology used in CCTV/IP security cameras to deal with images that are exposed to lights like headlights or spotlights. The image sensor of the camera detects strong lights in the video and reduce exposure in these spots to enhance the overall quality of the image.

Step 4 Configure the exposure parameters.

Figure 3-31 Exposure parameter

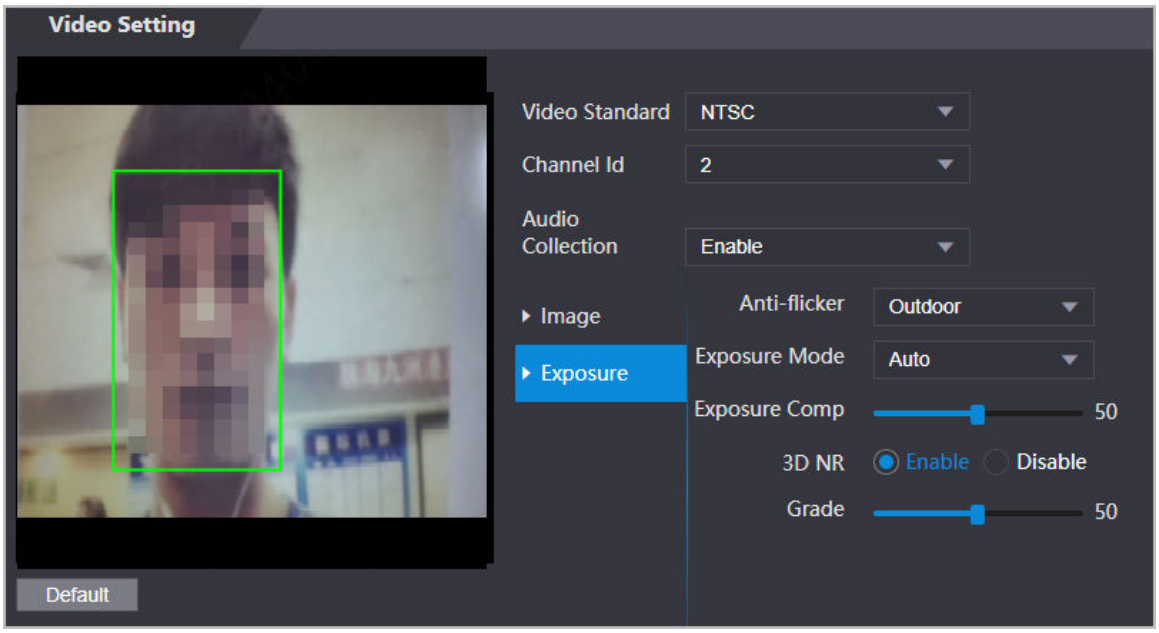


Table 3-16 Exposure parameter description

Parameter	Description
Anti-flicker	Set anti-flicker to reduce flicker and decrease or eliminate uneven colors or exposure. • **50Hz** : When the mains power supply is 50 Hz, the exposure is automatically adjusted to prevent the appearance of horizontal lines. • **60 Hz** : When the mains power supply is 60 Hz, the exposure is automatically adjusted to reduce the appearance of horizontal lines. • **Outdoor** : When **Outdoor** is selected, the exposure mode can be switched.
Exposure Mode	You can set the exposure to adjust image brightness. • **Auto** : The Access Controller automatically adjusts the brightness of images. • **Shutter Priority** : The Access Terminal will adjust image brightness according to shutter exposure range. If the image brightness is not enough and the shutter value has reached its upper or lower limit, the Access Controller will adjust the gain value automatically for ideal brightness level. • **Manual** : You can configure gain and shutter value manually to adjust image brightness. ◇ When you select **Outdoor** from the **Anti-flicker** list, you can select **Shutter Priority** as the exposure mode. ◇ Exposure model might differ depending on different models of Access Controller.
Shutter	Shutter is a device that allows light to pass for a determined period. The higher the shutter speed, the shorter the exposure time, and the darker the image.
Gain	When the gain value range is set, video quality will be improved.
Exposure Compensation	You can make a photo brighter or darker by adjusting exposure compensation value.
3D NR	When 3D Noise Reduction (RD) is turned on, video noise can be reduced to ensure high definition videos. You can set its grade when this function is turned on.
Grade	

3.10.2 Setting Volume

Background Information

You can adjust the volume of the speaker.

Procedure

Step 1 Log in to the webpage.

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

Step 3 Drag the slider the adjust the volume.

Step 4 Click **OK**.

3.10.3 Configuring Local Coding

Configure the monitoring area on the VTO, and the VTH can provide a real-time monitoring screen.

Background Information

To avoid video data loss, we recommend you turn on the local coding function when the VTO is connected to VTH.

Procedure

Step 1 Select **Video & Audio** > **Local Coding**.

Step 2 Select **Enable** to turn on the function.

Step 3 Click **OK**.

3.10.4 Configuring Image Mode

Select the image mode based on the installation site of Access Controller.

Procedure

Step 1 On the home page, select **Video Setting** > **Image Mode**.

Step 2 Select image mode according to the installation location of the Access Controller.

- Indoor: The Access Controller is installed indoor such as offices. The artificial light is even across the room and there is no daylight.
- Outdoor: The Access Controller is installed outdoor and the daylight is bright and even.
- Other: The human face is in back-lighting, which makes the face dim. We recommend you select other mode to make it easier for the Access Controller to detect.

Step 3 Click **OK**.

3.11 Configuring Face Detection

Background Information

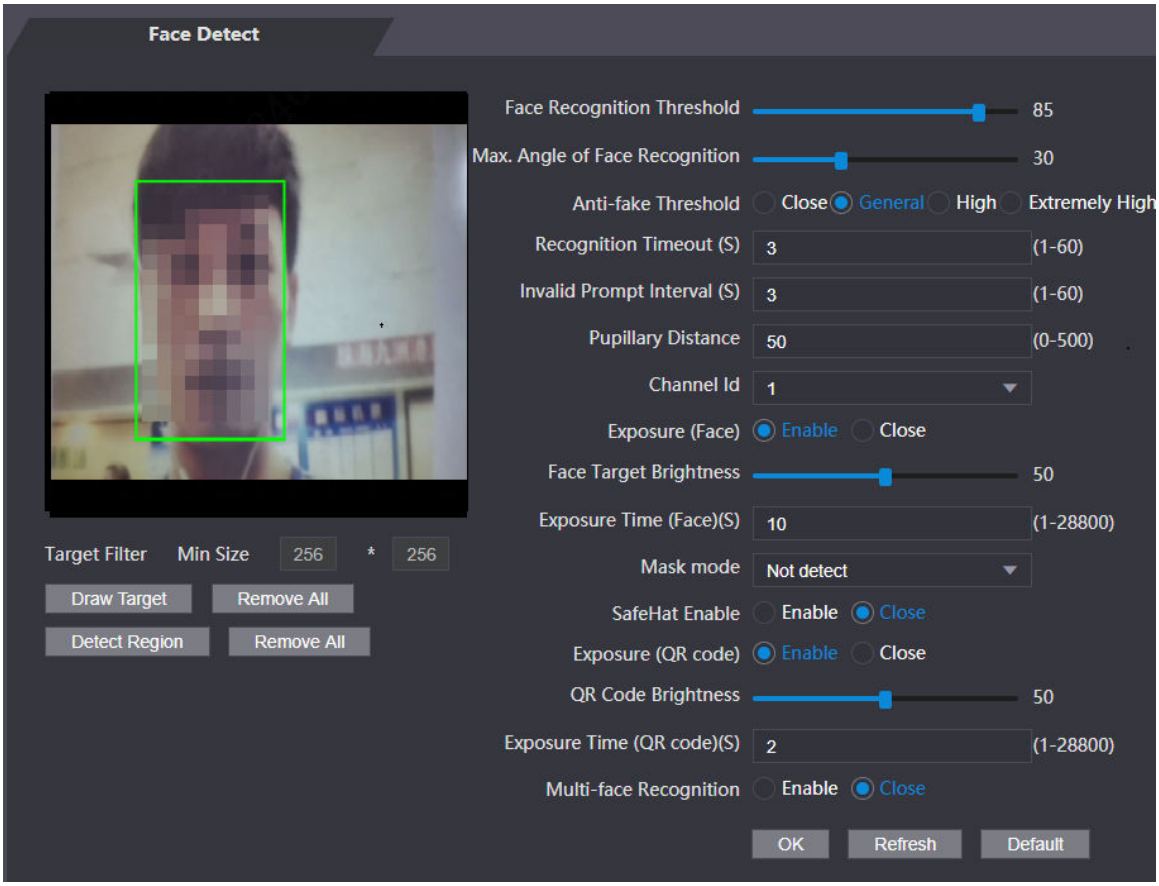
You can configure human face related parameters on this interface to increase the accuracy of the face recognition.

Procedure

Step 1 Log in to the webpage.

Step 2 Select **Face Detect**.

Figure 3-32 Face detect



Step 3 Configure the parameters.

Table 3-17 Description of face detection parameters

Parameter	Description
Face Recognition Threshold	Adjust the face recognition accuracy. Higher threshold means higher accuracy.
Max. Angle of Face Recognition	Set the maximum face pose angle for face detection. Larger value means larger face angle range. If the face pose angle is out of the defined range, the face detection box will not appear.
Anti-fake Threshold	Avoid false face recognition when people using a photo, video, mask or a different substitute for an authorized person's face. • Close: Turns off this function. • General: Normal level of anti-spoofing detection means higher door access rate for people with face masks. • High: Higher level of anti-spoofing detection means higher accuracy and security. • Extremely High: Extremely high level of anti-spoofing detection means extremely high accuracy and security.

Parameter	Description
Recognition Timeout (S)	If a person with access permission has their face successfully recognized, the Access Controller will prompt face recognition success. You can enter the prompt interval time.
Invalid Prompt Interval (S)	If a person without access permission attempts to unlock the door for several times in the defined interval, the Access Controller will prompt face recognition failure. You can enter the prompt interval time.
Pupillary Distance	Face images require desired pixels between the eyes (called pupillary distance) for successful recognition. The default pixel is 45. The pixel changes according to the face size and the distance between faces and the lens. If an adult is 1.5 meters away from the lens, the pupillary distance can be 50 px–70 px.
Channel Id	1 is for the white light camera and 2 is for the IR light camera.
Exposure (Face)	After face exposure is enabled, human faces 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	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.
Mask Mode	• **No detect** : Mask is not detected during face recognition. • **Mask reminder** : Mask is detected during face recognition. If the person does not wear a mask, the system will give them a reminder to wear masks, and access is allowed. • **Mask intercept** : Mask is detected during face recognition. If a person is not wearing a mask, the system will give them a reminder to wear masks, and access is denied.
SafeHat Enable	Detects whether people wear safe hats.
Exposure (QR code)	When the Access Controller is installed outdoors, the QR code will be clearer based on the defined QR code brightness when you scan it.
QR code Brightness	
Exposure Time (QR code) (S)	After a QR code is scanned, the Access Controller will give out light to illuminate the QR code, and the Access Controller will not give out light again until the defined exposure time has passed.
Multi-face Recognition	Supports detecting 6 face images at the same time, and the unlock combinations mode becomes invalid. The door is unlocked after any one of them gain access.
Draw Target	• Click **Draw Target**, and then draw the minimum face detection frame. • Click **Remove All**, and you can remove all the frames you drew.

Parameter	Description
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 Draw the face detection box.

1. Click **Draw Target**,
2. Draw a rectangle by dragging the mouse and then release the left mouse button.

   The target in the defined area will be detected.

Step 5 Draw the target size.

1. Click **Draw target**
2. Right-click to draw the face recognition box to define the minimum size of detected face.

   Only when the size of the face is larger than the defined size, the face can be detected by the Access Controller.

Step 6 Click **OK**.

3.12 Configuring Network

3.12.1 Configuring TCP/IP

Background Information

You need to configure IP address of Access Controller to make sure that it can communicate with other devices.

Procedure

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

Step 2 Configure parameters.

Figure 3-33 TCP/IP

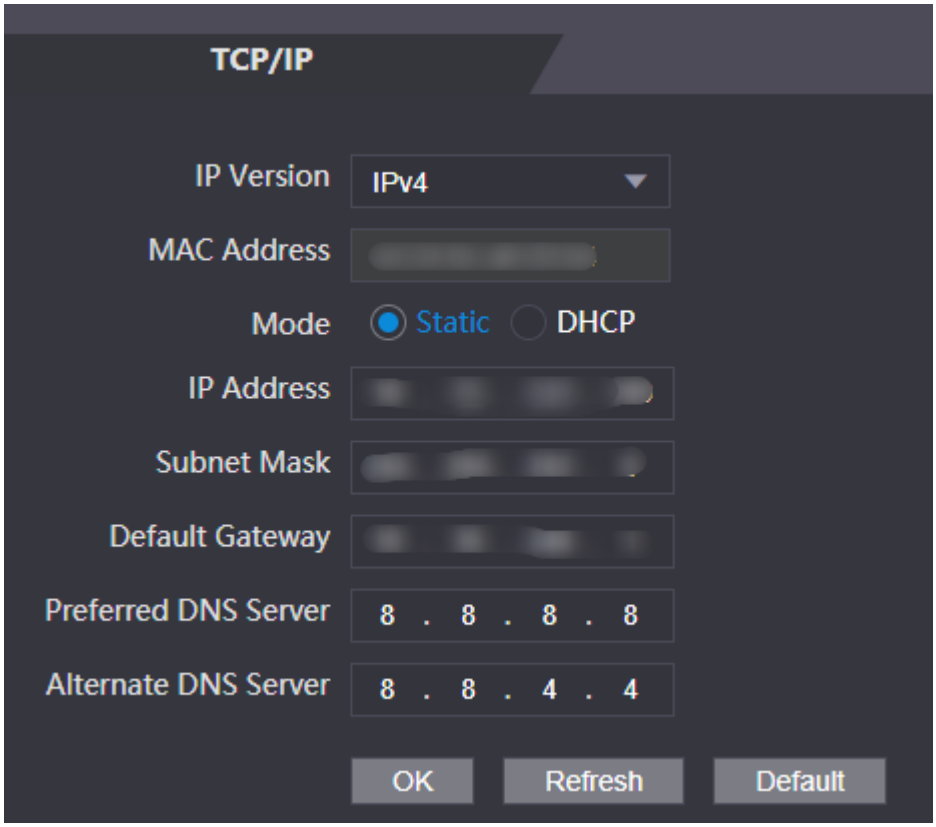


Table 3-18 Description of TCP/IP

Parameter	Description
IP Version	IPv4
MAC Address	MAC address of the Access Controller.
Mode	• **Static** : Manually enter IP address, subnet mask, and gateway. • **DHCP** : It stands for Dynamic Host Configuration Protocol. When DHCP is turned on, the Access Controller will automatically be assigned with IP address, subnet mask, and gateway.
IP Address	If you select static mode, configure the IP address, subnet mask and gateway. IP address and gateway must be on the same network segment.
Subnet Mask	
Default Gateway	
Preferred DNS	Set IP address of the preferred DNS server.
Alternate DNS	Set IP address of the alternate DNS server.

Step 3 Click **OK**.

3.12.2 Configuring Port

Background Information

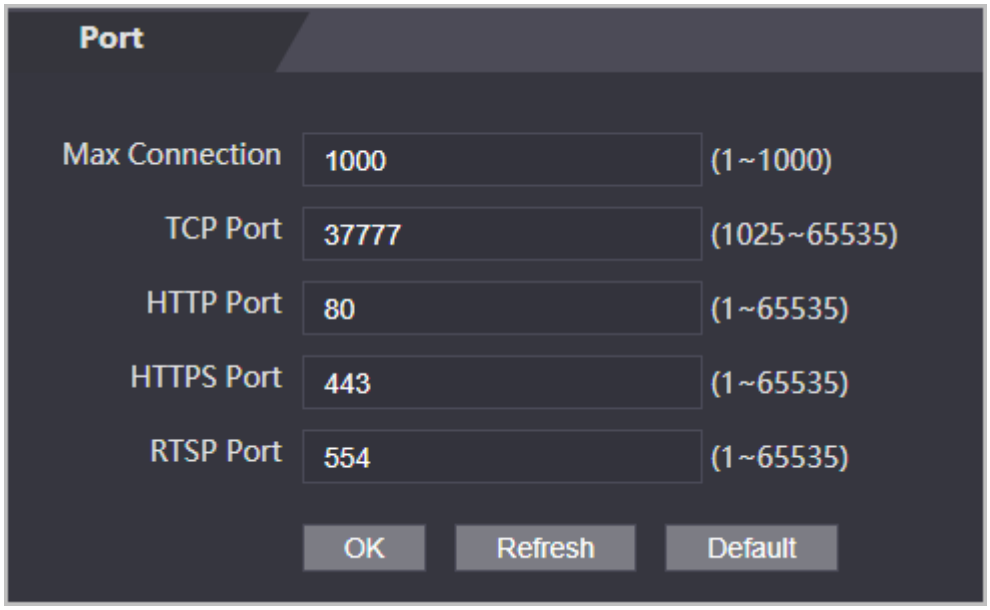
You can limit access to the Access Controller at the same through web, desktop client and phone.

Procedure

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

Step 2 Configure port numbers.

Figure 3-34 Configure ports



Except **Max Connection** and **RTSP Port**, you need to restart the Access Controller to make the configurations effective after you change other parameters.

Table 3-19 Description of ports

Parameter	Description
Max Connection	You can set the maximum number of clients (such as web, desktop client and phone) that can access the Access Terminal at the same time.
TCP Port	Default value is 37777.
HTTP Port	Default value is 80. If you want to change the port number, add the new port number after the IP address when you log in to the webpage.
HTTPS Port	Default value is 443.
RTSP Port	Default value is 554.

Step 3 Click **OK**.

3.12.3 Configuring Automatic Registration

Background Information

The Access Controller reports its address to the designated server so that you can get access to the Access Controller through the management platform.

Procedure

Step 1 On the home page, select **Network Setting** > **Register**.

Step 2 Enable the automatic registration function and configure the parameters.

Figure 3-35 Register

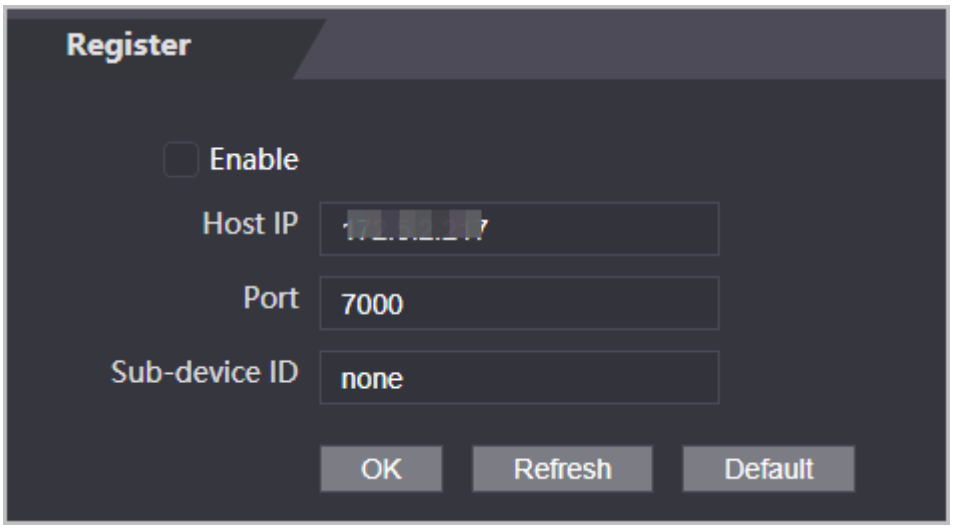


Table 3-20 Automatic registration description

Parameter	Description
Host IP	The IP address or the domain name of the server.
Port	The port of the server used for automatic registration.
Sub-Device ID	Enter the sub-device ID (user defined). When you add the Access Controller to the management platform, the sub-device ID on the management platform must conform to the defined sub-device ID on the Access Controller.

Step 3 Click **Apply**.

3.12.4 Configuring Cloud Service

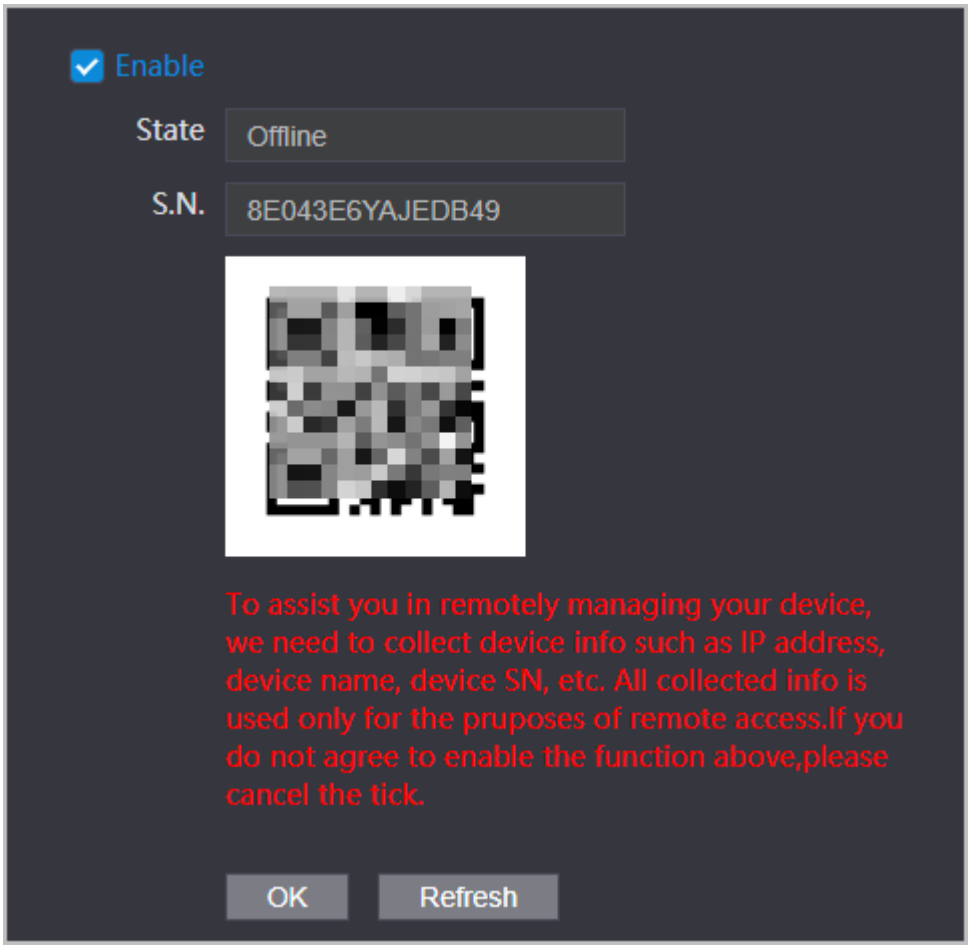
The cloud service provides a NAT penetration service. Users can manage multiple devices through DMSS. You do not have to apply for dynamic domain name, configuring port mapping or deploying server.

Procedure

Step 1 On the home page, select **Network Setting** > **Cloud Service**.

Step 2 Turn on the cloud service function.

Figure 3-36 Cloud service



Step 3 Click **OK**.

Related Operations

Download DMSS and sign up, you can scan the QR code through DMSS to add the Access Controller to it.

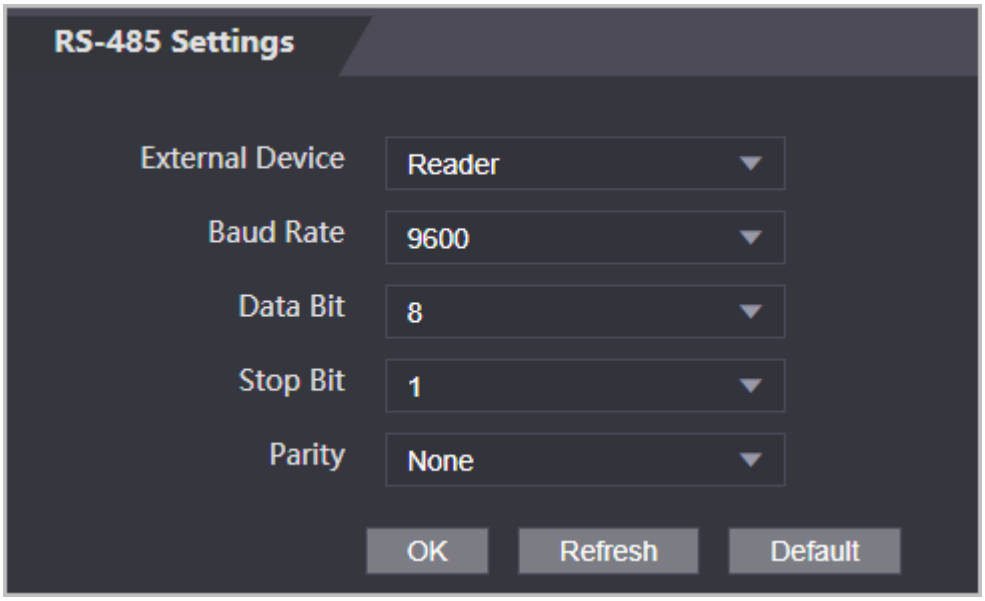
3.12.5 Configuring Serial Port

Procedure

Step 1 On the home page, select **Network Setting** > **Wiegand serial port setting**.

Step 2 Select a port type.

Figure 3-37 Serial port



- Select **Reader** when the Access Controller connects to a card reader.
- Select **Controller** when the Access Controller functions as a card reader, and the Access Controller will send data to the Access Controller to control access.

  Output Data type:

  - Card: Outputs data based on card number when users swipe card to unlock door; outputs data based on user's first card number when they use other unlock methods.
  - No.: Outputs data based on the user ID.
- Select **Reader (OSDP)** when the Access Controller is connected to a card reader based on OSDP protocol.
- Security Module: When a security module is connected, the exit button, lock and fire alarm linkage will be not effective.

3.12.6 Configuring Wiegand

Background Information

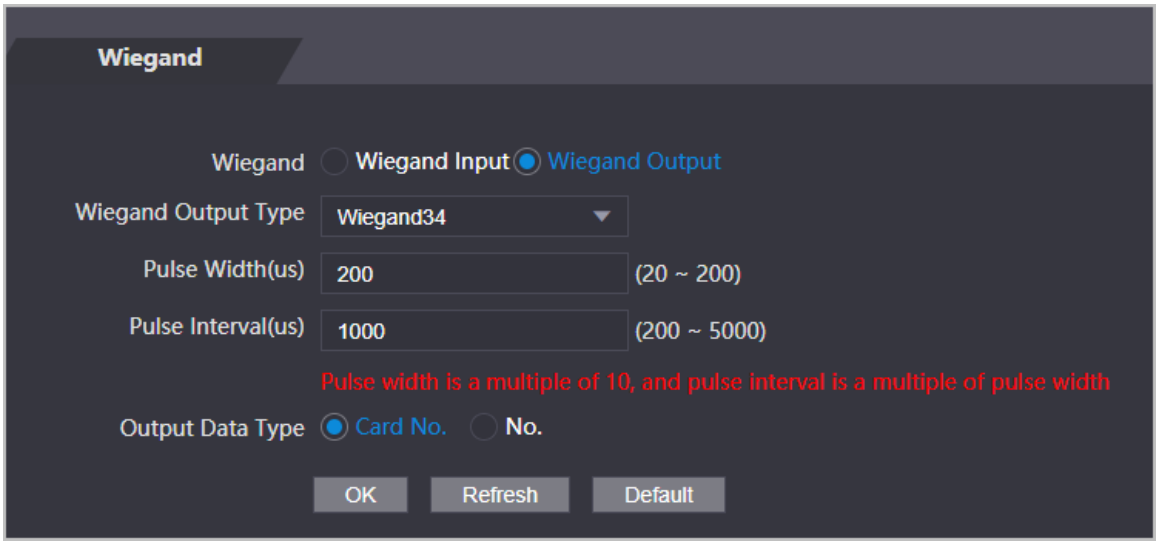
The access controller allows for both Wiegand input and Output mode.

Procedure

Step 1 On the **Main Menu**, select **Connection** > **Wiegand**.

Step 2 Select a Wiegand.

Figure 3-38 Wiegand output



- Select **Wiegand Input** when you connect an external card reader to the Access Controller.
- Select **Wiegand Output** when the Access Controller functions as a card reader, and you need to connect it to a controller or another access terminal.

Table 3-21 Description of Wiegand output

Parameter	Description
Wiegand Output Type	Select a Wiegand format to read card numbers or ID numbers. • **Wiegand26** : Reads three bytes or six digits. • **Wiegand34** : Reads four bytes or eight digits. • **Wiegand66** : Reads eight bytes or sixteen digits.
Pulse Width	Enter the pulse width and pulse interval of Wiegand output.
Pulse Interval	
Output Data Type	Select the type of output data. • **User ID** : Outputs data based on user ID. • **Card No.** : Outputs data based on user's first card number.

3.13 Safety Management

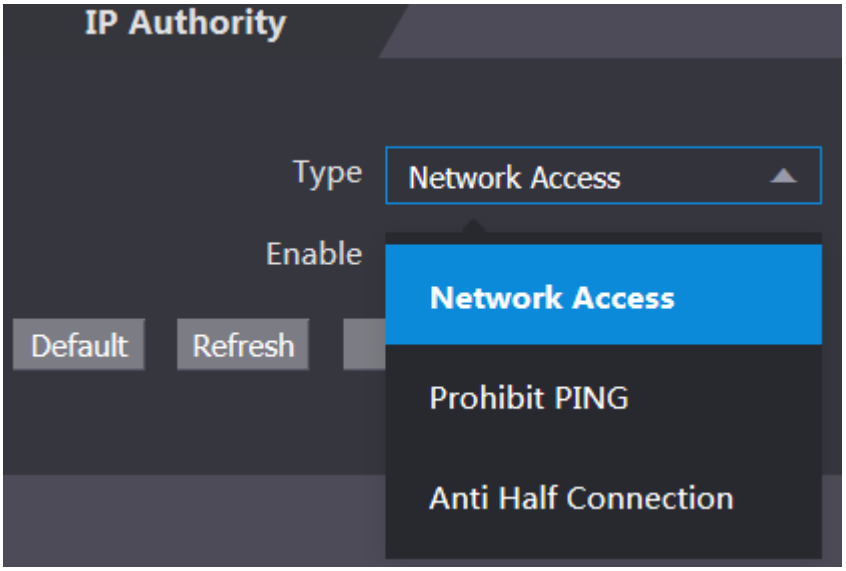
3.13.1 Configuring IP Authority

Procedure

Step 1 Log in to the webpage.

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

Figure 3-39 IP authority



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

- **Network Access** : Set allowlist and blocklist to control access to the access controller.
- **Prohibit PING** : Enable **PING prohibited** function, and the access controller will not respond to the Ping request.
- **Anti Half Connection** : Enable **Anti Half Connection** function, and the access controller can still function properly under half connection attack.

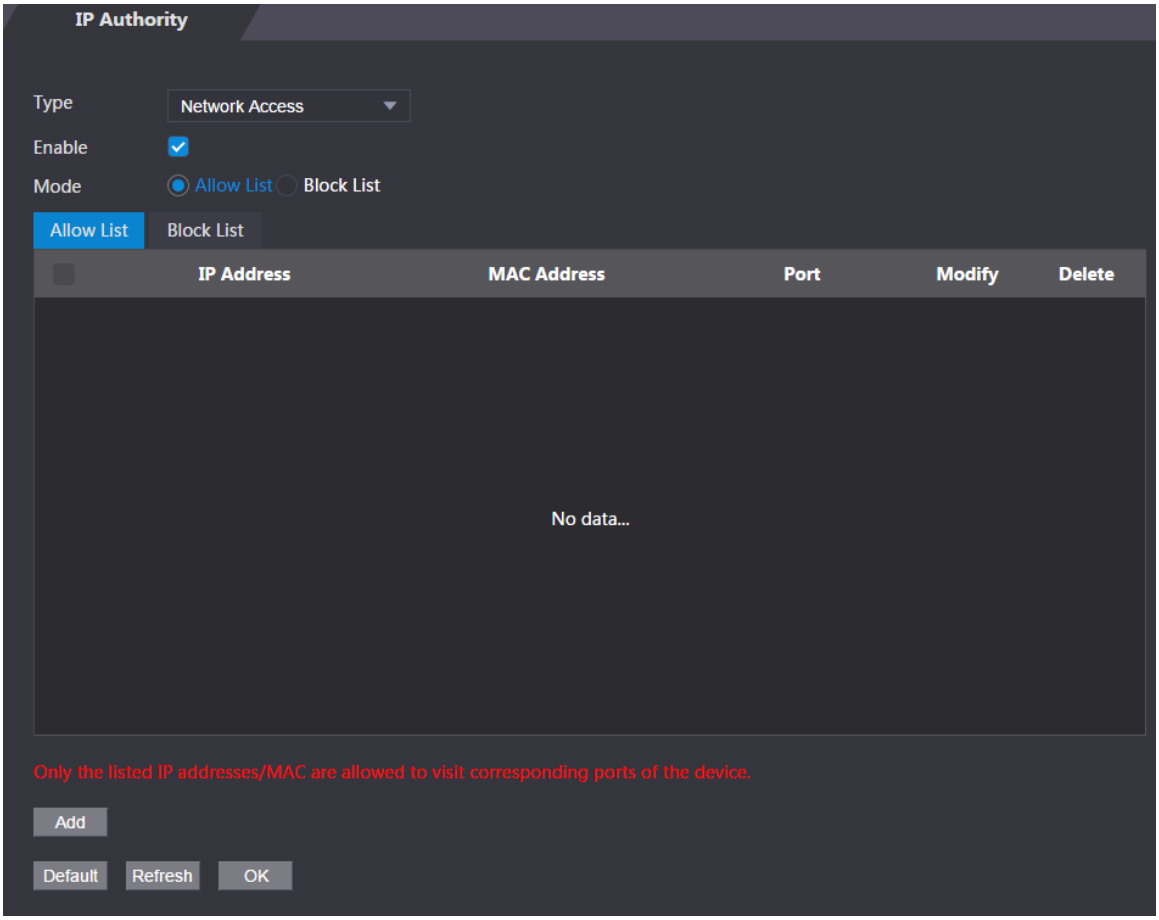
3.13.1.1 Network Access

Procedure

Step 1 Select **Network Access** from the **Type** list.

Step 2 Select the **Enable** check box.

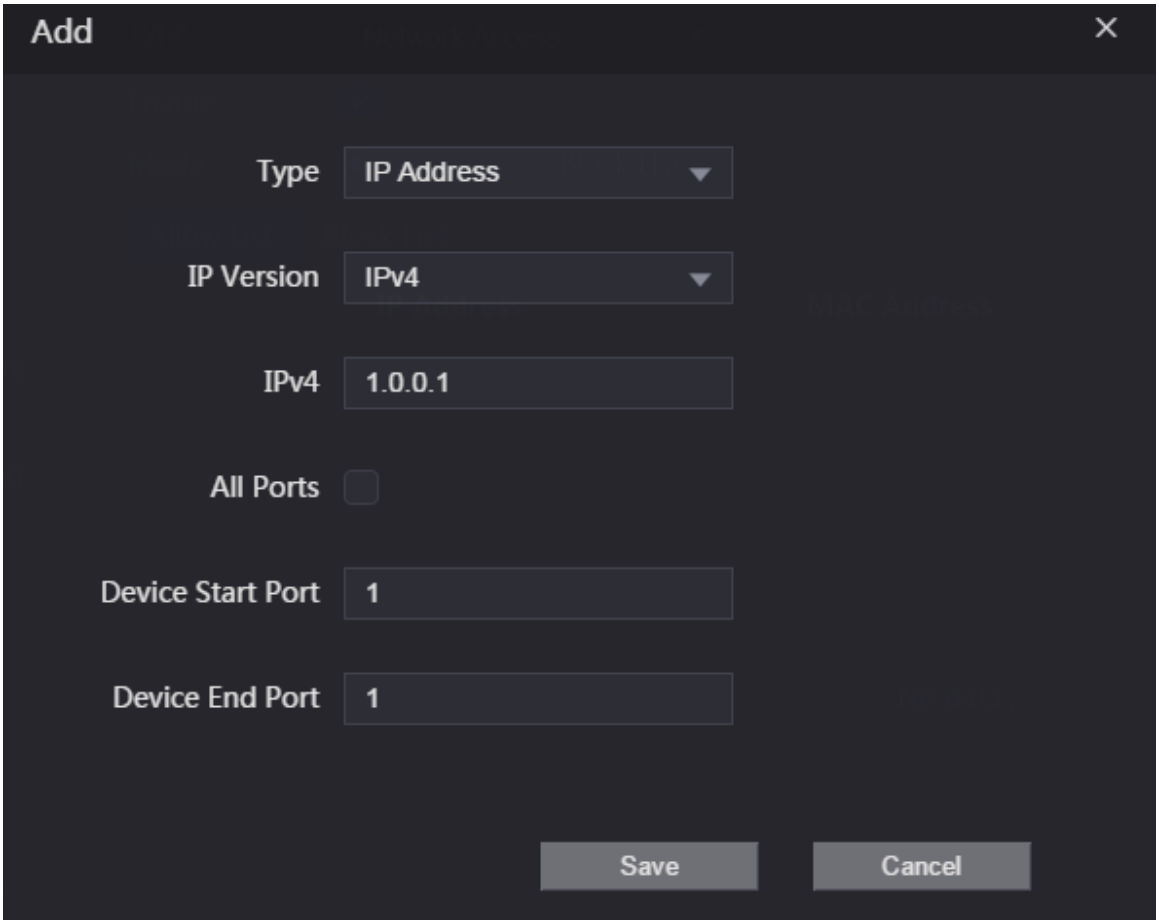
Figure 3-40 Network access



Step 3 Select **Allow List** or **Block List**.

Step 4 Click **Add**.

Figure 3-41 Add IP



Step 5 Configure parameters.

Table 3-22 Description of adding IP parameters

Parameter	Description
Type	Select the address type from the **Type** list.
IP Version	IPv4 by default.
All Ports	Select **All Ports** check box, and your settings will apply to all ports.
Device Start Port	If you clear **All Ports** check box, set the device start port and device end port.
Device End Port	

Step 6 Click **Save** , and the **IP Authority** interface is displayed.

Step 7 Click **OK**.

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

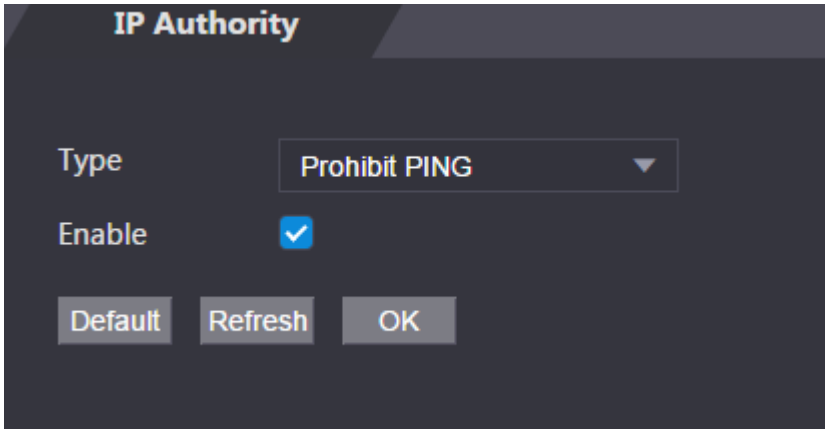
3.13.1.2 Prohibit PING

Procedure

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

Step 2 Select the **Enable** check box.

Figure 3-42 Prohibit PING



Step 3 Click **OK**.

3.13.1.3 Anti Half Connection

Procedure

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

Step 2 Select the **Enable** check box.

Step 3 Click **OK**.

3.13.2 Configuring System

Procedure

Step 1 Log in to the web interface.

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

Step 3 Enable or disable the system services as needed.

Figure 3-43 System service

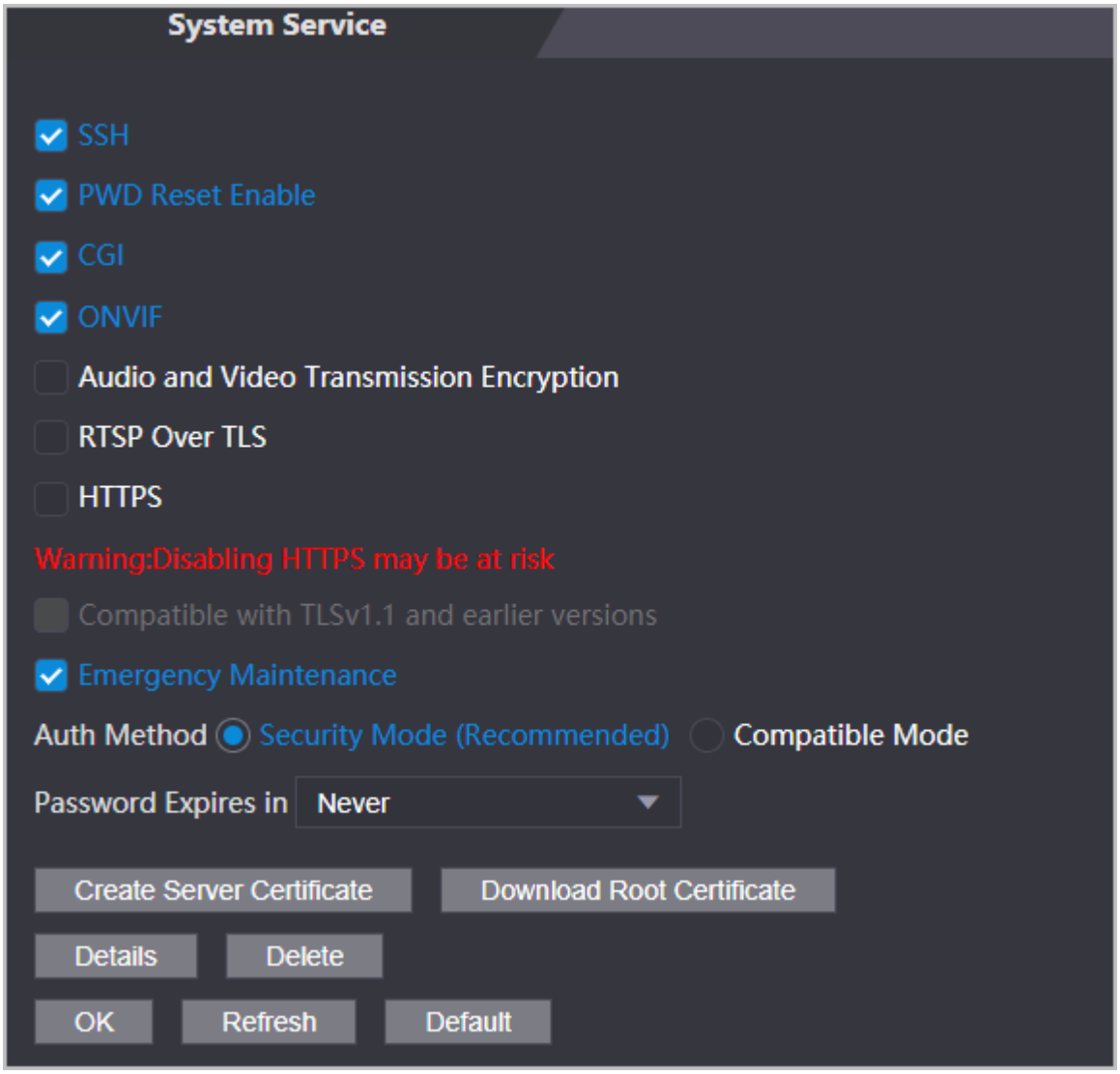


Table 3-23 Description of system service

Parameter	Description
SSH	Secure Shell (SSH) is a cryptographic network protocol for operating network services securely over an unsecured network. When SSH is enabled, SSH provides cryptographic service for the data transmission.
PWD Reset Enable	If enabled, you can reset the password. This function is enabled by default.
CGI	Common Gateway Interface (CGI) offers a standard protocol for web servers to execute programs similarly to console applications running on a server that dynamically generates webpages. When CGI is enabled, CGI commands can be used. The CGI is enabled by default.

Parameter	Description
ONVIF	Enable other devices to pull the video stream of the VTO via the ONVIF protocol.
Audio and Video Transmission Encryption	If this function is enabled, audio and video transmission is automatically encrypted.
RTSP Over TLS	If this function is enabled, audio and video transmission is encrypted via THE RTSP protocol.
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.
Compatible with TLSv1.1 and earlier versions	Enable this function if your browser is using TLS V1.1 or earlier versions.
Emergency Maintenance	Enable it for faults analysis and maintenance.
Password Expires in	Set the password expiration date.

Step 4 Click **OK**.

3.13.2.1 Creating Server Certificate

Background Information

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

- If you use HTTPS for the first time or the IP address of the Access Controller is changed, create a server certificate and install a root certificate.
- If you use another computer to log in to the webpage of the Access Controller, you need to download and install the root certificate again on the new computer or copy the root certificate to the it.

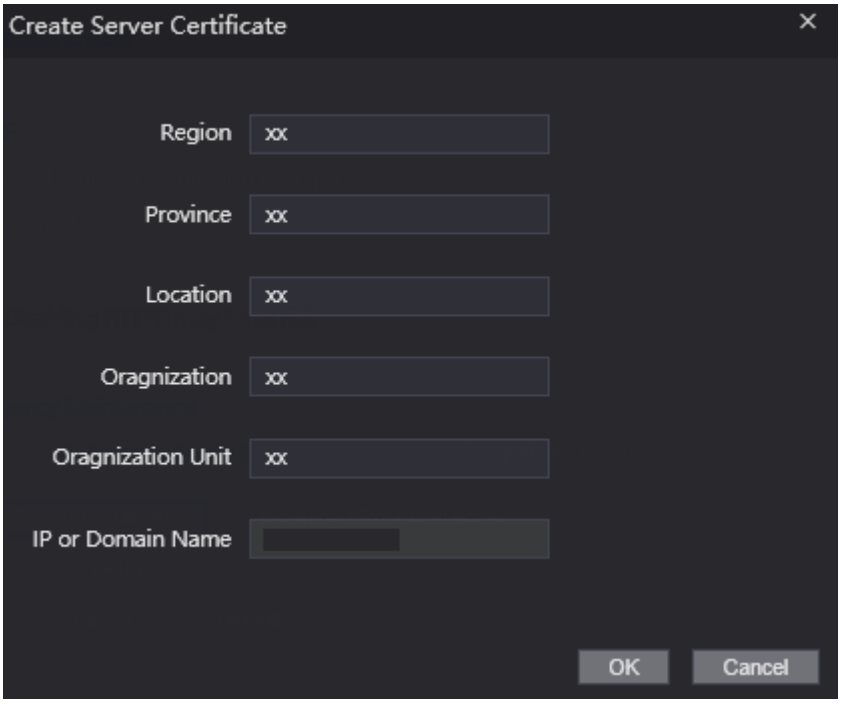
Procedure

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

Step 2 Enter information and click **OK**.

The Access Controller will restart.

Figure 3-44 Create Server Certificate



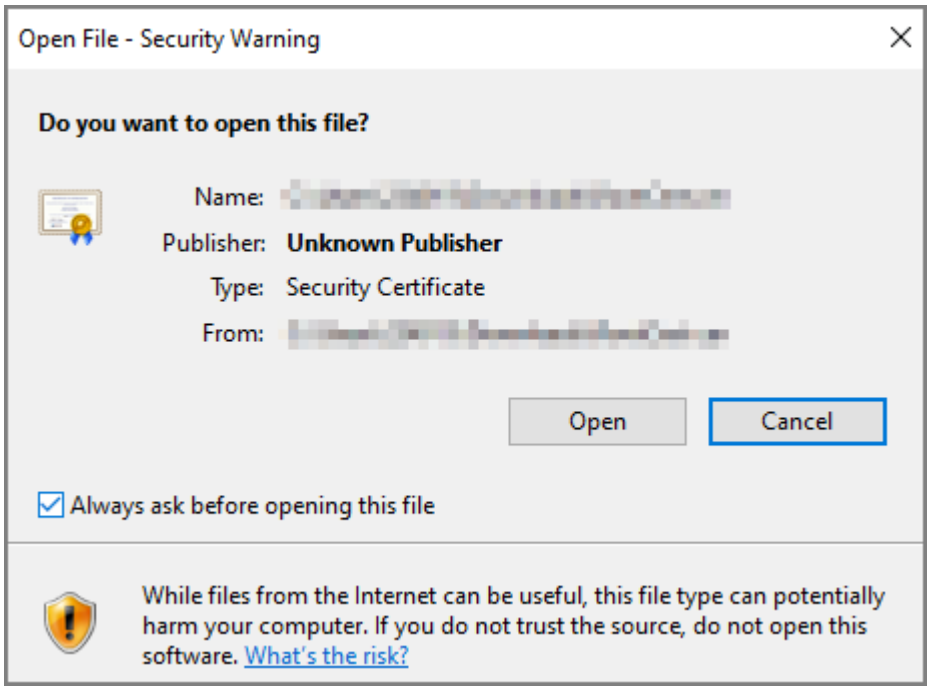
3.13.2.2 Downloading Root Certificate

Procedure

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

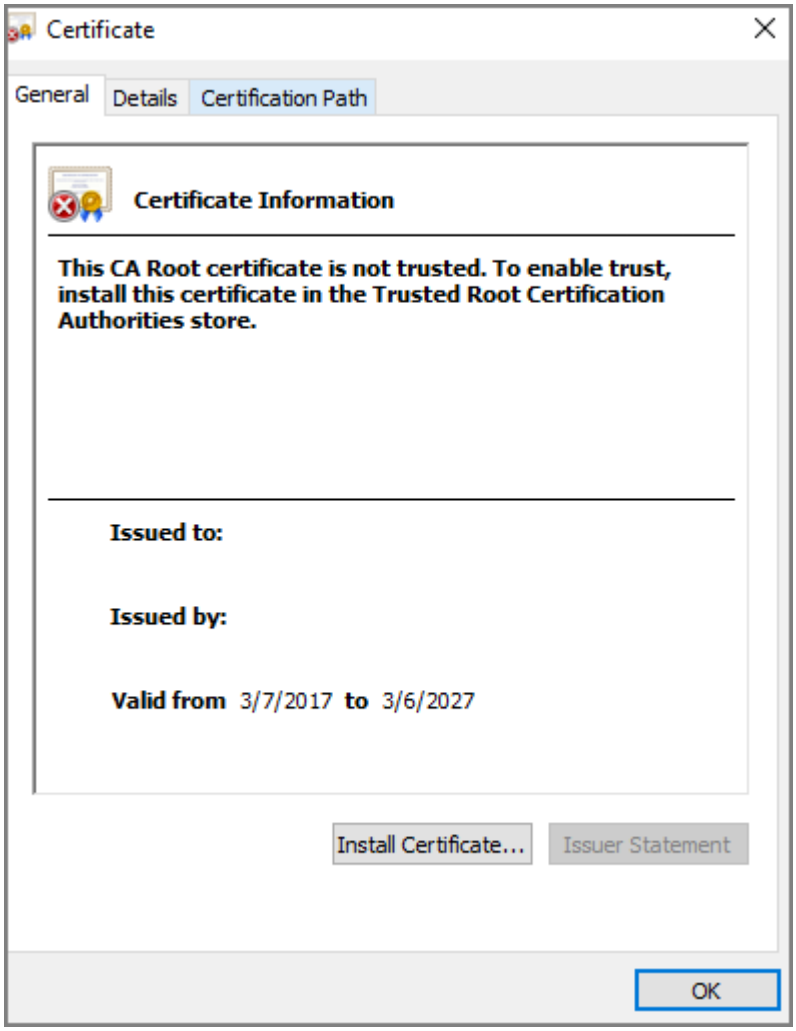
Step 2 Double-click the file that you have downloaded, and then click **Open**.

Figure 3-45 File download



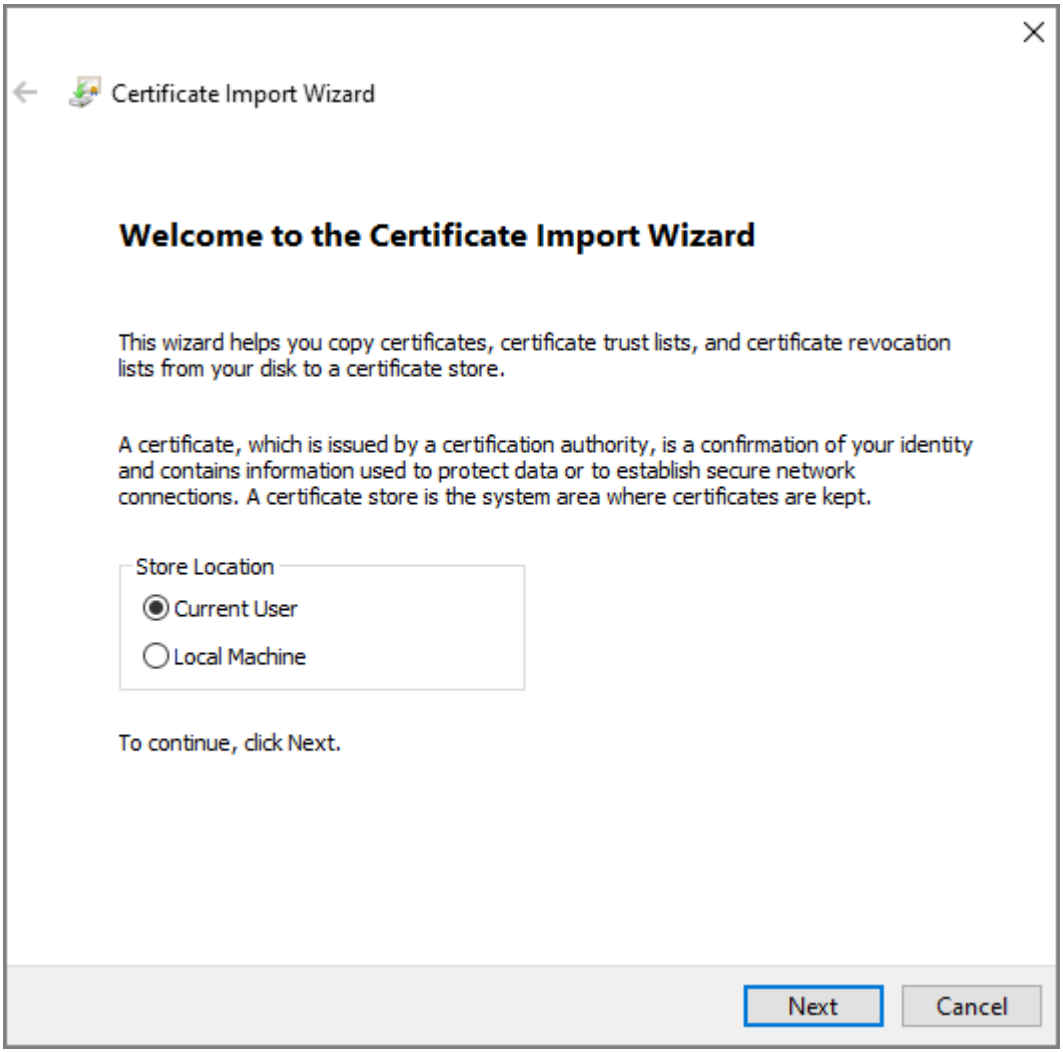
Step 3 Click **Install Certificate**.

Figure 3-46 Certificate information



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

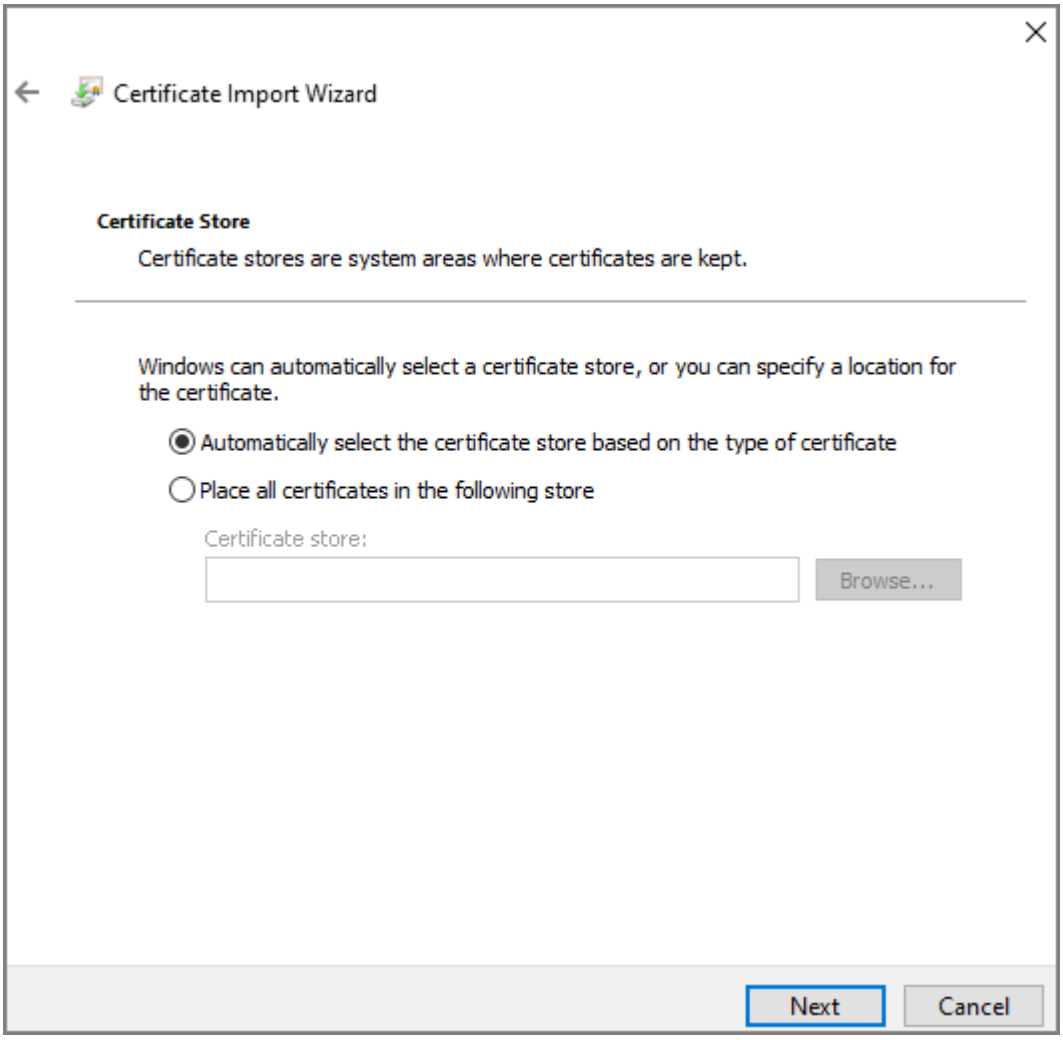
Figure 3-47 Certificate import wizard (1)



Step 5 Select the appropriate storage location.

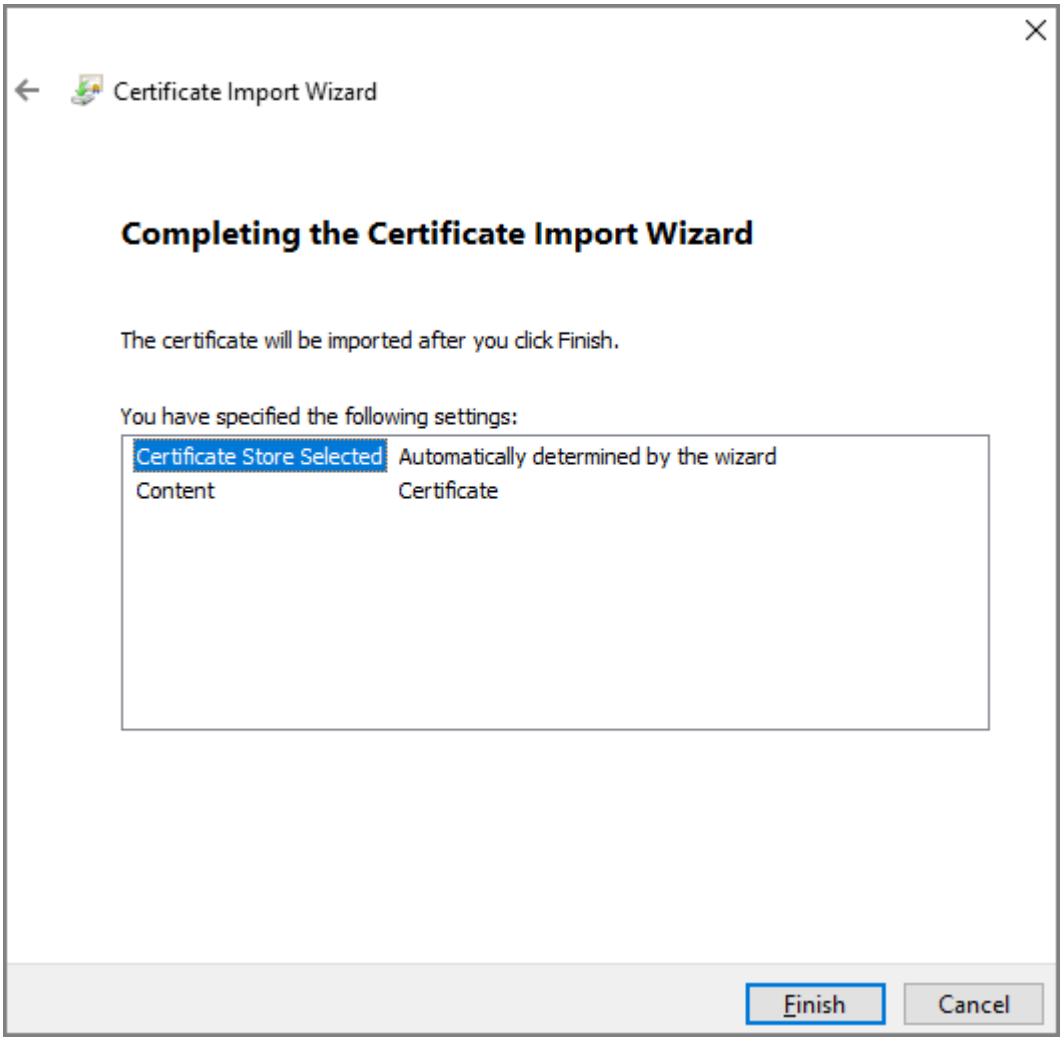
1. Select **Place all certificates in the following store**.
2. Click **Browse** to import the certificate to the **Trusted Root Certification Authorities** store, and then click **Next**.

Figure 3-48 Certificate Import Wizard (2)



Step 6 Click **Finish**.

Figure 3-49 Certificate import wizard (3)



3.14 User Management

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

3.14.1 Adding Users

You can add new users and then they can log in to the webpage of the Access Controller.

Procedure

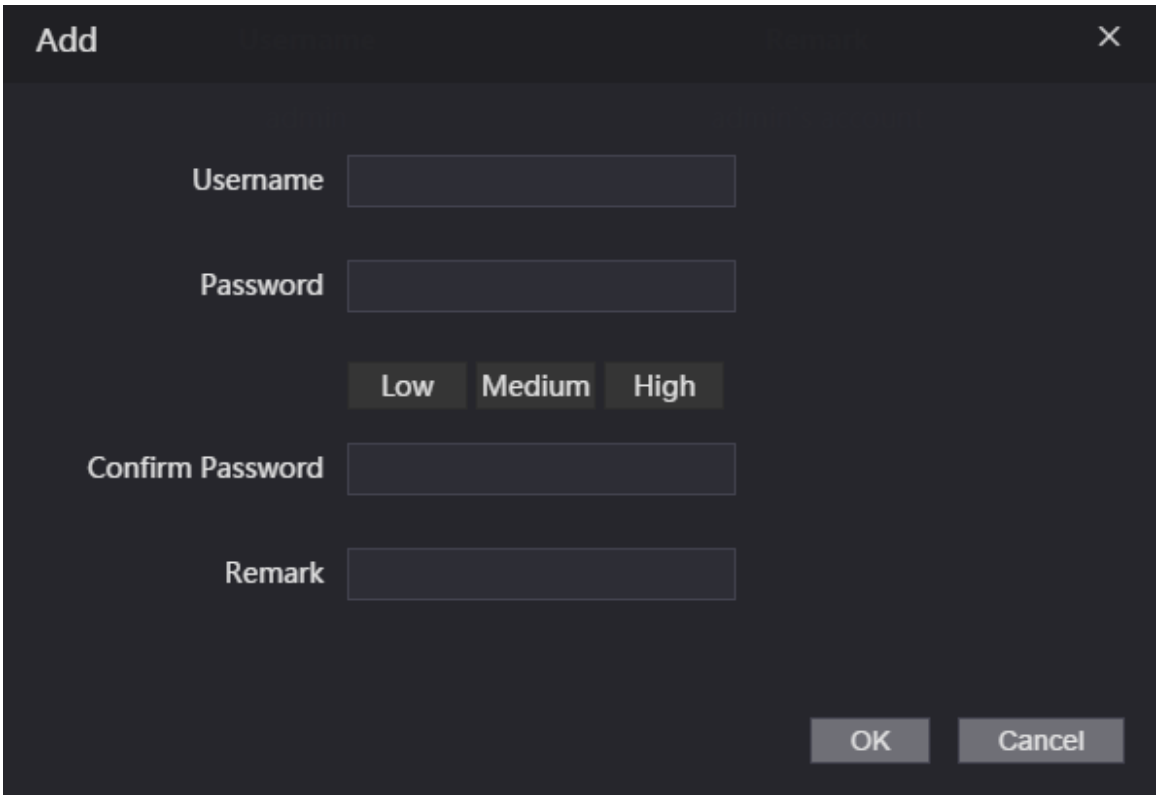
Step 1 On the home page, select **User Mgmt.** > **User Mgmt.**.

Step 2 Click **Add**, and enter the user information.

- The username cannot be the same with existing account. The username consists of up to 31 characters and only allows for numbers, letters, underscores, midlines, dots, or @.
- The password must consist of 8 to 32 non-blank characters and contain at least two types of the following characters: Upper case, lower case, numbers, and special characters (excluding ' " ; : &).

Set a high-security password by following the password strength prompt.

Figure 3-50 Add user



Step 3 Click **OK**.

Only admin account can change password and admin account cannot be deleted.

3.14.2 Adding ONVIF Users

Background Information

Open Network Video Interface Forum (ONVIF), a global and open industry forum that is established for the development of a global open standard for the interface of physical IP-based security products, which allows the compatibility from different manufactures. ONVIF users have their identities verified through ONVIF protocol. The default ONVIF user is admin.

Procedure

Step 1 On the home page, select **User Mgmt.** > **Onvif User**.

Step 2 Click **Add** and then configure parameters.

Figure 3-51 Add ONVIF user

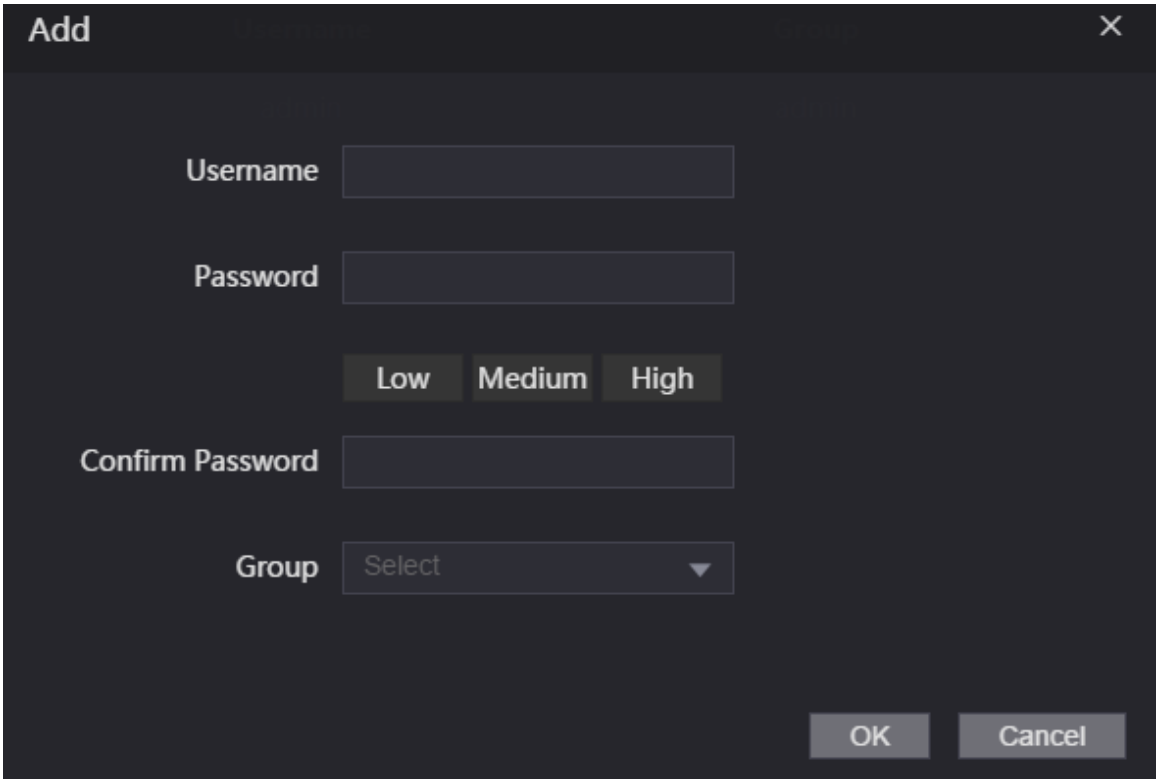


Table 3-24 ONVIF user description

Parameter	Description
Username	The username cannot be the same with existing account. The username consists of up to 31 characters and only allows for numbers, letters, underscores, midlines, dots, or @.
Password	The password must consist of 8 to 32 non-blank characters and contain at least two types of the following characters: Upper case, lower case, numbers, and special characters (excluding ' " ; : &).
Group	There three permission groups which represents different permission levels. • admin: You can view and manage other user accounts on the ONVIF Device Manager. • Operator: You cannot view or manage other user accounts on the ONVIF Device Manager. • User: You cannot view or manage other user accounts and system logs on the ONVIF Device Manager.

Step 3 Click **OK**.

3.14.3 Viewing Online Users

You can view online users who currently log in to the webpage.

Background Information

On the home page, select **Online User** .

3.15 Maintenance

Background Information

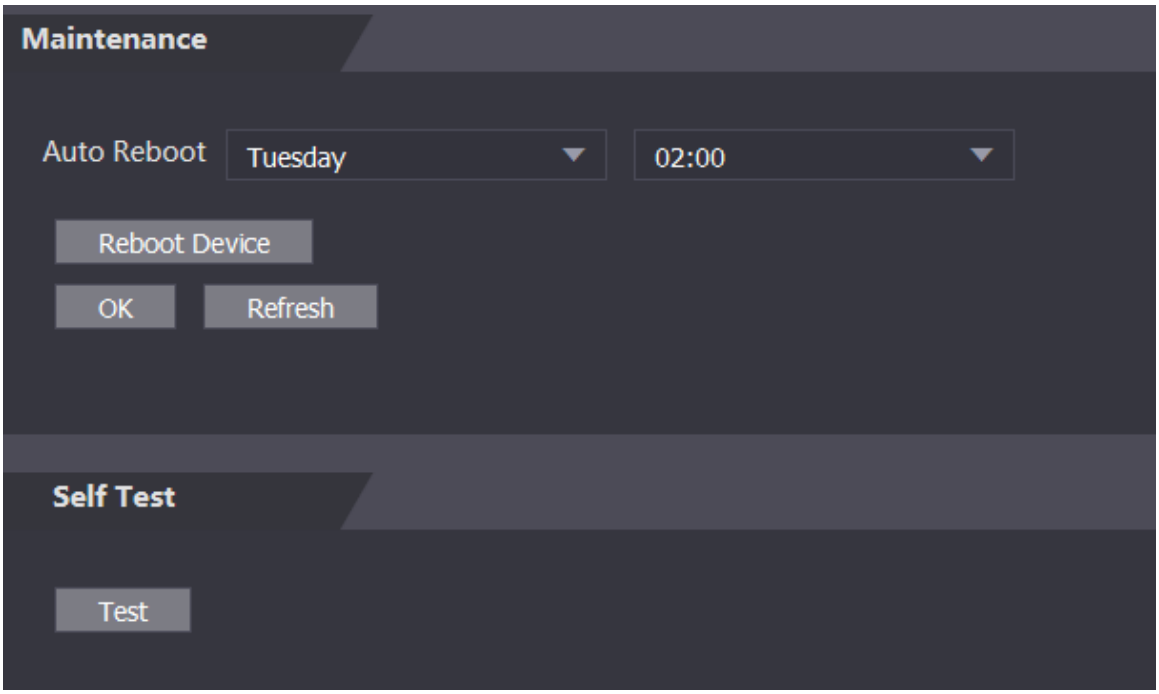
You can regularly restart the Access Controller during the idle time to improve its performance.

Procedure

Step 1 Log in to the webpage.

Step 2 Select **Maintenance**.

Figure 3-52 Maintenance



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

Step 4 (Optional) Click **Reboot Device**, the Access Controller will restart immediately.

3.16 Configuration Management

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

3.16.1 Exporting/Importing Configuration Files

Background Information

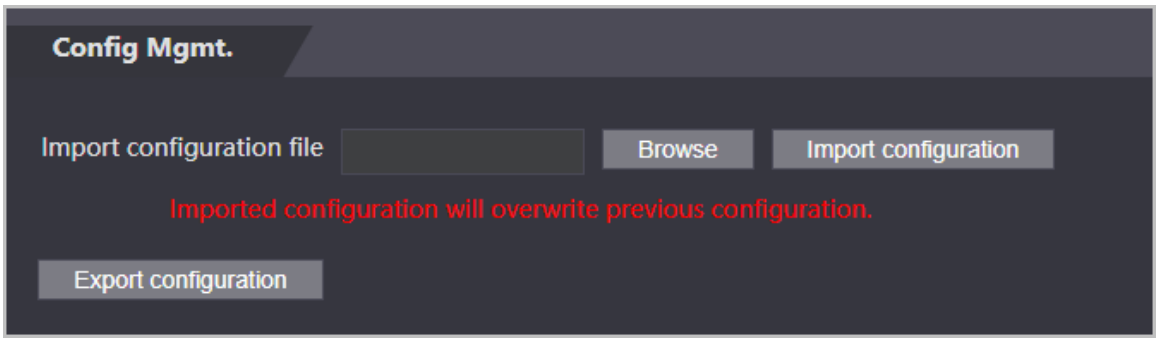
You can import or export the configuration file of the Access Controller. When you want to apply the same configurations to multiple devices, you can import the configuration file to them.

Procedure

Step 1 Log in to the webpage.

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

Figure 3-53 Configuration management



Step 3 Export or import configuration files.

- Export configuration file.

  Click **Export Configuration** to download the file to the local.

  IP will not be exported.

- Import configuration file.

  1. Click **Browse** to select the configuration file.
  2. Click **Import configuration**.

     Configuration file can only be imported to the device with the same model.

3.16.2 Restoring Factory Defaults

Background Information

Restoring the **Access Controller** to default configurations will cause data loss. Please be advised.

Procedure

Step 1 Select **Config Mgmt.** > **Default**

Step 2 Restore factory defaults if necessary.

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

3.16.3 Card Settings

This configuration is only available on Access Controller that supports IC cards.

Procedure

Step 1 On the home page, select **Config Mgmt.** > **Card Settings**.

Step 2 Configure the parameters.

Figure 3-54 Card settings

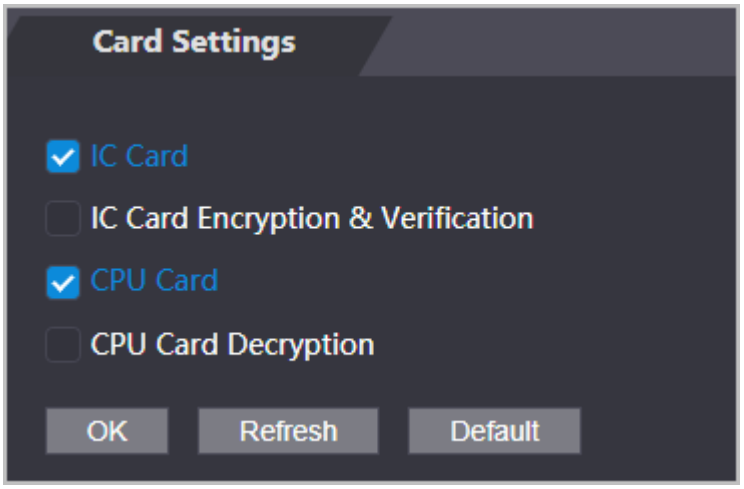


Table 3-25 Card settings description

Parameter	Description
IC card	The IC card number can be read when this function is turned on.
IC card Encryption & Verification	The number of the encrypted IC card can be read when this function is turned on. You need to turn on **IC card** first.
CPU Card	The physical card number of the CPU card can be read after this function is turned on.
CPU Card Decryption	The logical card number of the CPU card can be read when this function is turned on. You need to turn on **CPU card** first. The PSAM card needs to be inserted to the Access Controller to read CPU card, and the PSAM card does not support hot swapping.

3.16.4 Configuring External Module Type

Select the type of the external extension module that is mounted to the Access Controller.

Procedure

Step 1 On the home page, select **External Module Type**.

Step 2 Select an external module.

- FP
- QR Code
- FP+QR Code:

Step 3 Click **OK**.

The Access Controller restarts. is displayed on the standby screen, which indicates connection success. If is displayed, it indicates that selected module type and the actual module mounted to the Access Controller do not match.

3.17 Upgrading System

Background Information

- Use the correct update file. Make sure you get the correct update file from the technical support.
- Do not disconnect the power supply or network, or restart or shut down the Access Controller during the update.

3.17.1 File Update

Procedure

Step 1 On the home page, select **Upgrade**.

Step 2 In the **File Upgrade** area, click **Browse**, and then upload the update file.

The upgrade file should be a .bin file.

Step 3 Click **Update**.

The Access Controller will restart after update completes.

3.17.2 Online Update

Procedure

Step 1 On the home page, select **Upgrade**.

Step 2 In the **Online Upgrade** area, select an update method.

- Select **Auto Check**, the Access Controller will automatically check whether the its latest version is available.
- Select **Manual Check**, and you can immediately check whether the latest version is available.

Step 3 Update the Access Controller when the latest version is available.

3.18 Viewing Version Information

Background Information

On the home page, select **Version Info** , and you can view version information, such as device model, serial number, hardware version, legal information and more.

3.19 Viewing Logs

View logs such as system logs, admin logs, and unlock records.

3.19.1 System Logs

Background Information

View and search for system logs.

Procedure

Step 1 Log in to the webpage.

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

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

Click **Backup** to download the system log.

3.19.2 Admin Logs

Background Information

Search for admin logs by using admin ID.

Procedure

Step 1 Log in to the webpage.

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

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

3.19.3 Unlocking Logs

Background Information

Search for unlock records and export them.

Procedure

Step 1 Log in to the webpage.

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

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

You can click **Export Data** to download the log.

4 SmartPSS AC Configuration

This section introduces how to manage and configure the Access Controller through SmartPSS AC. For details, see the user's manual of SmartPSS AC.

4.1 Installing and Logging In

Install and log in to SmartPSS AC. For details, see the user manual of SmartPSS AC.

Procedure

Step 1 Get the software package of the SmartPSS AC from the technical support, and then install and run the software according to instructions.

Step 2 Initialize SmartPSS AC when you log in for the first time, including setting password and security questions.

Password is for login, and security questions are for password resetting.

Step 3 Enter your username and password to log in to SmartPSS AC.

4.2 Adding Devices

You need to add the Access Controller to SmartPSS AC. You can add them in batches or individually.

4.2.1 Adding Individually

Background Information

You can add Access Controller individually by entering their IP addresses or domain names.

Procedure

Step 1 Log in to SmartPSS AC.

Step 2 Click **Device Manager** and click **Add**.

Step 3 Enter the device information.

Figure 4-1 Device information

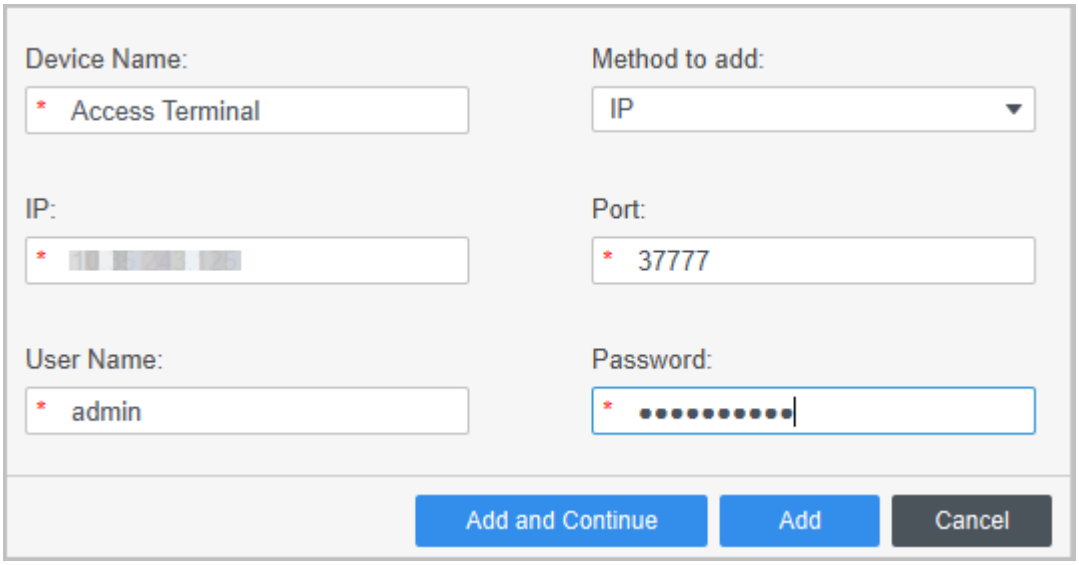


Table 4-1 Device parameters Description

Parameter	Description
Device Name	Enter a name of the Access Controller. We recommend you name it after its installation area.
Method to add	Select **IP** to add the Access Terminal by entering its IP Address.
IP	Enter IP address of the Access Controller.
Port	The port number is 37777 by default.
User Name/Password	Enter the username and password of the Access Terminal.

Step 4 Click **Add**.

The added Access Controller displays on the **Devices** page. You can click **Add and Continue** to add more Access Controllers.

4.2.2 Adding in Batches

Background Information

We recommend you use the auto-search function when you add want to Access Controllers in batches. Make sure the Access Controllers you add must be on the same network segment.

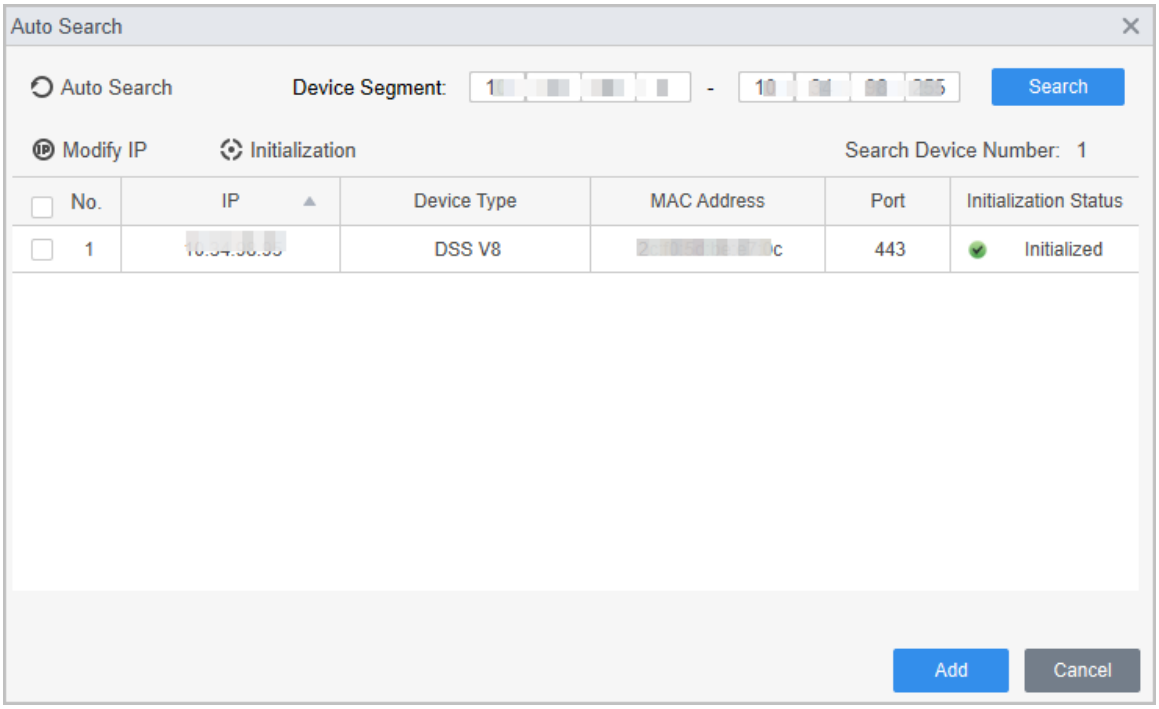
Procedure

Step 1 Log in to SmartPSS AC.

Step 2 Click **Device Manager** and search for devices.

- Click **Auto Search**, to search for devices on the same LAN.
- Enter the network segment range, and then click **Search**.

Figure 4-2 Auto search



A device list will be displayed.

Select a device, and then click **Modify IP** to modify its IP address.

Step 3 Select the Access Controller that you want to add to SmartPSS AC, and then click **Add**.

Step 4 Enter the username and the password of the Access Controller.

You can view the added Access Controller on the **Devices** page.

The Access Controller automatically logs in to SmartPSS AC after being added. **Online** is displayed after successful login.

4.3 User Management

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

4.3.1 Configuring Card Type

Background Information

Set the card type before you assign cards to users. For example, if the assigned card is an ID card, set card type to ID card.

Procedure

Step 1 Log in to SmartPSS AC.

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

Step 3 Click **Card**

Step 4 On the **Card Issuing Type** and then select a card type.

Make sure that the card type is same to the actually assigned card; otherwise, the card number cannot be read.

Step 5 Click **OK**.

4.3.2 Adding Users

4.3.2.1 Adding Individually

Background Information

You can add users individually.

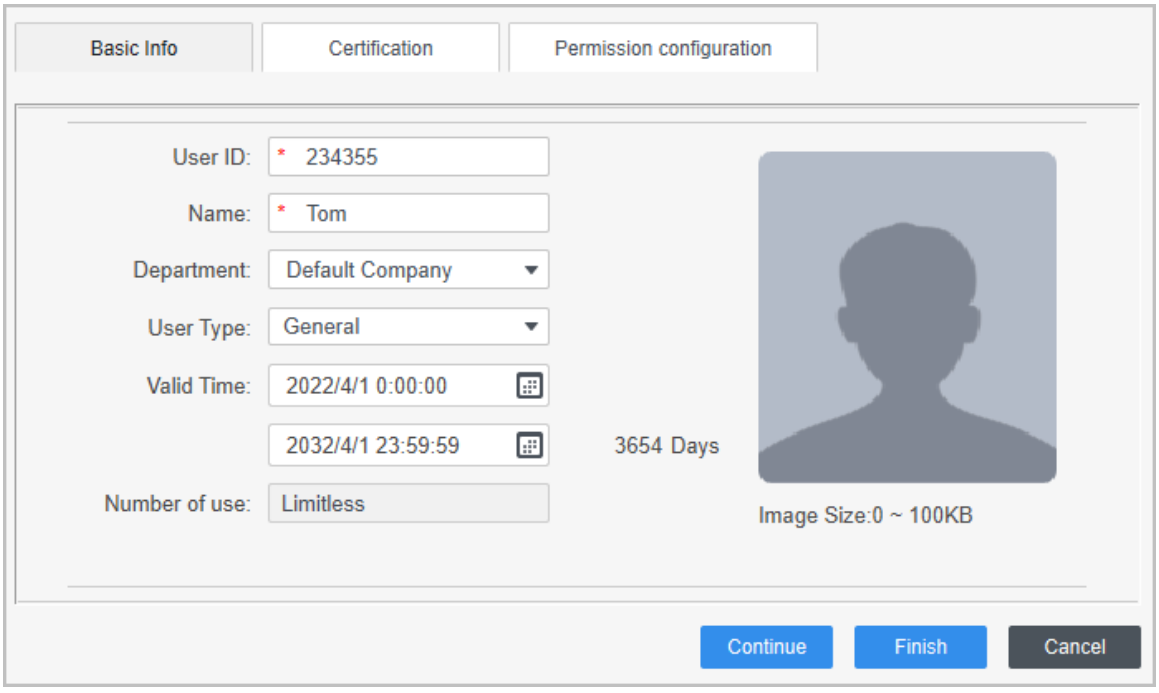
Procedure

Step 1 Log in to SmartPSS AC.

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

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

Figure 4-3 Add basic information



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

- Configure password: The password must consist of 6–8 digits.
- Configure card: The card number can be read automatically or entered manually. To read the card number automatically, select a card reader, and then place the card on the card reader.

  1. On the **Card** area, click and select **Card issuer**, and then click **OK**.
  2. Click **Add**, swipe a card on the card reader.

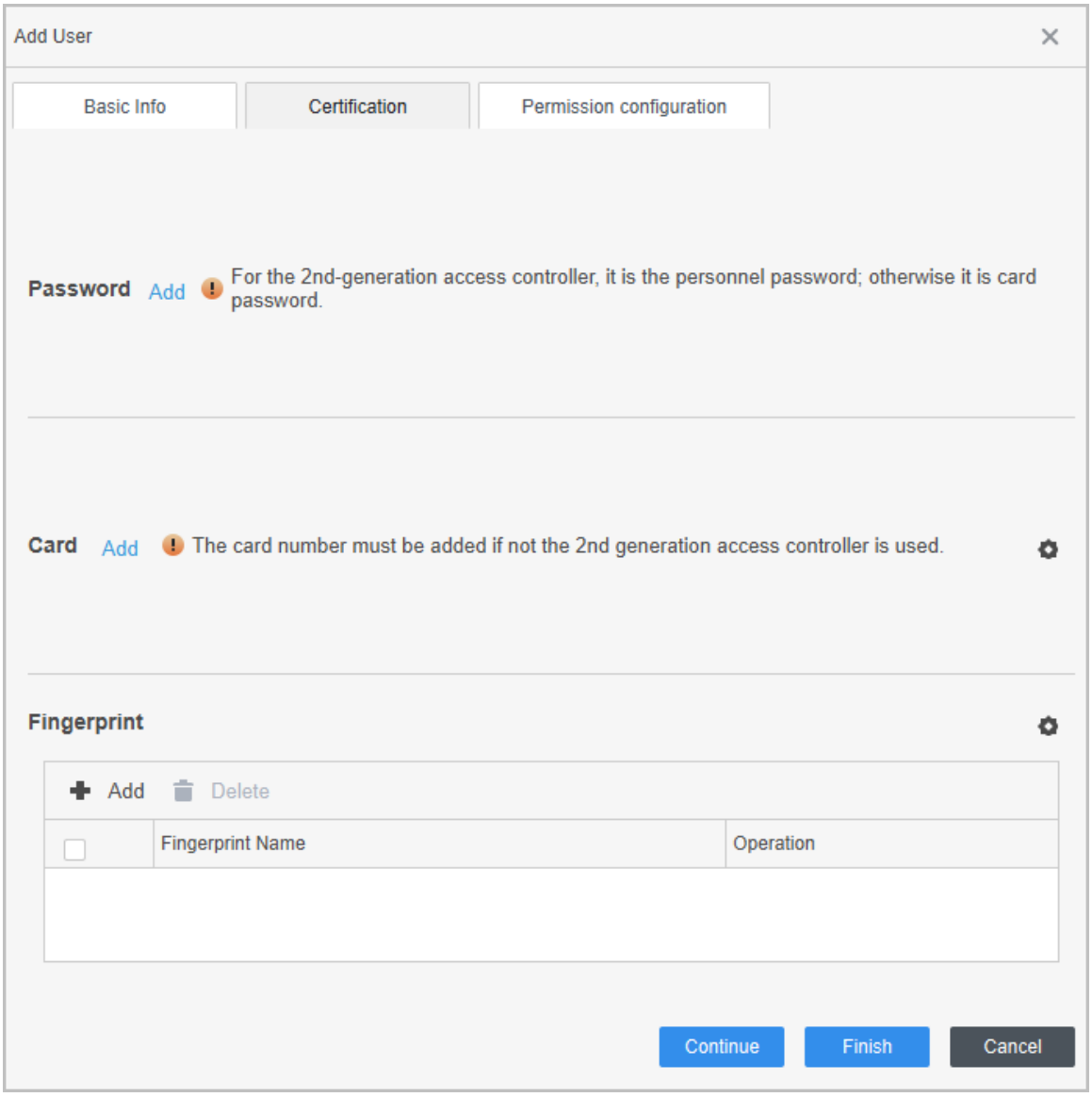
     The card number is displayed.
  3. Click **OK**.

4. (Optional) After adding a card, you can set the card to main card or duress card, or replace the card with a new one, or delete the card.

- Configure fingerprint.

1. On the **Fingerprint** area, click and select **Fingerprint Scanner**, and then click **OK**.
2. Click **Add Fingerprint**, press your finger on the scanner three times in a row.

Figure 4-4 Add password, card, and fingerprint



Step 5 Configure permissions for the user. For details, see "4.3.3 Assigning Access Permission".

Step 6 Click **Finish**.

4.3.2.2 Adding in Batches

Background Information

You can add users in batches.

Procedure

Step 1 Log in to SmartPSS AC.

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

Step 3 Select **Card issuer** from the **Device** list, and then configure the parameters.

Figure 4-5 Add users in batches

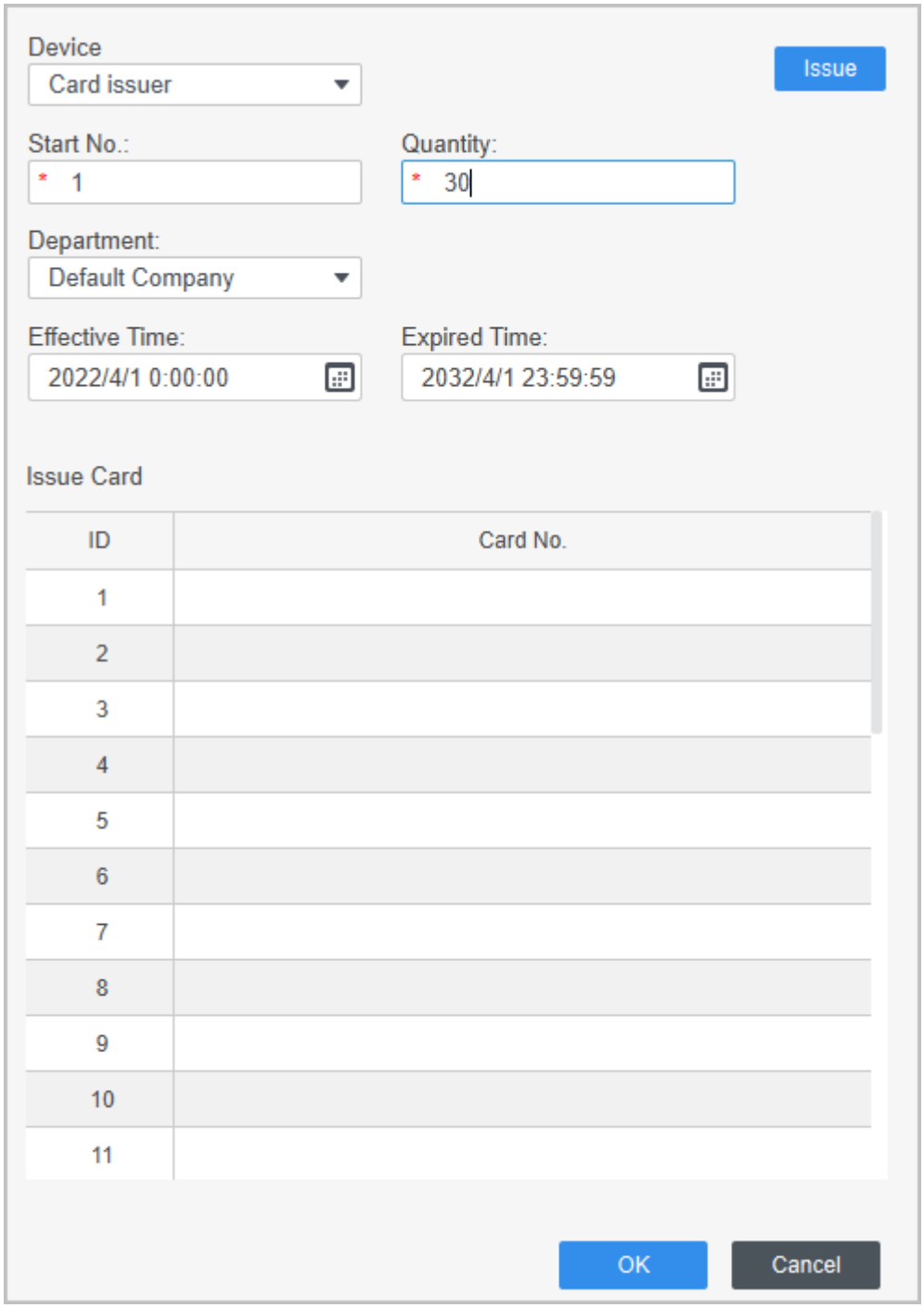


Table 4-2 Add users in batches parameters

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

Parameter	Description
Effective Time/Expired Time	The users can unlock the door within the defined period.

Step 4 Click **Issue**.

The card number will be read automatically.

Step 5 Click **OK**.

Step 6 On the **User** page, click to complete user information.

4.3.3 Assigning Access Permission

Create a permission group that is a collection of door access permissions, and then associate users with the group so that users can unlock corresponding doors.

Procedure

Step 1 Log in to the SmartPSS AC.

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

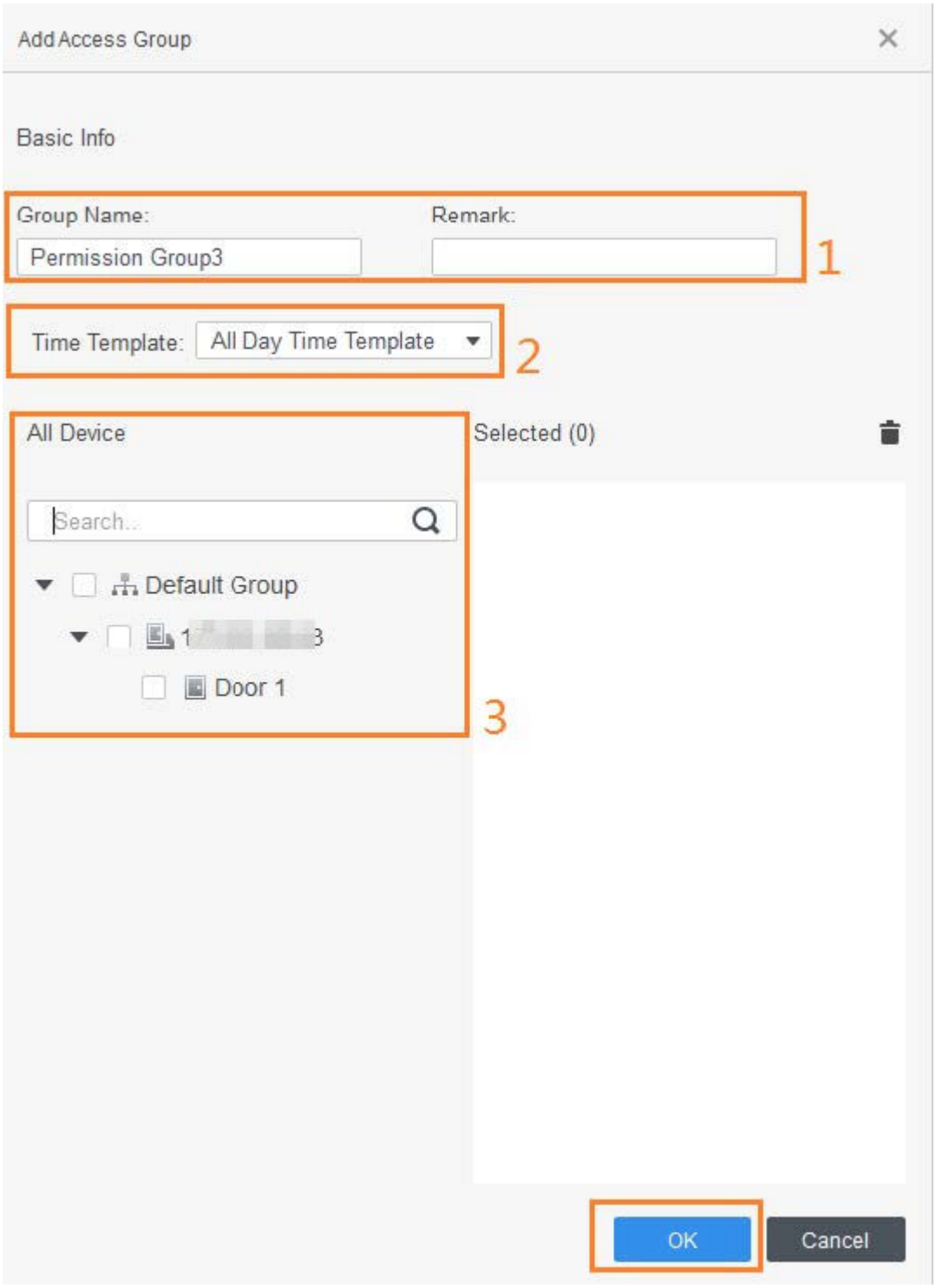
Step 3 Click .

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

Step 5 Select the access control device.

Step 6 Click **OK**.

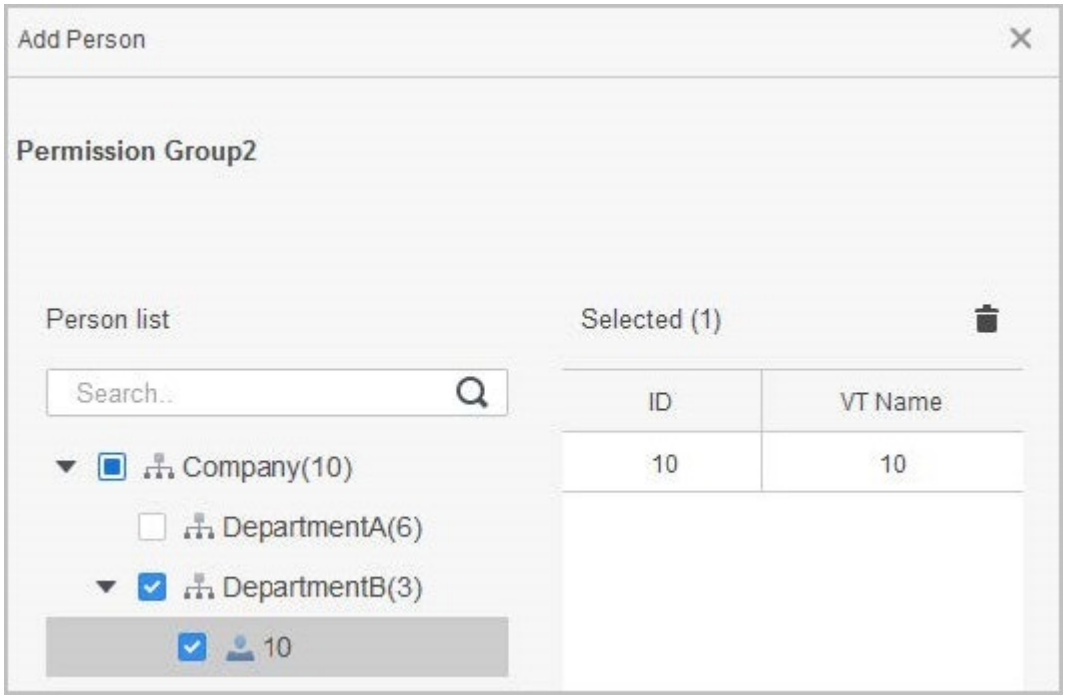
Figure 4-6 Create a permission group



Step 7 Click of the permission group you added.

Step 8 Select users to associate them with the permission group.

Figure 4-7 Add users to a permission group



Step 9 Click **OK**.

Users in the permission group can unlock the door after valid identity verification.

4.4 Access Management

4.4.1 Remotely Opening and Closing Door

You can remotely monitor and control door through SmartPSS AC. For example, you can remotely open or close the door.

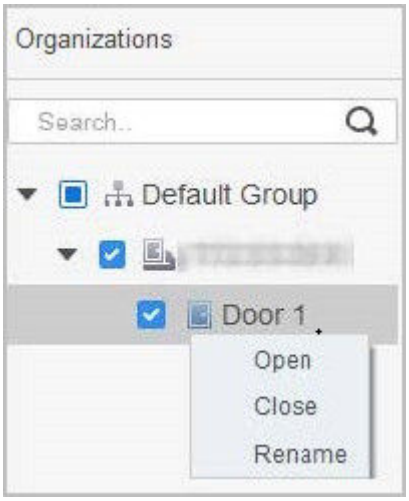
Procedure

Step 1 Click **Access Solution** > **Access Manager** on the homepage.

Step 2 Remotely control the door.

- Select the door, right click and select **Open** or **Close**.

Figure 4-8 Open door



- Click or to open or close the door.

Related Operations

- Event filtering: Select the event type in the **Event Info**, and the event list displays the selected event type, such as alarm events and abnormal events.
- Event refresh locking: Click to lock the event list, and then event list will stop refreshing. Click to unlock.
- Event deleting: Click to clear all events in the event list.

4.4.2 Setting Always Open and Always Close

After setting always open or always close, the door remains open or closed all the time.

Procedure

Step 1 Click **Access Solution** > **Access Manager** on the homepage.

Step 2 Click **Always Open** or **Always Close** to open or close the door.

Figure 4-9 Always open or close

The door will remain open or closed all the time. You can click **Normal** to restore the access control to normal status, and then the door will be open or closed based on the configured verification methods.

4.4.3 Monitoring Door Status

Procedure

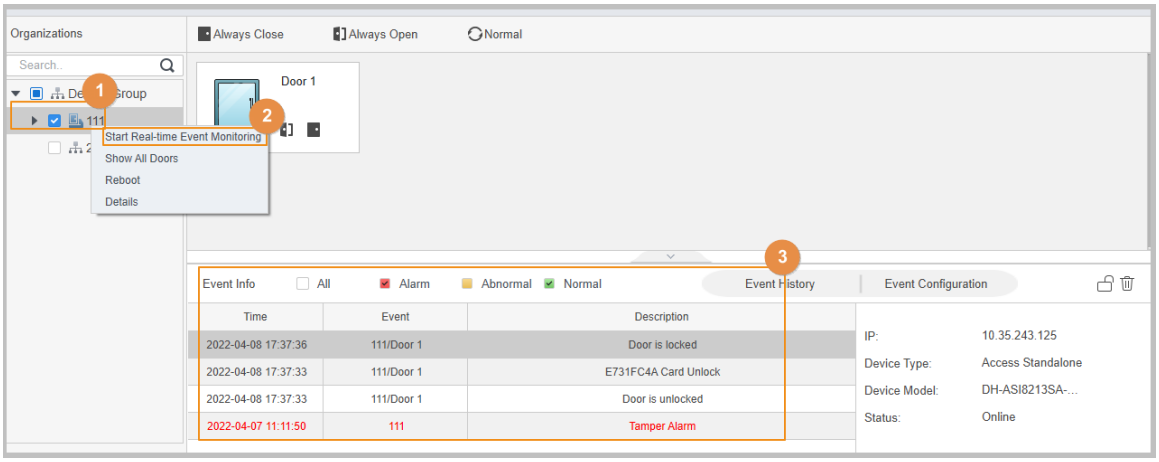
Step 1 Click **Access Solution** > **Access Manager** on the homepage.

Step 2 Select the Access Controller in the device tree, and right click the Access Terminal and then select **Start Real-time Event Monitoring**.

Real-time access control events will display in the event list.

Click **Stop Monitor**, real-time access control events will not display.

Figure 4-10 Monitor door status



Related Operations

- Show All Door: Displays all doors controlled by the Access Controller.
- Reboot: Restart the Access Controller.
- Details: View the device details, such as IP address, model, and status.

Appendix 1 Important Points of Intercom Operation

The Access Controller can function as VTO to realize intercom function.

Prerequisites

The intercom function is configured on the Access Controller and VTO.

Procedure

Step 1 On the standby screen, tap 

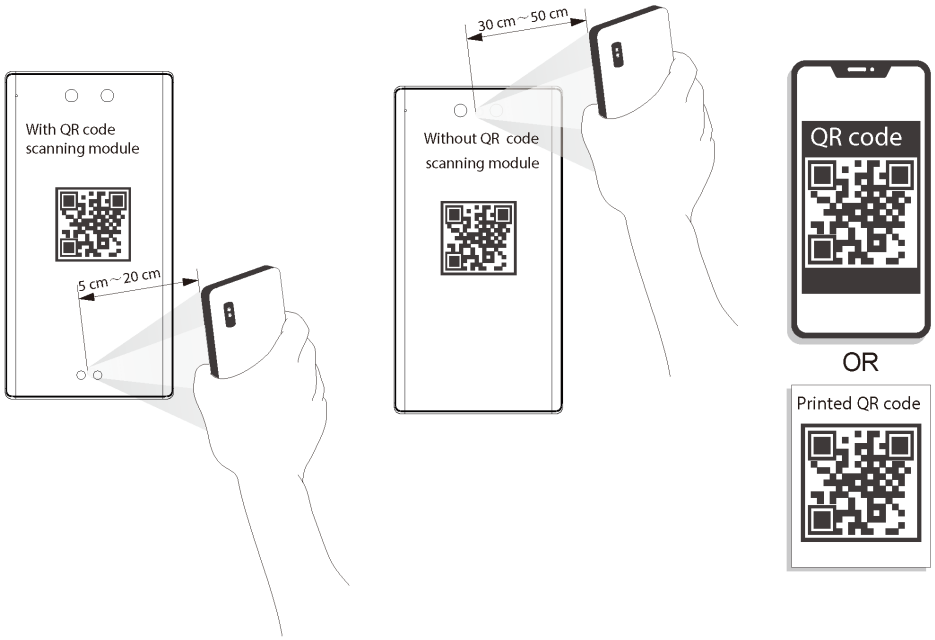
Step 2 Enter the room No, and then tap  .

Appendix 2 Important Points of QR Code Scanning

- Access Controller (with QR code scanning module): Place the QR code on your phone at a distance of 3 cm - 5 cm away from the QR code scanning lens. It supports QR code that is larger than 30 mm ×30 mm - 5 cm × 5 cm and less than 100 bytes in size.

QR code detection distance differs depending on the bytes and size of QR code.

Appendix Figure 2-1 QR code scanning



Appendix 3 Important Points of Fingerprint Registration Instructions

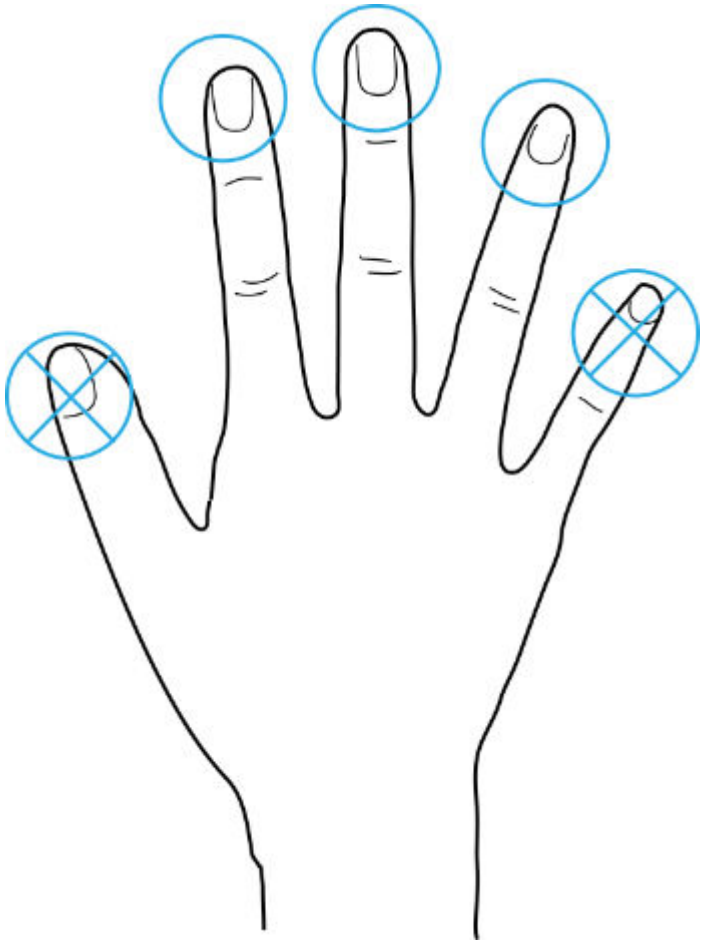
When you register the fingerprint, pay attention to the following points:

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

Fingers Recommended

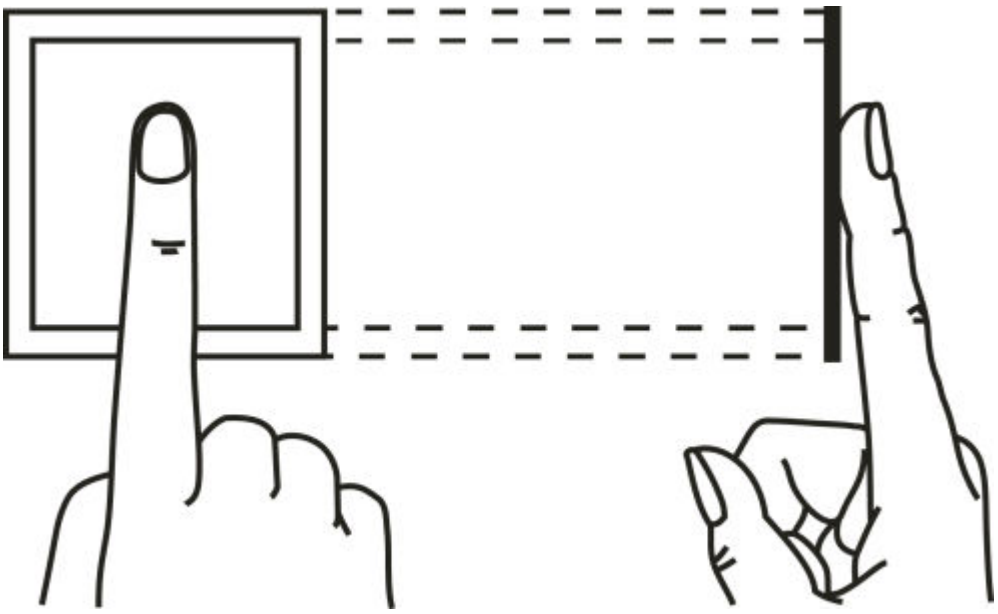
Forefingers, middle fingers, and ring fingers are recommended. Thumbs and little fingers cannot be put at the recording center easily.

Appendix Figure 3-1 Recommended fingers

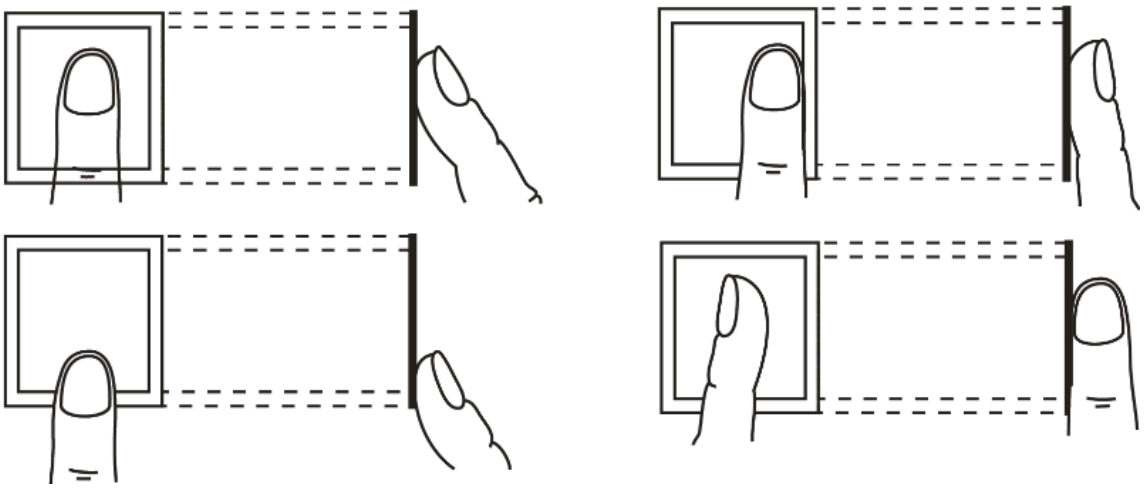


How to Press Your Fingerprint on the Scanner

Appendix Figure 3-2 Correct placement



Appendix Figure 3-3 Wrong placement



Appendix 4 Important Points of Face Registration

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 use the Device; otherwise face recognition might fail.
- Keep your face clean.
- Keep the Device at least 2 meters away from light source and at least 3 meters away from windows or doors; otherwise backlight and direct sunlight might influence face recognition performance of the access controller.

During Registration

- You can register faces through the Device or through the platform. For registration through the platform, see the platform user manual.
- Make your head center on the photo capture frame. The face image will be captured automatically.

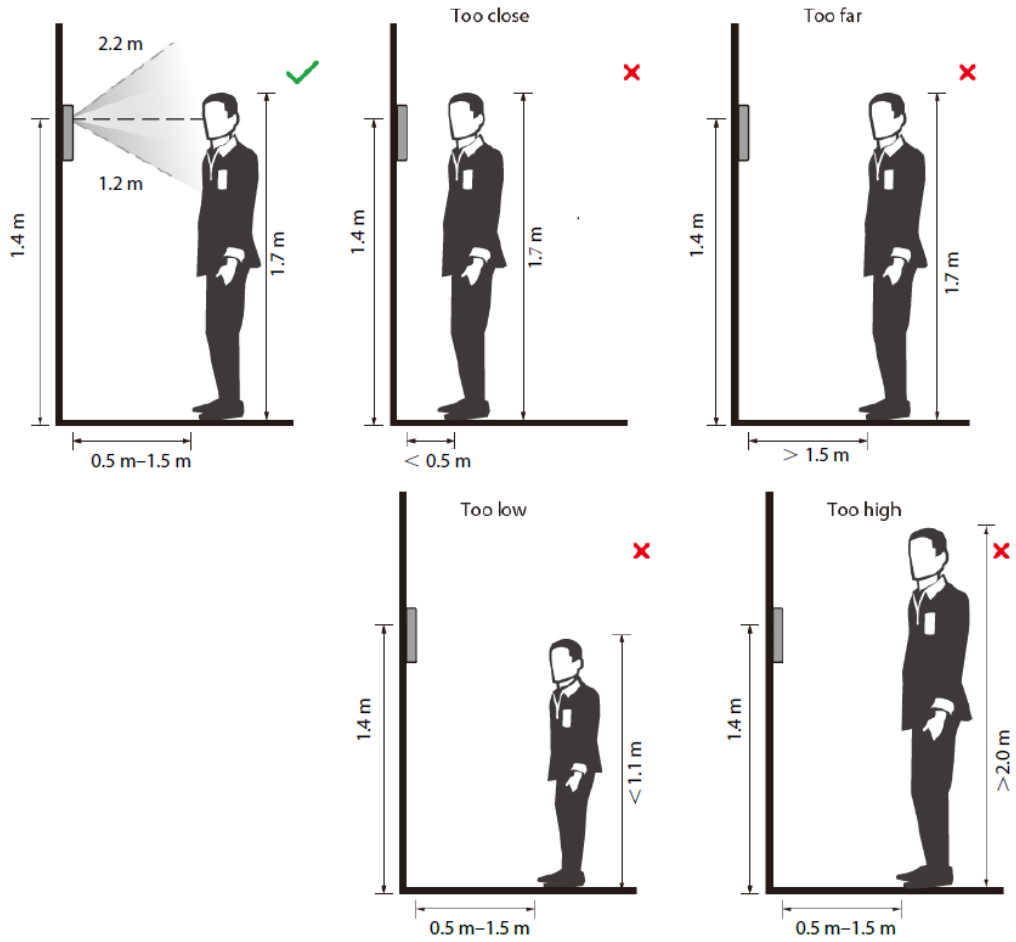
- Do not shake your head or body, otherwise the registration might fail.
- Avoid 2 faces appear in the capture frame at the same time.

Face Position

If your face is not at the appropriate position, face recognition accuracy might be affected.

The face position below is for reference only, and might differ from the actual situation.

Appendix Figure 4-1 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 4-2 Head position

Appendix Figure 4-3 Face distance

- When importing face images through the management platform, make sure that image resolution is within the range from 150 × 300 pixels to 600 × 1200 pixels. It is recommended that the resolution be greater than 500 × 500 pixels, the image size be less than 100 KB, and the image name and person ID be 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 5 Security Recommendation

Account Management

1. **Use complex 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: 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 repeating characters, such as 111, aaa, etc.
2. **Change passwords periodically**

   It is recommended to periodically change the device password to reduce the risk of being guessed or cracked.
3. **Allocate accounts and permissions appropriately**

   Appropriately add users based on service and management requirements and assign minimum permission sets to users.
4. **Enable account lockout function**

   The account lockout function is enabled by default. You are advised to keep it enabled to protect account security. After multiple failed password attempts, the corresponding account and source IP address will be locked.
5. **Set and update password reset information in a timely manner**

   The device supports password reset function. To reduce the risk of this function being used by threat actors, if there is any change in the information, please modify it in time. When setting security questions, it is recommended not to use easily guessed answers.

Service Configuration

1. **Enable HTTPS**

   It is recommended that you enable HTTPS to access web services through secure channels.
2. **Encrypted transmission of audio and video**

   If your audio and video data contents are very important or sensitive, it is recommended to use encrypted transmission function in order to reduce the risk of your audio and video data being eavesdropped during transmission.
3. **Turn off non-essential services and use safe mode**

   If not needed, it is recommended to turn off some services such as SSH, SNMP, SMTP, UPnP, AP hotspot etc., to reduce the attack surfaces.

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

   - SNMP: Choose SNMP v3, and set up strong encryption and authentication passwords.
   - SMTP: Choose TLS to access mailbox server.
   - FTP: Choose SFTP, and set up complex passwords.
   - AP hotspot: Choose WPA2-PSK encryption mode, and set up complex passwords.
4. **Change HTTP and other default service ports**

   It is recommended that you change the default port of HTTP and other services to any port between 1024 and 65535 to reduce the risk of being guessed by threat actors.

Network Configuration

1. **Enable Allow list**

   It is recommended that you turn on the allow list function, and only allow IP in the allow list to access the device. Therefore, please be sure to add your computer IP address and supporting device IP address to the allow list.
2. **MAC address binding**

   It is recommended that you bind the IP address of the gateway to the MAC address on the device to reduce the risk of ARP spoofing.
3. **Build a secure network environment**

   In order to better ensure the security of devices and reduce potential cyber risks, the following are recommended:

   - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network;
   - According to the actual network needs, partition the network: if there is no communication demand between the two subnets, it is recommended to use VLAN, gateway and other methods to partition the network to achieve network isolation;
   - Stablish 802.1x access authentication system to reduce the risk of illegal terminal access to the private network.

Security Auditing

1. **Check online users**

   It is recommended to check online users regularly to identify illegal users.
2. **Check device log**

   By viewing logs, you can learn about the IP addresses that attempt to log in to the device and key operations of the logged users.
3. **Configure network log**

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

Software Security

1. **Update firmware in time**

   According to the industry standard operating specifications, the firmware of devices needs to be updated to the latest version in time in order to ensure that the device has the latest functions and security. If the device is connected to the public network, it is recommended to enable the online upgrade automatic detection function, so as to obtain the firmware update information released by the manufacturer in a timely manner.
2. **Update client software in time**

   It is recommended to download and use the latest client software.

Physical Protection

It is recommended that you carry out physical protection for devices (especially storage devices), such as placing the device in a dedicated machine room and cabinet, and having access control

and key management in place to prevent unauthorized personnel from damaging hardware and other peripheral equipment (e.g. USB flash disk, serial port).