Swing Barrier Speed Gate

User Manual

V1.00

Contents

Disclaimer and Safety Warnings

Preface

The purpose of this section is to ensure that users correctly utilize the product to prevent dangers caused by improper operation or property damage. Before using this product, please read this manual carefully and keep it properly for future reference.

About This Manual

- This manual is for use with multiple product models; we apologize for not listing the appearance and functions of each product individually. Please refer to your actual product for use.
- This manual is compatible with multiple software versions. The product interface and functions should be based on the actual software.
- Despite our best efforts, the content of this manual may contain technical or printing errors. Final interpretation resides solely with us.
- Please follow the operating instructions in this manual. Any losses caused by not following the guidance in this manual are the responsibility of the user.
- We reserve the right to modify the content of this manual without notice. Due to product version upgrades or regulatory requirements in relevant regions, the content of this manual will be updated periodically, and the updated content will be reflected in the new version.
- This manual will be updated in real time according to the laws and regulations of relevant regions. Please refer to the product's paper copy, QR code, or official website for details. If there is any inconsistency between the paper copy and the electronic version, the digital version shall prevail.

About the Product

If the product you have chosen is a video product, please strictly adhere to the applicable laws and regulations. You can visit our official website to inquire about the relevant content.

User Guidelines

- This document serves as a guide for use only. All statements, information, and suggestions in this document do not constitute any express or implied warranty.
- We assume no responsibility for any special, incidental, consequential, or indirect damages resulting from the use of this manual or the use of our products, including but not limited to loss of business profits, loss of data or documents, and abnormal product operation or information leakage caused by cyber-attacks, hacker attacks, or virus infections.
- Due to uncertain factors such as the physical environment, there may be discrepancies between the actual values of some data and the reference values provided in the manual. If there are any questions or disputes, our final interpretation shall prevail.

Formatting Conventions

The UI formatting conventions used in this document are as follows:

Format	Meaning
>	Indicate a sequence of actions, e.g., click Device Management > Add Device, which means first click Device Management, and then click Add Device.

Symbol Conventions

This document uses various distinctive symbols to highlight contents that require special attention during the operation process. The meanings of these symbols are as follows:

Symbol	Meaning
	NOTE: Provides tips and additional information related to the operation and use of the product.

Symbol	Meaning
	CAUTION: Alerts to matters that require attention during operation, as improper handling may lead to product damage, data loss, or functional abnormalities.
	WARNING: The annotations following this symbol demand extra attention, as improper handling could potentially cause personal injury.

Legal Statement

Copyright Statement

Trademark Acknowledgements

Export Compliance Statement

We comply with applicable export control laws and regulations worldwide, including that of the People's Republic of China and the United States, and abide by relevant regulations relating to the export, re-export and transfer of hardware, software and technology. Regarding the product described in this manual, we ask you to fully understand and strictly abide by the applicable export laws and regulations worldwide.

Disclaimer of Liability

- To the extent allowed by applicable law, in no event will we be liable for any special, incidental, indirect, consequential damages, nor for any loss of profits, data, and documents.
- The product described in this manual is provided on an "as is" basis. Unless required by applicable law, this manual is only for informational purpose, and all statements, information, and recommendations in this manual are presented without warranty of any kind, expressed or implied, including, but not limited to, merchantability, satisfaction with quality, fitness for a particular purpose, and noninfringement.
- Users must assume total responsibility and all risks for connecting the product to the Internet, including, but not limited to, network attack, hacking, and virus. We strongly recommend that users take all necessary measures to enhance the protection of network, device, data and personal information. We disclaim any liability related thereto but will readily provide necessary security related support.
- To the fullest extent permitted by applicable law, in no event shall we, our employees, licensors, or affiliates be liable for any indirect, incidental, special, consequential, or punitive damages, including but not limited to loss of profits, loss of sales or business, loss of data, or costs of procurement of substitute goods or services, arising out of or related to your use or inability to use the product or service, even if advised of the possibility of such damages. Some jurisdictions do not allow the exclusion or limitation of liability for personal injury, or of incidental or consequential damages, so the above limitations may not apply to you.
- To the extent allowed by applicable law, in no event shall our total liability to you for all damages for the product described in this manual exceed the amount of money that you have paid for the product.
- When using this product, please strictly adhere to the applicable laws and regulations to avoid infringing upon the rights of third parties, including but not limited to intellectual property rights, data rights, or other privacy

rights. You must also not use this product for the purposes of developing or facilitating the use of weapons of mass destruction, biological or chemical weapons, nuclear weapons, or for any other purposes that violate international norms and regulations.

Privacy Protection Reminder

Uniview complies with applicable privacy protection laws and is committed to protecting user privacy. You may want to read our full privacy policy at our website and get to know the ways we process your personal information.

Please be aware, using the product described in this manual may involve the collection of personal information such as face, fingerprint, license plate number, email, phone number, GPS. Please abide by your local laws and regulations while using the product.

Safety Warnings

The device must be installed, serviced and maintained by a trained professional with necessary safety knowledge and skills. Before you start using the device, please read through this guide carefully and make sure all applicable requirements are met to avoid danger and loss of property.

Storage, Transportation, and Use

- Store or use the device in a proper environment that meets environmental requirements, including and not limited to, temperature, humidity, dust, corrosive gases, electromagnetic radiation, etc.
- Make sure the device is securely installed or placed on a flat surface to prevent falling.
- Unless otherwise specified, do not stack devices.
- Ensure good ventilation in the operating environment. Do not cover the vents on the device. Allow adequate space for ventilation.
- Prevent water or other liquids from entering the device. It may cause device damage and risks such as electric shock and fire.
- Make sure the power supply provides a stable voltage that meets the power requirements of the device. Make sure the power supply's output power exceeds the total maximum power of all the connected devices.
- Verify that the device is properly installed before connecting it to power.
- Do not remove the seal from the device body without consulting us first. Do not attempt to service the product yourself. Contact a trained professional for maintenance.
- Always disconnect the device from power before attempting to move the device.
- Take proper waterproof measures in accordance with requirements before using the device outdoors.
- Warning: Operating this device in a residential environment may cause radio interference.

Power Requirements

- Install and use the device in strict accordance with your local electrical safety regulations.
- Use the recommended cordset (power cord) in accordance with the specified ratings.
- Only use the power adapter supplied with your device.
- Use a mains socket outlet with a protective earthing (grounding) connection.
- Ground your device properly if the device is intended to be grounded.

Battery Safety

Please use batteries properly; otherwise, there is a risk of fire or explosion.

- Warning: Using incorrect battery models can lead to explosion.
- If you need to replace the battery, it is recommended that you go to an authorized service center or have it replaced under professional supervision. We shall not be held responsible for any issues arising from unauthorized battery replacement.

- When replacing the battery, be sure to use a battery of the same type as the original. Using the wrong model for replacement (such as certain types of lithium batteries) may cause safety protection to fail.
- Batteries must not be exposed to overheat environments such as sunlight, fire, as this may lead to fire, explosion, or combustion.
- Do not dispose of batteries in fire or heating appliances. Do not squeeze, bend, or cut batteries, as it may cause explosion.
- Do not expose batteries to extremely high or low temperatures, or to very low-pressure environments, as this may cause explosion or leakage of flammable liquid/gas.
- For products or the included remote control containing a button cell battery: Do not ingest the battery-chemical burn hazard! If swallowed, a button cell battery can cause severe internal burns within 2 hours and may be fatal. Precautions (including but not limited to):
  - Keep new and used batteries away from children.
  - Stop using the product and keep it away from children if the battery compartment is not securely closed.
  - If you suspect that a battery may have been swallowed or inserted inside any part of the body, seek immediate medical attention.

Network Security

Please take all necessary measures to enhance network security for your device.

The following are necessary measures for the network security of your device:

- **Change the default password and set a strong password:** You are strongly recommended to change the default password after your first login and set a strong password of at least nine characters including all three elements: digits, letters and special characters.
  - Do not include the account name or the reverse of the account name.
  - Avoid using consecutive characters, such as 123, abc, etc.
  - Do not use overlapping characters, such as 111, aaa, etc.
- **Keep firmware up to date:** It is recommended that your device is always upgraded to the latest version for the latest functions and better security. Visit our website or contact your local dealer for the latest firmware.

The following are recommendations for enhancing network security of your device:

- **Change password regularly:** Change your device password on a regular basis and keep the password safe. Make sure only the authorized user can log in to the device.
- **Enable HTTPS/SSL:** Use SSL certificate to encrypt HTTP communications and ensure data security.
- **Enable IP address filtering:** Allow access only from the specified IP addresses.
- **Minimum port mapping:** Configure your router or firewall to open a minimum set of ports to the WAN and keep only the necessary port mappings. Never set the device as the DMZ host or configure a full cone NAT.
- **Disable the automatic login and save password features:** If multiple users have access to your computer, it is recommended that you disable these features to prevent unauthorized access.
- **Choose username and password discretely:** Avoid using the username and password of your social media, bank, email account, etc., as the username and password of your device, in case your social media, bank and email account information is leaked.
- **Restrict user permissions:** If more than one user needs access to your system, make sure each user is granted only the necessary permissions.
- **Disable UPnP:** When UPnP is enabled, the router will automatically map internal ports, and the system will automatically forward port data, which results in the risks of data leakage. Therefore, it is recommended to disable UPnP if HTTP and TCP port mapping have been enabled manually on your router.
- **SNMP:** Disable SNMP if you do not use it. If you do use it, then SNMPv3 is recommended.
- **Multicast:** Multicast is intended to transmit video to multiple devices. If you do not use this function, it is recommended you disable multicast on your network.
- **Check logs:** Check your device logs regularly to detect unauthorized access or abnormal operations.
- **Physical protection:** Keep the device in a locked room or cabinet to prevent unauthorized physical access.

- **Isolate video surveillance network:** Isolating your video surveillance network with other service networks helps prevent unauthorized access to devices in your security system from other service networks.

You may also obtain security information under Security Response Center at Uniview's official website.

1 Before Use

Default Network Parameters

Username: admin	Password: 123456
Static IP: 192.168.1.13	Subnet mask: 255.255.255.0

Application Scenarios

Speed gates are typically installed in public places (airports, train stations, museums, theaters, etc.), office premises (office buildings, hospitals, schools, etc.), campus areas, residential communities, and some other locations.

Definitions

Referring to the aforementioned application scenarios collectively as the "target area", the definitions for "entry" and "exit" are as follows:

- Entry: Entering the target area
- Exit: Exiting the target area

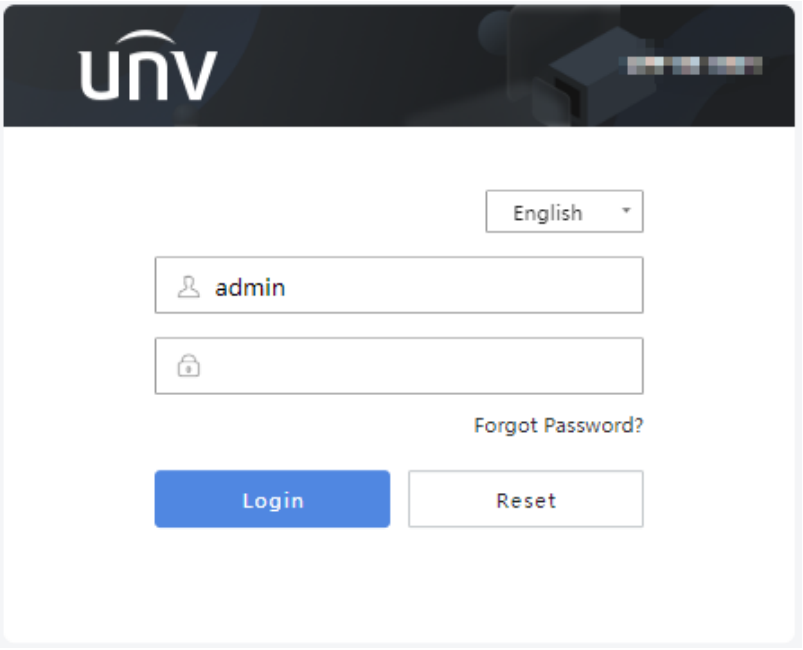
2 Login

Check Before Login

- The device runs normally.
- The client computer (hereinafter referred to as "client") is on the same network segment as the device and is connected to the network

Web Login

1. Open a browser, enter the device's IP address (default: 192.168.1.13) in the address bar, and press **Enter**.



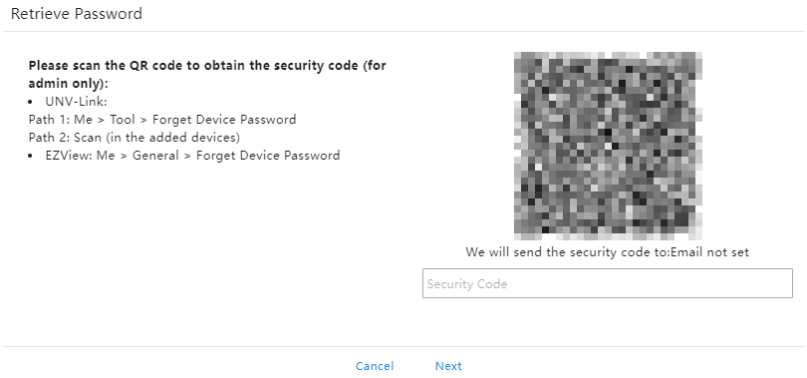
2. Enter the username/password (admin/123456 by default).
3. Click **Login**.
4. (For first-time login) Follow the on-screen instructions to change the password into a strong one and then use the new password to log in

Forgot Password

If you forgot the password after changing it, you can obtain the security code to reset the password.

Note: To use this function, you must have bound an email address with the device (System > User); otherwise contact the local technical support to reset the password.

1. Click **Forgot Password** on the login page, and the **Retrieve Password** page appears.



2. Follow the on-screen instructions to obtain a security code.
3. Enter the security code, and click **Next** to reset the password. For the security of your account, keep the password properly.

Logout

Click ... in the upper-right corner, choose **Logout**, and click **OK** to log out.

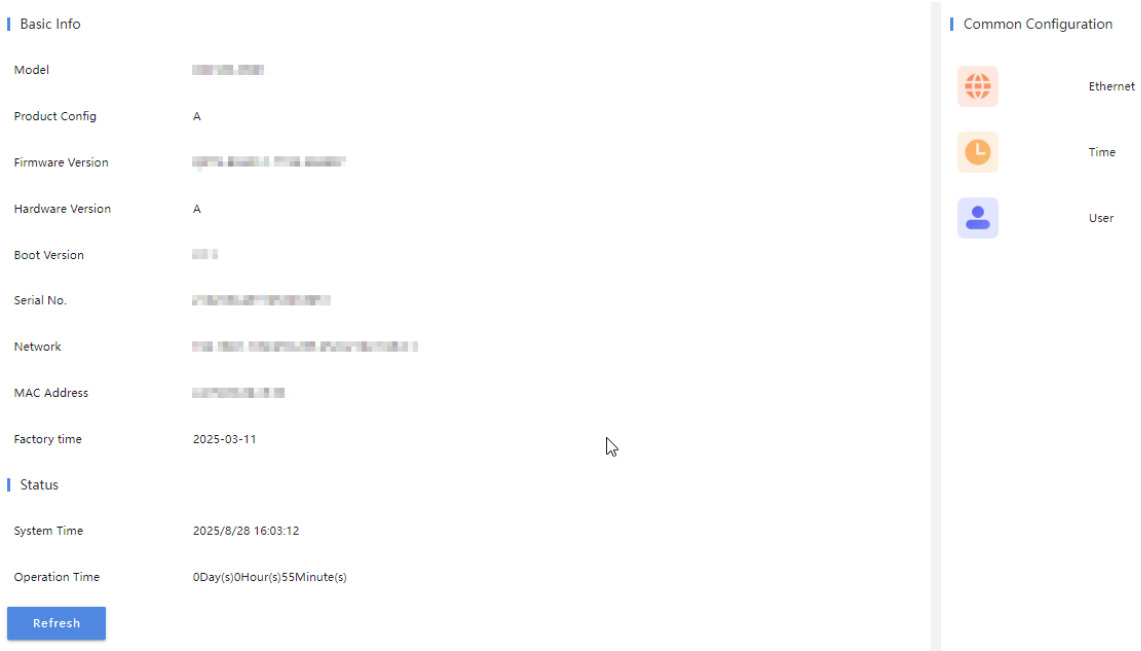
3 Common

Configure commonly used functions.

3.1 Basic Information

View the basic information and real-time operation status of the device and quickly access certain common functions.

Go to **Common > Basic Info**.

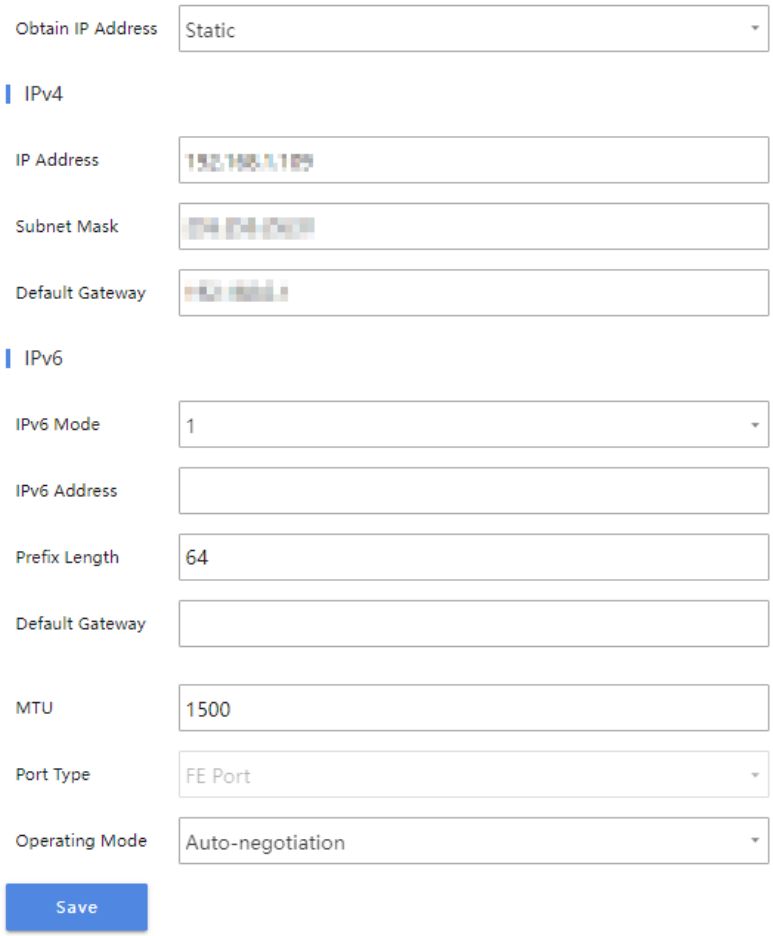


Common configuration: Includes Ethernet, Time, User. You can click the icon or text to open the corresponding page.

3.2 Basic Network Configuration

3.2.1 Ethernet

1. Go to **Setup > Common > Network Basic Config > Ethernet**.



2. Configure Ethernet parameters. Some of the parameters are described below.

Parameter		Description
IPv4	Obtain IP Address	• Static: Configure a static public network IP address for the device manually. Set **Obtain IP Address** to **Static**, and enter the IP address, subnet mask, and default gateway. • DHCP (default): If a DHCP (Dynamic Host Configuration Protocol) server is deployed in the network, the device can automatically obtain an IP address from the DHCP server. • PPPoE: Configure PPPoE (Point to Point Protocol over Ethernet) to assign the device a dynamic IP address to establish network connection. Set **Obtain IP Address** to **PPPoE**, and enter the username and password.
IPv6	Mode	IPv6 has a lot more IP addresses than IPv4, and is faster and safer than IPv4 in terms of data transfer. The IPv6 mode includes DHCP and Manual. The default mode is DHCP.
Parameter	MTU	Maximum transmission unit, the maximum packet size supported by the device in bytes. Range: [576-1500]. Default: 1500.

Parameter		Description
		The greater the value, the higher the communication efficiency, but the higher the transmission delay.
	Operating Mode	• Rate + Half Duplex: At the set rate, the port can only receive or send data at a given time, and there is a physical transmission distance limitation. • Rate + Full Duplex: At the set rate, the port can receive and send data at any given time, without the physical transmission distance limitation. • (Rate +) Auto-negotiation: The port automatically negotiates with the port of the peer end about the (speed and) operating mode, allowing both to run in the most efficient mode.

3. Click **Save**.

3.2.2 Wi-Fi

Wi-Fi modes include: Off, Wi-Fi, and Wi-Fi Hotspot.

Go to **Setup > Common > Network Basic Config > Wi-Fi**.

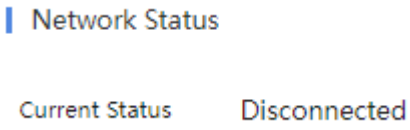
Off

Disable this function.

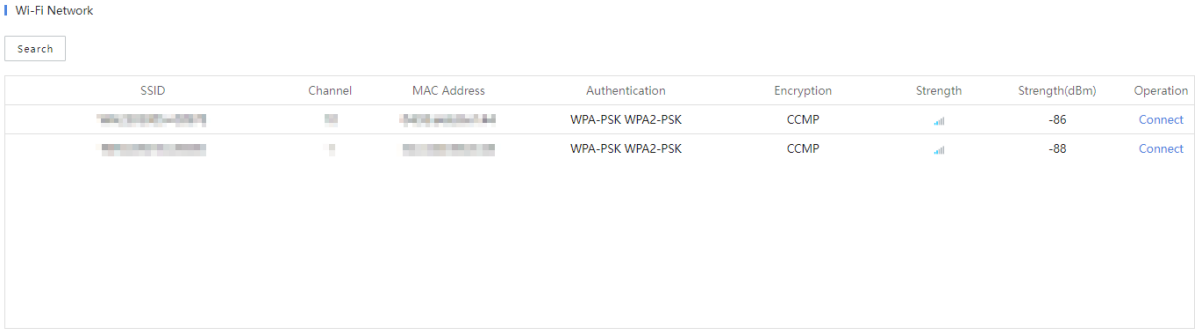
Wi-Fi

Connect the speed gate to the network via the Wi-Fi hotspot.

1. Select Wi-Fi for the Wi-Fi mode. You can see the current network status (for example, Disconnected).



2. Search for the Wi-Fi network you want to connect to in the list of Wi-Fi networks, sorted by signal strength from highest to lowest. Click **Search** to update the list.

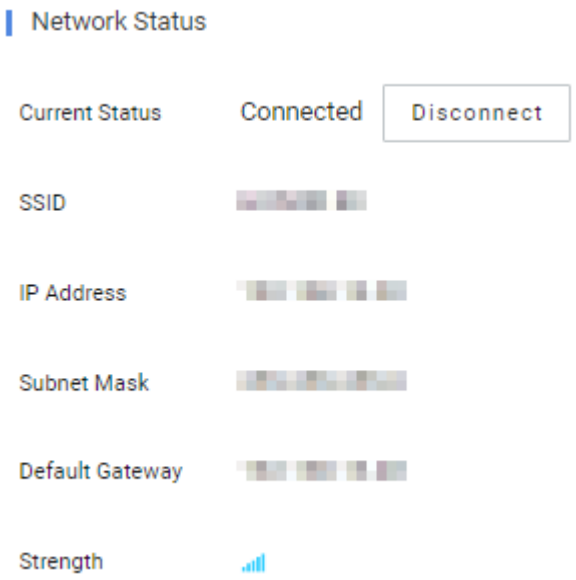


3. Click the corresponding **Connect** for the Wi-Fi network you want to connect to, and configure the parameters.

Parameter	Description
SSID	The name of the wireless signal sent by the router, used to distinguish between different networks. This field is automatically filled in after you select the Wi-Fi network to connect.
Password	Wi-Fi password.
Encryption	Keep the default. If you wish to change it, please select the encryption type that matches the connected Wi-Fi network. Five modes are supported: None, WEP, CCMP, TKIP, and CCMP-TKIP.
Authentication	Keep the default. If you wish to change it, please select the authentication mode that matches the connected Wi-Fi network. Three modes are supported: OPEN, SHARED, and WPA-PSK WPA2-PSK. • OPEN: No password configuration is needed. • SHARED: Enter a password that is an 8-63 character string (the string can be a combination of pure numbers, pure letters, common characters, or a mix of these types). • WPA-PSK WPA2-PSK: Enter a password that is an 8-63 character string (the string can be a combination of pure numbers, pure letters, common characters, or a mix of these types).
Obtain IP Address	Choose based on actual needs. Currently supports DHCP and static address.

4. Click **Connect**, and the current status will display as "Connecting...". If the password is correct, the current status will switch to "Connected", and network information will be displayed; otherwise, it will switch to "Disconnected".

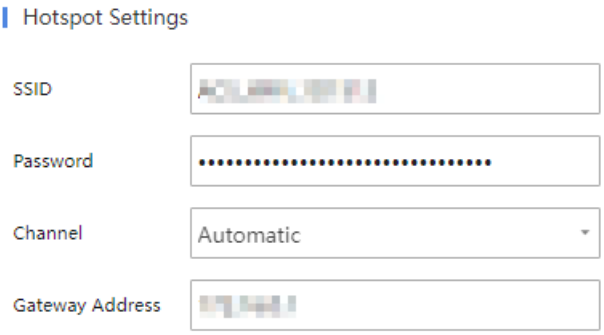
   In connected state, clicking **Disconnect** will disconnect the Wi-Fi connection.



5. Click **Save**.

Wi-Fi Hotspot Mode

1. Select the **Wi-Fi Hotspot** mode.
2. Configure the Wi-Fi hotspot parameters.



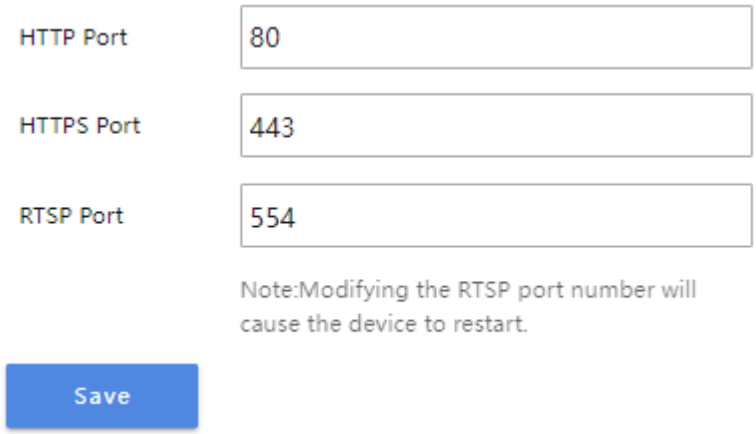
Parameter	Description
SSID	Customize the Wi-Fi hotspot name. 1-32 characters: Uppercase and lowercase letters, digits, underscores, and hyphens.
Password	Customize the Wi-Fi hotspot password. 8-32 characters: Commonly used characters entered via the keyboard.
Channel	Select the appropriate channel based on your actual needs. Default: Automatic
Gateway Address	Enter the gateway address of the router administrator. Enter according to the actual situation.

3. Click **Save**.

3.2.3 Port

Set service ports to access the device via network.

1. Go to **Setup > Common > Network Basic Config > Port**.



2. You can use the defaults or customize them in case of port conflicts.

   Note: If the HTTP port number you entered has been used, the message "Port conflicts. Please try again." will appears.

   Ports 23, 81, 82, 85, 3260, and 49152 have been assigned for other purposes and cannot be used. In addition, the system can also dynamically detect other port numbers that are already in use.

   - HTTP/HTTPS Port: After changing the HTTP/HTTPS port number, you need to add the new port number after the IP address when logging in. For example, if the HTTP port number is set to 88, you need to use http://192.168.1.13:88 to log in to the device.
   - RTSP Port: Port for the Real-Time Streaming Protocol. Enter an available port number.

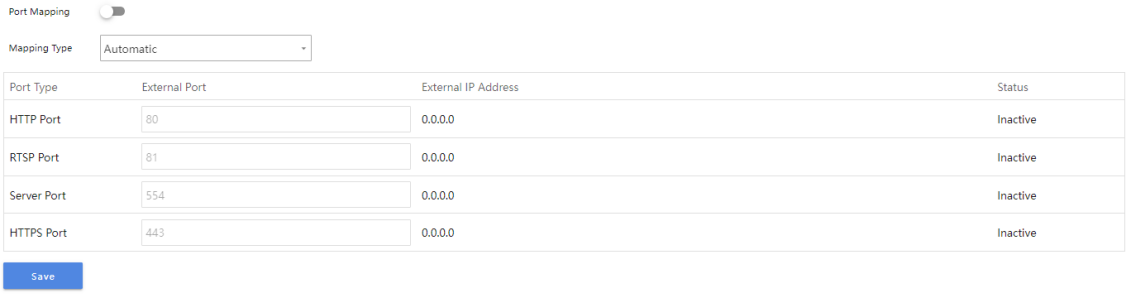
3. Click **Save**.

3.2.4 Port Mapping

Configure port mapping so computers on the WAN can access the device on the LAN.

This function is disabled by default.

1. Go to **Setup > Common > Network Basic Config > Port Mapping**.



2. Enable **Port Mapping**.
3. Set the mapping type, including Automatic (default) and Manual.
   - Automatic: The external port numbers and IP address are assigned automatically.
   - Manual: The external port numbers need to be set manually.
4. Click **Save**.

3.3 External Device Configuration

3.3.1 485 Serial Port

The RS485 port can connect an external card reader for authentication.

Go to **Common > External Device > 485 Serial Port Configuration**.

If an RS485 card reader is installed on the entry direction of the speed gate, the corresponding parameters need to be configured; the same applies to the exit direction. After configuration is complete, click **Save**.

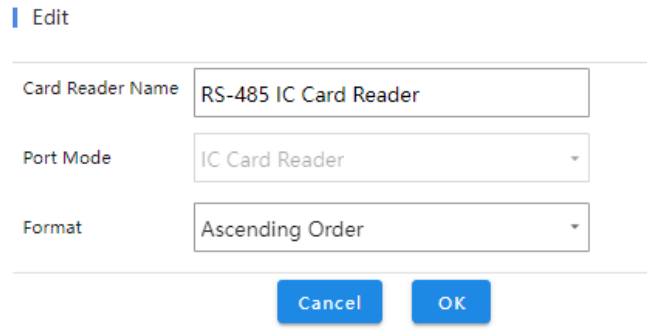
RS485

Parameter	Description
Baud Rate	Data transmission speed. Default: 115200.
Data Bits	The actual number of data bits in a group of data packets. Default: 8.
Stop Bits	Indicates the end of transmission of a group of data. Default: 1.
Parity	Used to check whether the received data bits are erroneous. Default: None.
Flow Control	Used to control data transmission to prevent data loss. Default: None.

RS485 External Device Configuration

Set the parameters of the external card reader connected to the RS485 serial port.

Click  to modify the parameters of the corresponding card reader.



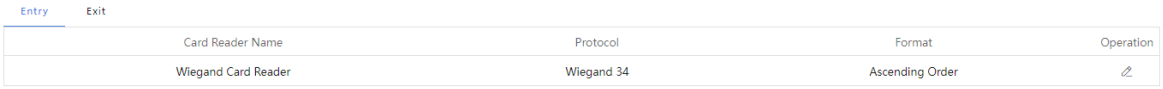
Parameter	Description
Card Reader Name	Set a unique custom name.
Port Mode	• IC Card Reader: Bind an IC card reader. • QR Code Reader: Bind a QR code reader.
Format	• Ascending Order: The sequence is the same as the card number read by the card reader. • Descending Order: The sequence is the reverse of the card number read by the card reader.

3.3.2 Wiegand Interface

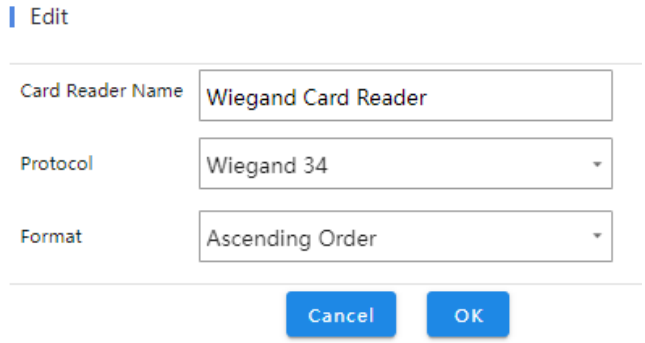
The Wiegand interface can connect an external card reader for authentication.

Go to **Common > External Device > Wiegand Interface**. The parameters will be automatically saved when the configuration is finished

If a Wiegand card reader is installed on the entry direction of the speed gate, the corresponding parameters need to be configured; the same applies to the exit direction. After configuration is complete, click **Save**.



Click ✎ to modify the parameters of the corresponding card reader.



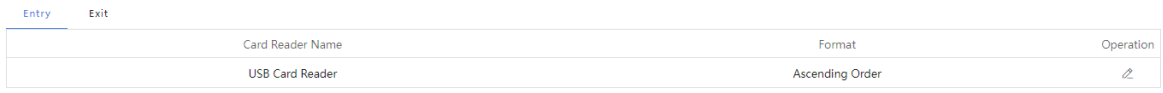
Parameter	Description
Card Reader Name	Set a unique custom name.
Protocol	• Wiegand 26: Read 3-byte card numbers via the Wiegand 26 protocol. • Wiegand 34: Read 4-byte card numbers via the Wiegand 34 protocol. • Custom: Custom Wiegand protocol.
Format	• Ascending Order: Show the same sequence of the card number as the number read by the card reader. • Descending Order: Show the opposite sequence of the card number as the number read by the card reader.

3.3.3 USB

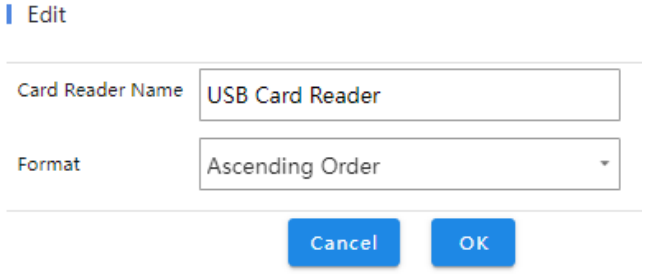
The USB interface can connect an external card reader for authentication.

Go to **Common > External Device > USB**.

If a USB card reader is installed on the entry direction of the speed gate, the corresponding parameters need to be configured; the same applies to the exit direction. The configuration will be saved automatically.



Click the corresponding ✎ to modify the card reader settings



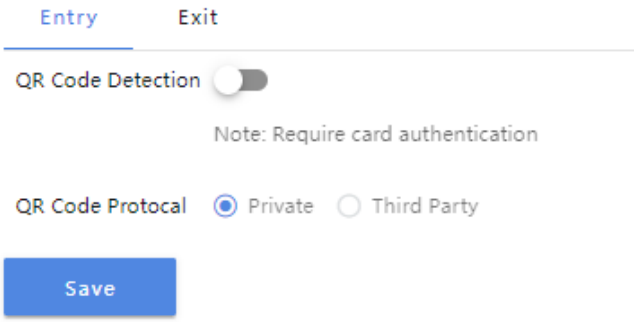
Parameter	Description
Card Reader Name	Enter a unique custom name.
Format	• Ascending Order: The sequence is the same as the card number read by the card reader. • Descending Order: The sequence is the reverse of the card number read by the card reader.

3.3.4 QR Code

When authentication mode is set to number allowlist, QR codes generated based on numbers can be used for verification and access.

If a QR code module is installed on the entry direction of the speed gate, the corresponding parameters need to be configured; the same applies to the exit direction.

1. Go to **Common > External Device > QR Code**.



2. Enable **QR Code Detection**, and select a QR code protocol.

   Note: It is required to add the number allowlist authentication mode in authentication template and bind the template in door verification config.

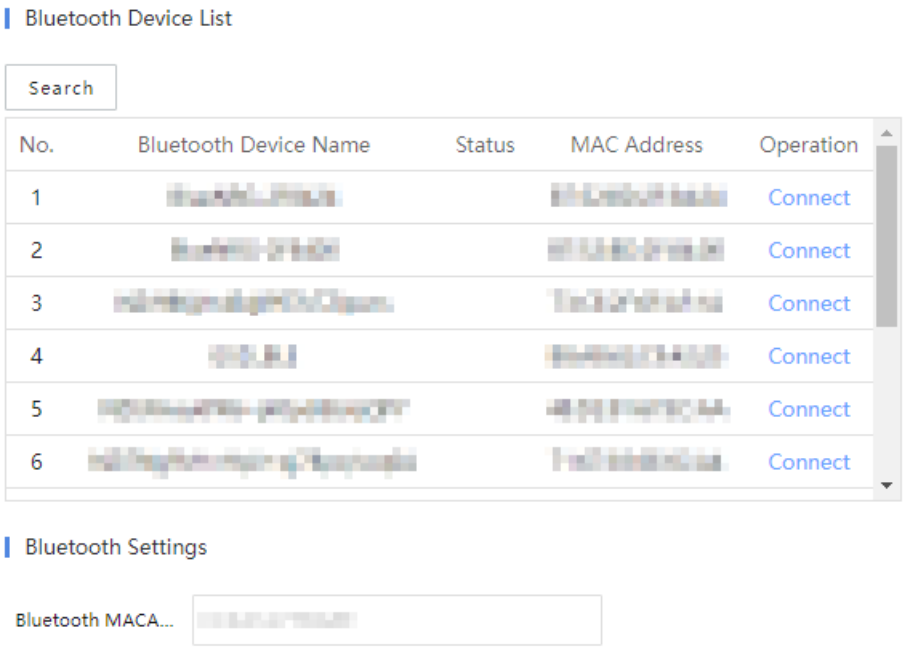
3. Click **Save**.

3.3.5 Bluetooth

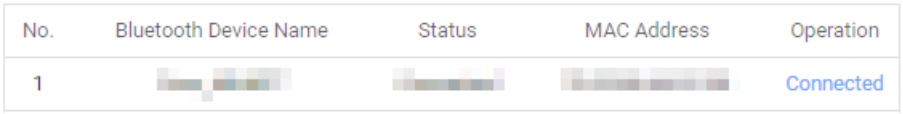
You can use the Bluetooth function to connect other devices.

1. Go to **Setup > Common > External Device > Bluetooth.**

2. Enable the Bluetooth function.
3. The discovered Bluetooth devices and their MAC addresses are displayed. You can click **Search** to search again.



4. Click the corresponding **Connect** for the Bluetooth you want to connect. A pop-up window appears. Confirm the connection to proceed.
5. On the device being connected, confirm the connection. When connected, the status of the Bluetooth device changes to "Connected."

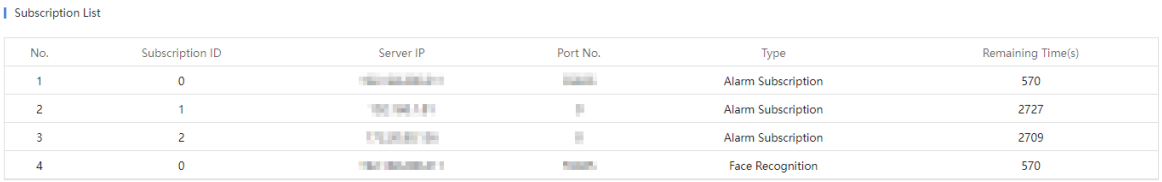


To disconnect, perform the operation on the connected device.

3.4 Server

View information about the server that the speed gate is connected to.

Go to **Common > Server** to view server information, including server IP, port number, and type.



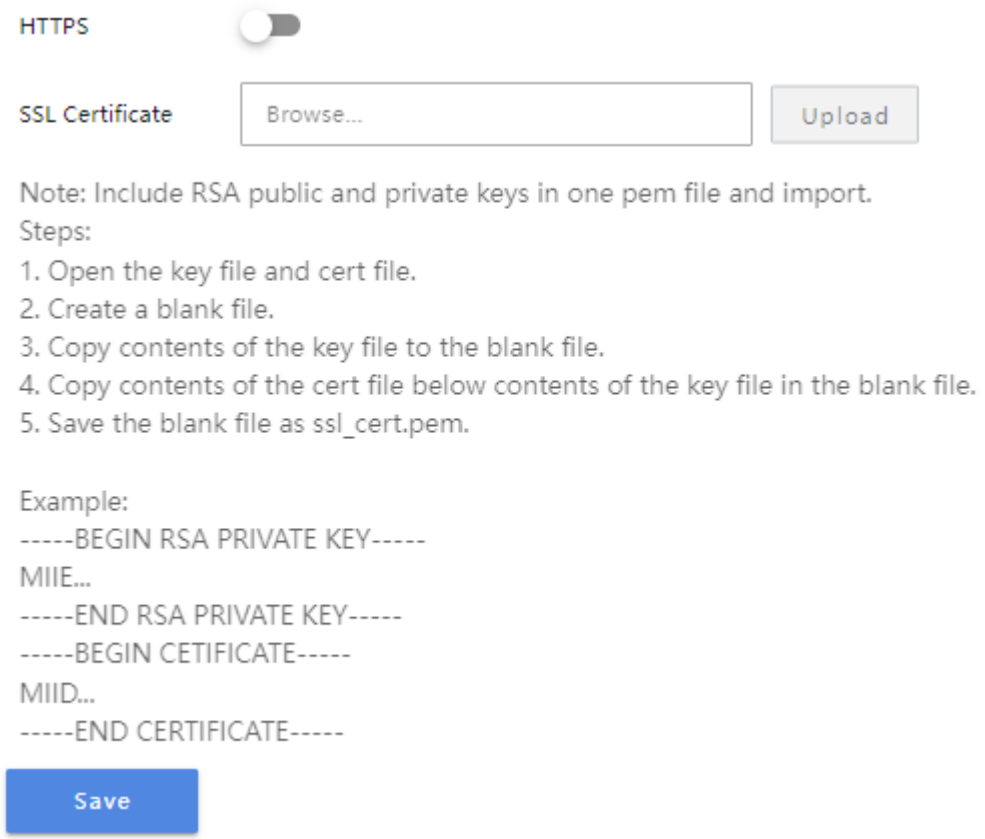
4 Security

4.1 Network Security

4.1.1 HTTPS

HTTPS is a secure version of the HTTP protocol that uses SSL protocol to authenticate both a client and a server, and encrypt data during transmission to prevent data from being stolen or altered, enhancing data security

1. Go to **Setup > Security > Network Security > HTTPS**.



2. Enable **HTTPS**.
3. Click **Browse**, locate the SSL certificate, and click **Upload**.

Note:

- An SSL certificate is issued by the Certificate Authority after verifying that the server is reliable and compliant with the SSL protocol. It is used to activate SSL protocol (an Internet protocol used for authentication and encryption), transmit encrypted data between client and server so that it cannot be leaked and tampered with, and confirm the reliability of the server.

  An SSL certificate includes a public key (for encryption) and private key (for decryption).
- Put the RSA public key and private key in one pem file, and then import.

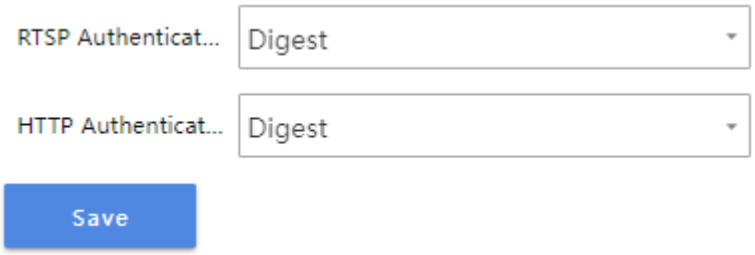
4. Click **Save**.

4.1.2 Authentication

Authentication refers to the procedure of identifying clients. Only after successful authentication can the data be transmitted based on the protocol, improving the security of data transmission.

- RTSP Authentication: Transmits audio and video data in real time through the RTSP protocol. It establishes a two-way connection between the server and the client, and controls either a single or several streams of continuous media such as audio and video for a long time.
- HTTP authentication: Transfers data as a file via the HTTP protocol. It establishes a one-way connection between the client and the server, and the connection will end after the server responds to the request from the client. The connection will be re-built to transfer data if there is a new request.

1. Go to **Setup > Security > Network Security > Authentication**.



2. Choose an authentication mode.

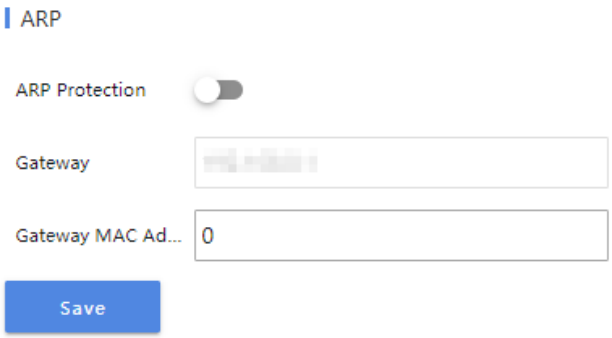
Parameter	Description
RTSP Authentication	Choose an authentication mode: None, Basic, or Digest. • None: Transmits data without authentication. • Basic: Authentication information is transferred in plaintext without encryption, which imposes serious security risks. • Digest: Authentication information is encrypted to provide higher security.
HTTP Authentication	Choose an authentication mode: None or Digest.

3. Click **Save**.

4.1.3 ARP Protection

ARP attack mainly exists in the local area network (LAN), which forges IP address and physical address (MAC address) to achieve ARP spoofing, causing communication failures among devices within the local area network. Configure ARP protection, and the device will verify the physical address (MAC address) of the access source, so as to avoid ARP spoofing attacks.

1. Go to **Setup > Security > Network Security > ARP Protection**.

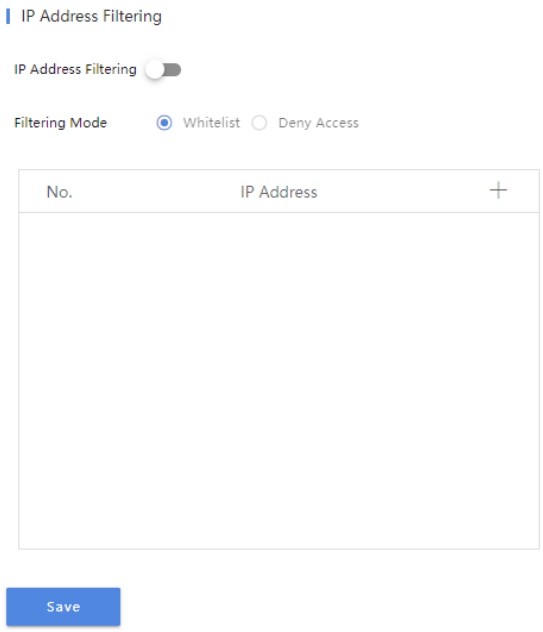


2. Enable **ARP Protection**.
3. Enter the gateway and its physical address (legal MAC address).
4. Click **Save**.

4.1.4 IP Address Filtering

Use IP address filtering to allow or forbid access from specified IP addresses.

1. Go to **Setup > Security > Network Security > IP Address Filtering**.

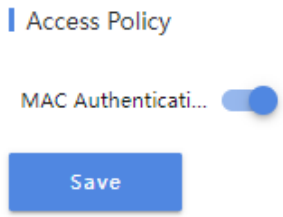


2. Enable **IP Address Filtering**.
3. Set the filtering mode to **Whitelist** or **Deny Access**. If Whitelist is selected, only the added IP addresses are allowed to access the device. If Deny Access is selected, only the added IP addresses cannot access the device.
4. Click **+**, enter IP address(es).
   - Up to 32 IP addresses can be added. Duplicate addresses are not allowed.
   - The first byte of the IP must be 1-233, and the fourth byte cannot be 0. Invalid IP addresses such as 0.0.0.0, 127.0.0.1, 255.255.255.255, and 224.0.0.1 are not allowed.
5. Click **Save**.

4.1.5 Access Policy

When enabled, access is allowed only if the MAC address is authenticated successfully, which has higher security; When disabled, access is allowed for any MAC address, which poses security risks.

1. Go to **Setup > Security > Network Security > Access Policy**.

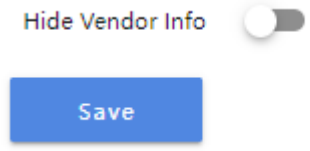


2. Enable **MAC Authentication**.
3. Click **Save**.

4.2 Registration Information

You can set to hide the vendor of the speed gate from the server.

1. Go to **Setup > Security > Registration Info**.



2. Enable **Hide Vendor Info**.
3. Click **Save**.

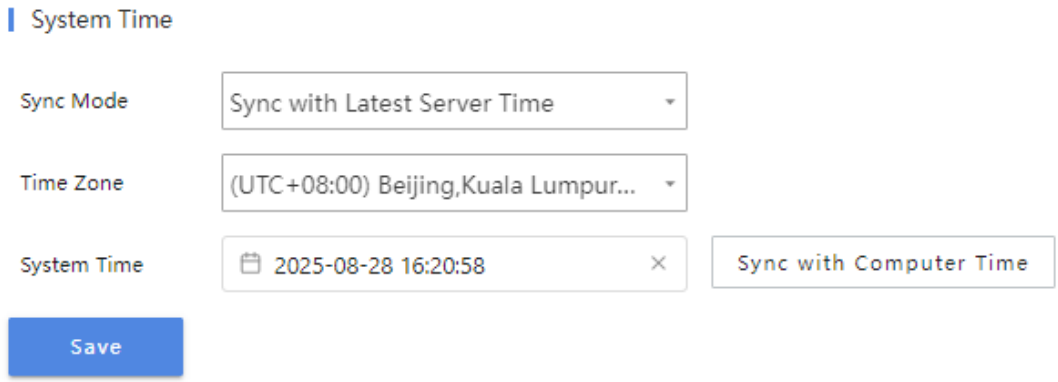
5 System

5.1 Time

5.1.1 Time

Set the system time.

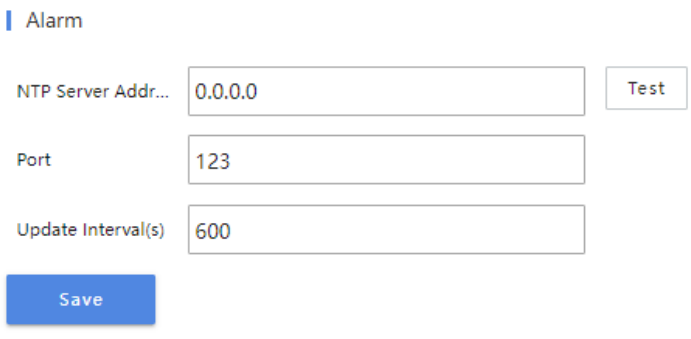
1. Go to **Setup > System > Time > Time**.



2. Choose a method to set the time.
   - Set the time manually in the **System Time** field.

     Note: Make sure **Sync Mode** is set to **Sync with Latest Server Time**; otherwise, the device time will still sync with other sources after you set it manually.
   - Sync time automatically:

     (1) Choose the time sync mode. Some parameters are described below.

Parameter	Description
Sync with System Configuration	Current system time.
Sync with Management Server (ONVIF)	The device regularly syncs time with the management server connected via Onvif. Each sync updates the time once.
Sync with Latest Server Time	Default sync mode. The device regularly syncs time with all the connected servers. Each sync updates the time once.
Sync with NTP Server	NTP Server: A server that operates based on the Network Time Protocol (NTP) to sync the time between distributed time servers and clients. To choose this sync mode, you need to configure the following parameters. 

Parameter	Description
	• NTP Server Address: Enter the NTP server address and click **Test** to check the network communication. A message will appear if the NTP is verified successfully. • Port: Range: [1-65535], integer only, default: 123. • Update Interval(s): Range: [30-86400], integer only, default: 600.

(2) Choose the time zone.

(3) Click **Sync with Computer Time**, and the device will sync time based on the set mode.

3. Click **Save**.

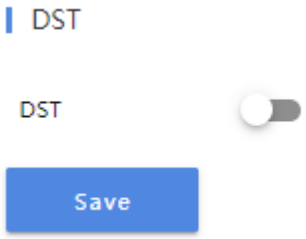
5.1.2 DST

DST (Daylight Saving Time) is a local time system designed to make full use of daytime to save energy, which sets clocks forward by one hour in summer months.

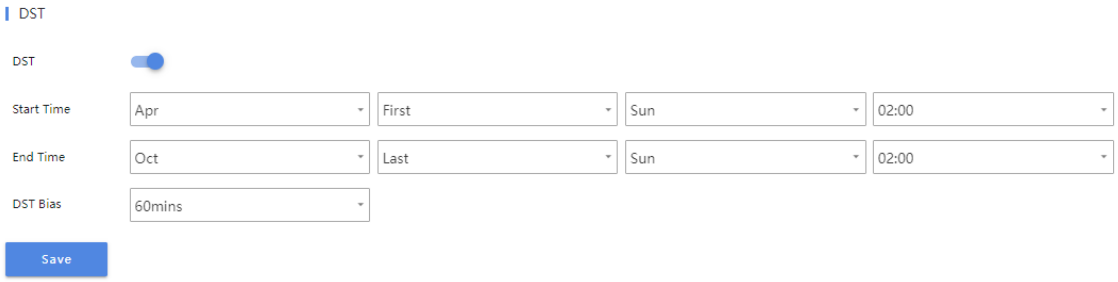
This function is disabled by default.

Note: DST rules vary in different countries.

1. Go to **Setup > System > Time > DST**.



2. Enable **DST**.

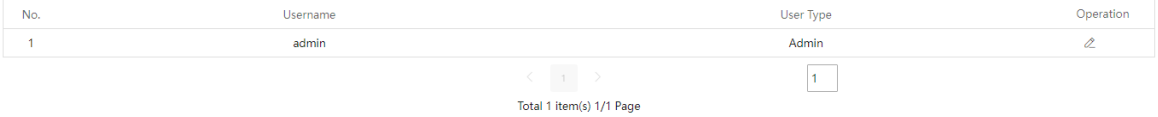


3. Set the start time, end time, and DST bias as needed.
4. Click **Save**.

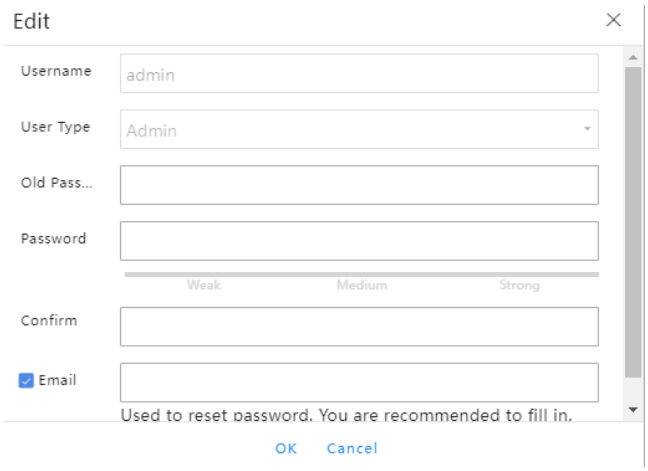
5.2 User

Users are entities that manage and operate the system. The speed gate has only one admin user, which can only be edited.

Go to **Setup > System > User**.



Click ✎ to change the user password and email address, and click **OK** to save the settings.



5.3 Maintenance

Note:

- The following operations will restart the device: software upgrade, system restart, restoring default configurations, importing configurations, and importing face library.
- Restarting the device will interrupt the ongoing services and so must be performed with caution.

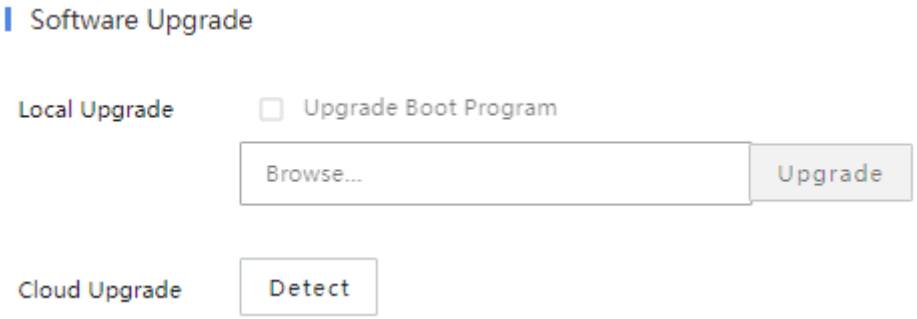
Go to **Setup > System > Maintenance**.

Software Upgrade

The software can be upgraded through local upgrade and cloud upgrade.

Note:

- Make sure the upgrade file matches the device; otherwise, unexpected problems may occur.
- The version file is a **.zip** file that includes all the upgrade files.
- Power must be connected throughout the upgrade.

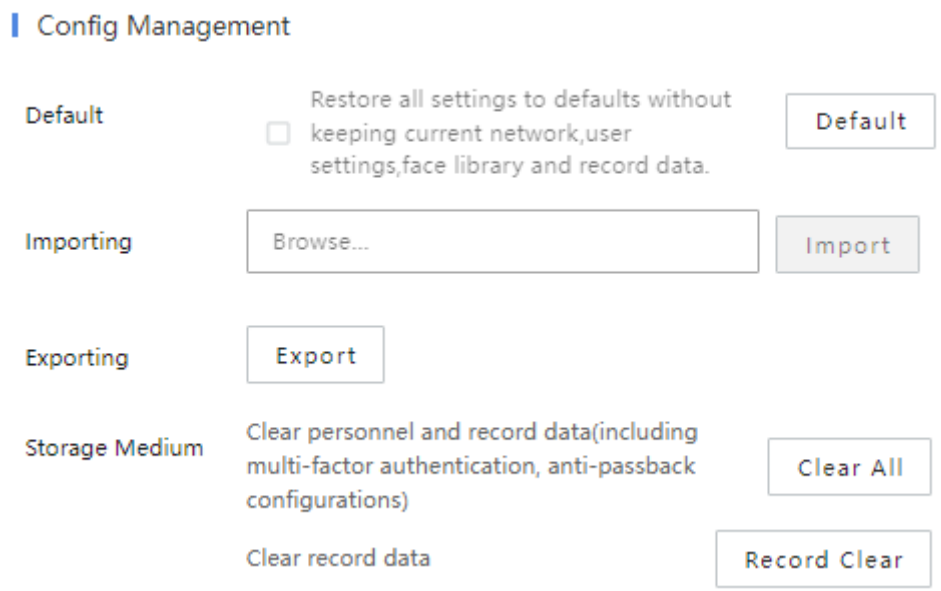


- Local upgrade
  1. Click **Browse**, and select the correct upgrade file.

     Note: If applicable, select **Upgrade Boot Program**, and the boot program will also be upgraded. Only some devices support this feature.
  2. Click **Upgrade** to start upgrade. The device will restart automatically after the upgrade is completed, and then the **Login** page is displayed.
- Cloud upgrade: Click **Detect** to check for new versions. You can perform a cloud upgrade if a new version is available on the cloud server.

System Configuration

You can export the current configurations of the device and save them to the computer or an external storage device. You can also restore configurations by importing an exported configuration file.



- Default: Clicking **Default** will restore default settings except network settings, user settings, face libraries, and record data. The device will automatically restart.

  To restart all settings, including network settings, user settings, face libraries, and record data, to factory defaults, select the **Restore all settings to defaults without keeping current network, user settings, face library and record data** checkbox.

- Import Configurations

  Note: Make sure the configuration file to import matches the device model; otherwise, unexpected results may occur.

  1. Click **Browse** next to the **Import** button.
  2. Select the configuration data, and then click **Import**.
  3. Click **OK**. The device will restart after you import the configuration file.

- Export Configurations

  1. Click **Browse**, and choose the destination folder.
  2. Click **Export**, enter the encryption password, confirm the password, and then click **OK**.

- Storage Medium: Click **Clear All** to clear face libraries and record data, or click **Record Clear** to clear record data only.

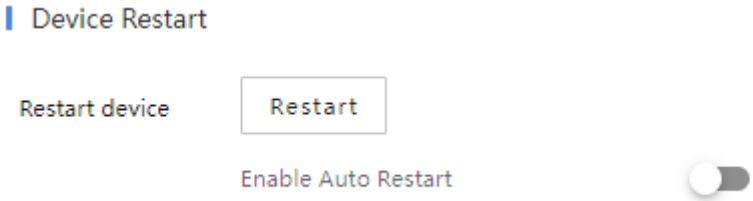
Diagnosis Info

Diagnosis information includes logs and system configurations, and you can click **Export** to save them to a custom path.

Device Restart

You can choose to restart the device manually or automatically.

Note: Restarting the device will interrupt the ongoing services.



- Restart manually: Click **Restart**, and then confirm to restart the device.
- Restart automatically:
  1. Turn on **Enable Auto Restart** and set the restart time.
  2. Click **OK**, and then the device will automatically restart at the set time.

6 Network

6.1 Basic

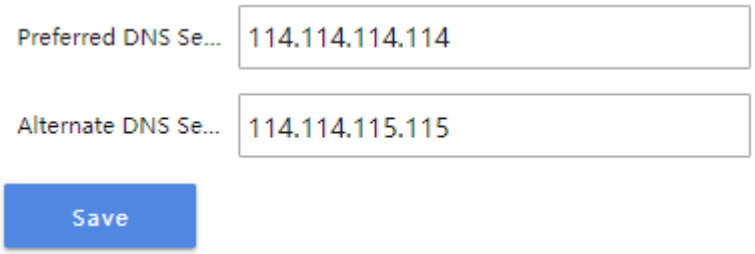
See **Common >** Ethernet.

6.2 Advanced Settings

6.2.1 DNS

The DNS server can automatically convert domain names into IP address and resolve the door station's domain name.

1. Go to **Setup > Network > Advanced Setting > DNS**.

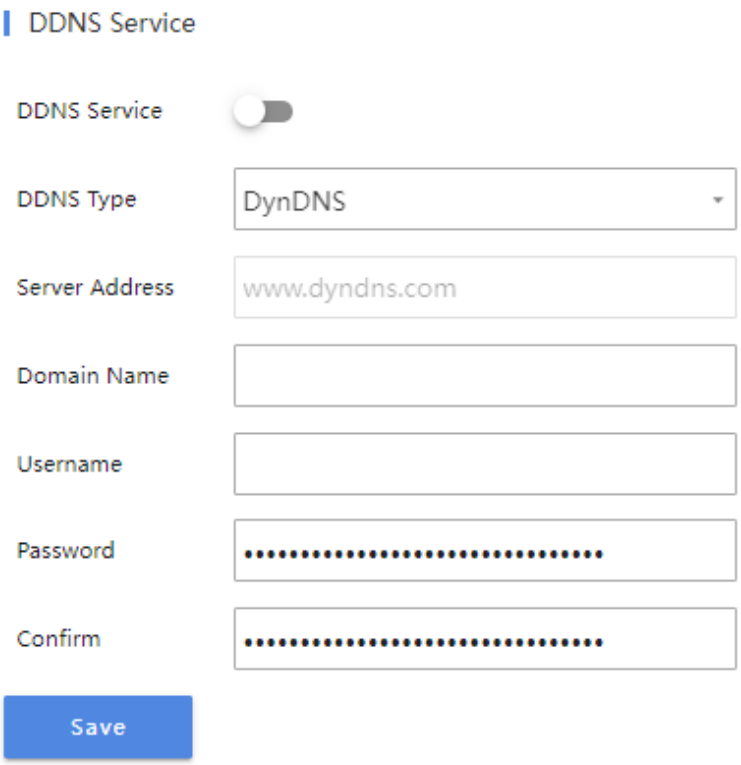


2. Set the DNS server address.
3. Click **Save**.

6.2.2 DDNS

Dynamic DNS (DDNS) automatically maps the device's dynamic public IP address to a static domain name. This allows other devices on the Internet to reliably access the device (e.g., for remote monitoring), even when its IP address changes.

1. Go to **Setup > Network > Advanced Setting > DDNS**.



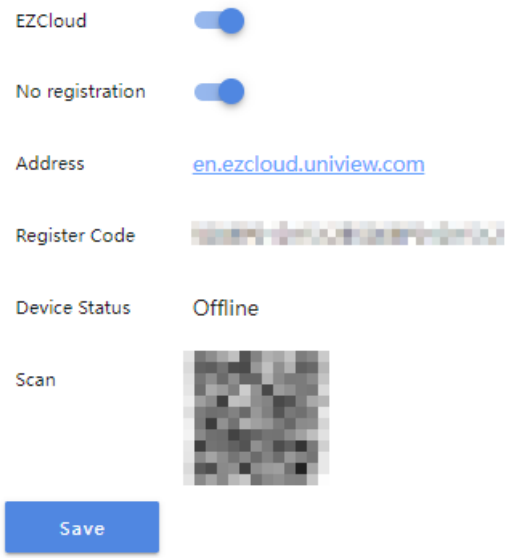
2. Enable **DDNS Service**.
3. Select the DDNS type.
   - DynDNS/No-IP: Enter the domain name, username, password, and confirm the password.
     - Domain name: Domain name assigned by your DDNS service provider, for example, www.dyndns.com.
     - Username and password: The corresponding username/password for your DDNS account on the domain name service website, for example, ww.dyndns.com.
   - EZDDNS: Customize a domain name for your device (4 to 63 characters are allowed, including uppercase and lowercase letters, digits, underscores, and hyphens).

     Click **Test** to check if the domain name is available.
4. Click **Save**.

6.3 EZCloud

You can add the device to the cloud website for remote access.

1. Go to **Setup > Network > EZCloud**.



2. Enable **EZCloud**.
3. (Optional) Enable **No registration**, and you can add the device to the app without registering an account.
4. Click **Save**.
5. Scan the QR code using the UNV-Link app, and follow the on-screen instructions to add the device to the app.

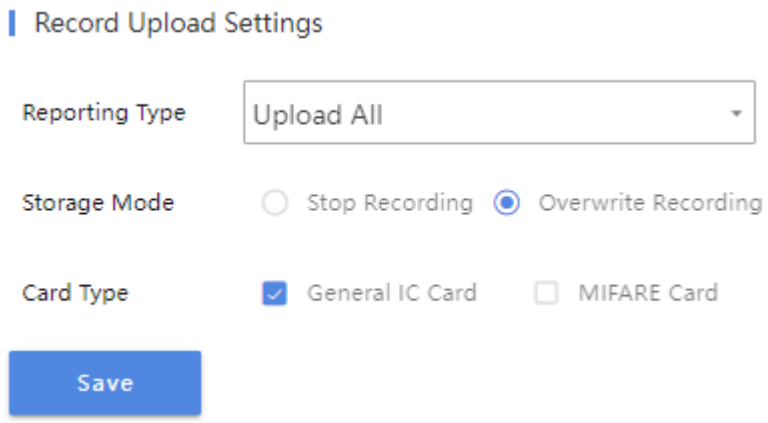
If the device is online and has been added to the app, the device status is **Online**. To delete the device from cloud, click **Logout**.

7 Access Control

7.1 Device Parameter Configuration

7.1.1 Device Parameter Configuration

1. Go to **Setup > Access Control > Device Parameter Config**.



2. Select a reporting type to report records to Server.
   - Upload All: The device reports all records, including success and failure records.
   - Upload Success Record: The device only reports success records.
3. Select a storage mode to specify the policy when the storage space is used up.
   - Stop Recording: Recording will stop.
   - Overwrite Recording: The oldest recording will be overwritten first.
4. Select a card type. The two card types cannot be selected simultaneously.

- General IC Card: The device can read general IC cards through a card reader.
- MIFARE Card: Inductive smart IC card.

5. Click **Save**.

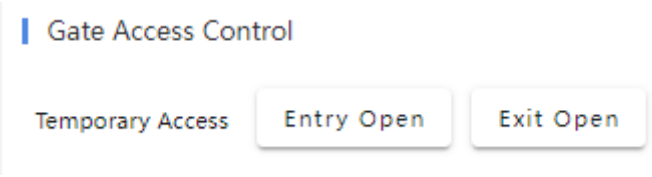
7.1.2 Gate Access Control

Control the opening of the speed gate, and configure gate opening parameters.

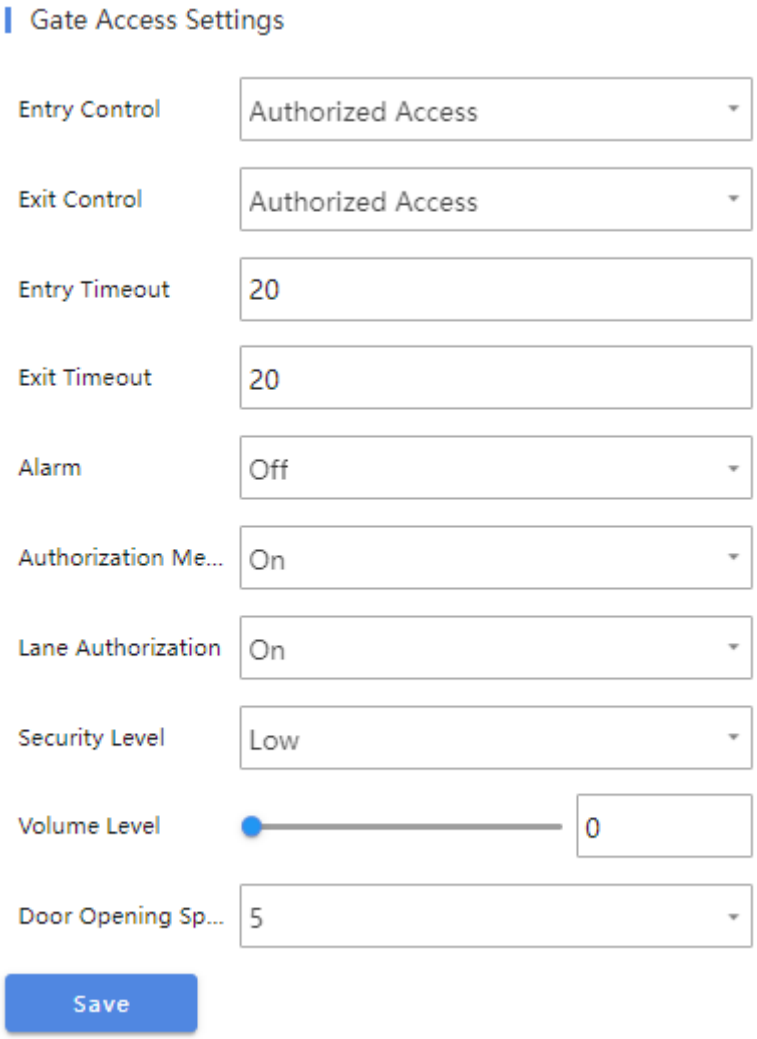
Go to **Setup > Access Control > Device Parameter Config > Gate Access Control**.

Gate Opening Control

Click the button to open the gate for the entry or exit direction.



Gate Access Settings



Some parameters are described below. Click **Save** when you complete the configuration.

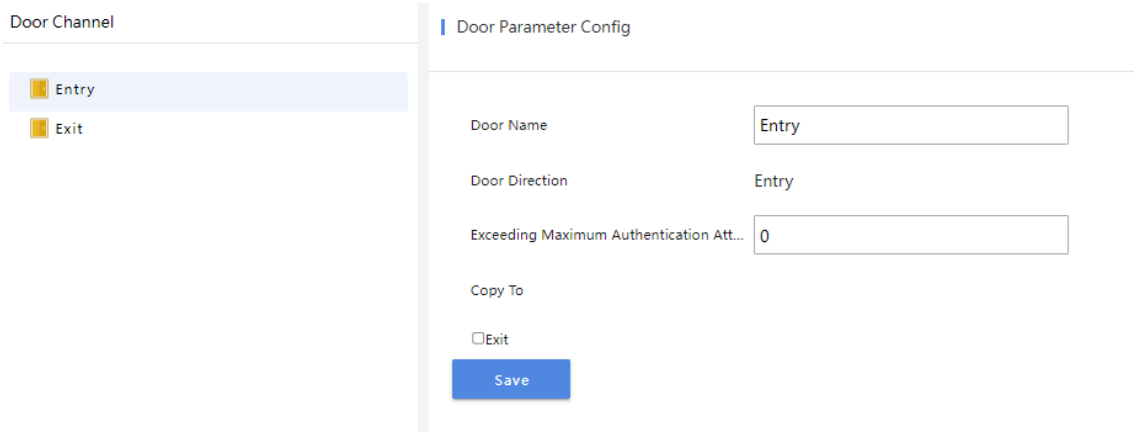
Parameter	Description
Entry/Exit Control	• Authorized Access: People can pass through after verification (face/card/QR code).

Parameter	Description
	• Free Access: The gate will open automatically when it detects an approaching person. • Forbidden Access: No people can pass through.
Entry/Exit Timeout	Prerequisites: For **Entry Timeout**, **Entry Control** must be set to **Authorized Access** or **Free Access**; for **Exit Timeout**, **Exit Control** must be set to **Authorized Access** or **Free Access**. Timing starts from the moment the gate opens. If no person is detected passing through within the set time, the gate will close automatically.
Alarm	Prerequisites: **Entry Control** must be set to **Authorized Access** or **Free Access**. When enabled, if an intrusion is detected, an audio alarm will sound.
Authorization Memory	Prerequisites: **Entry Control**/**Exit Control** must be set to **Authorized Access**. Taking the scenario where n individuals pass through consecutively in the entry direction as an example, the exit direction follows the same logic. 1. Initiate the first verification, which supports card swiping, QR code scanning (requires a QR code scanner), and face recognition (requires a recognition terminal). 2. Once the verification is successful, the barrier switches to the entry opening state. Within the Entry Timeout period, complete the second verification. 3. Repeat the first two steps to complete the remaining (n-2) verifications. During this period, the barrier remains in the entry opening state. 4. After the final verification, within the Entry Timeout period, the first person must pass through the speed gate. **Note:** If no people pass through within the set duration, the barrier will close, and no one will be allowed to pass. 5. The remaining n-1 people pass through the speed gate one after another, ensuring that the time interval between the passage of adjacent people does not exceed the Entry Timeout period. **Note:** If a person fails to pass through within the set duration, the barrier will close, and those following the person will not be allowed to pass. 6. Once the last person has passed through the speed gate, the barrier will close. Application example: A tour guide scans the tickets of 30 people consecutively at the entrance, and the speed gate can allow all 30 people to pass through in one go.
Lane Authorization	• Enabled: People can stand inside or outside the lane for verification. • Disabled: People can only stand outside the lane for verification.
Security Level	Sensitivity for detecting tailgating.
Volume Level	Sound volume outside the speed gate. The higher the number, the louder the volume. 0 indicates mute.
Door Opening Speed	Barrier opening/closing speed. Five options are available.

7.2 Door Parameter Configuration

Configure door opening parameters for entry and exit directions for the speed gate.

1. Go to **Setup > Access Control > Door Parameter Config**.



2. Configure the parameters for the entry direction.

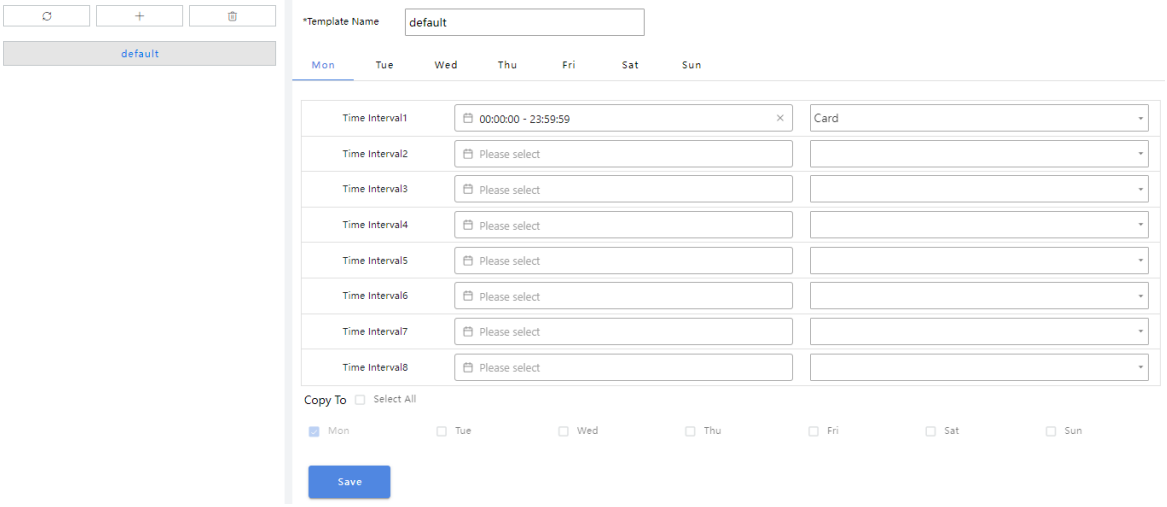
Parameter	Description
Door Name	Input a unique custom name.
Exceeding Maximum Authentication Attempt	An alarm will be triggered when the number of continuous failed card swipes reaches the set value. 0 means no alarm. If Linkage Configuration is set, the corresponding alarm will be generated.

3. Repeat the previous step to configure parameters for the exit direction. You may also copy the settings.
4. Click **Save**.

7.3 Authentication Template

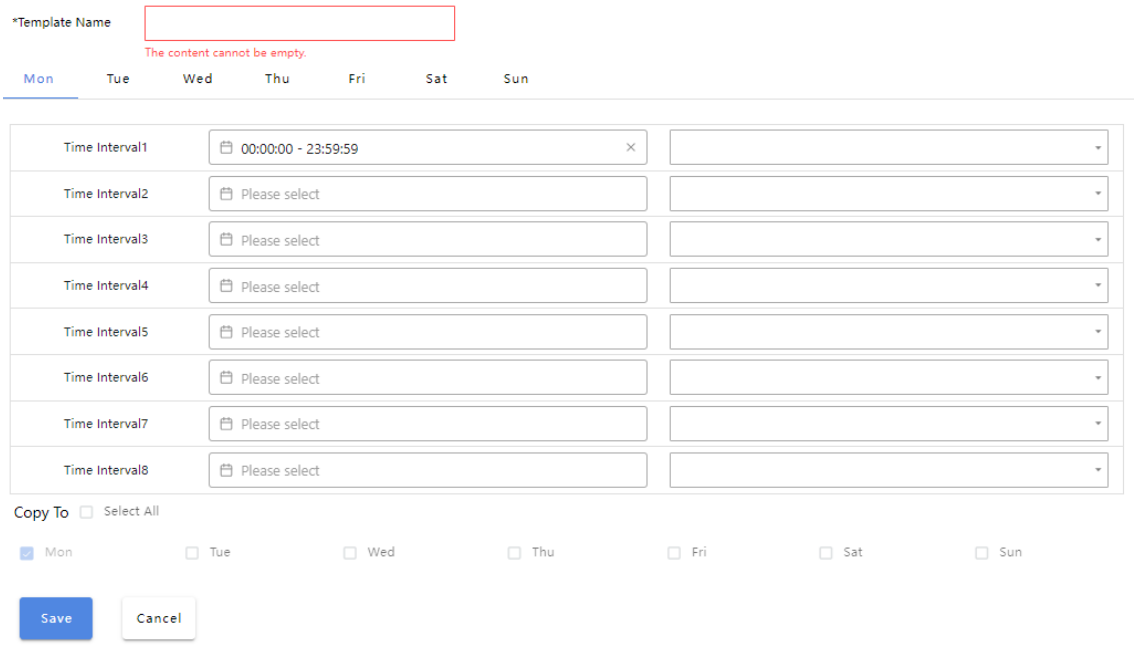
Set authentication modes for different time periods in a week for different scenarios.

Go to **Setup > Access Control > Check Template**.



Add

1. Click **+**, an empty template appears on the right.



2. Set the template name.
3. Set the time interval. Up to 8 periods are allowed, and periods cannot overlap.
4. Select the authentication modes from the drop-down list.
5. Complete the settings for other six days. To apply the current settings to other days, select the check box(es) for the days and then click **Copy**.
6. Click **Save**.

Edit

Click the template name on the left. The template details are displayed on the right. Edit the template and then click **Save**.

Delete

Click the template name on the left, click on the top, and then confirm the deletion.

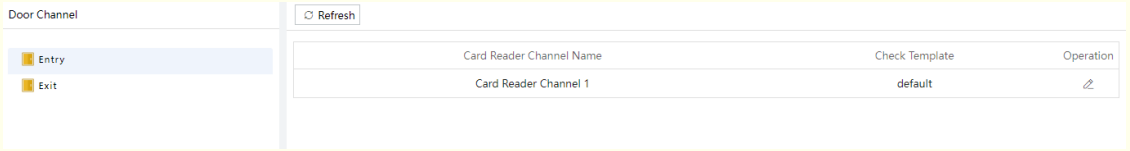
7.4 Door Verification Configuration

7.4.1 Door Verification Configuration

Configure the verification information for the card reader bound to the speed gate.

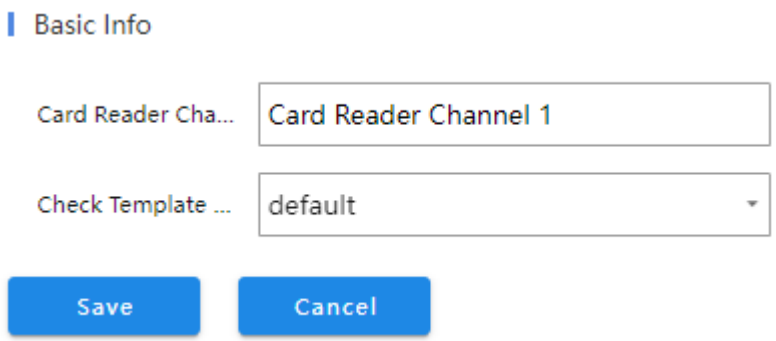
Go to **Setup > Access Control > Door Verification Config**.

Note: The card reader must be physically connected to the speed gate's Wiegand interface/RS485 interface.



If a card reader is installed on the entry direction of the speed gate, the corresponding parameters need to be configured; the same applies to the exit direction. The following takes the entry direction as an example.

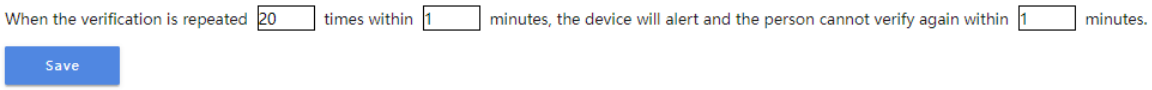
1. Click the corresponding .



2. Set the card reader channel name and direction, and select a verification template (set in device parameter configuration).
3. Click **Save**.

7.4.2 Repeated Authentication Lock

Go to **Setup > Access Control > Repeated Authentication Lock**.



Complete the settings as needed, and then click **Save**.

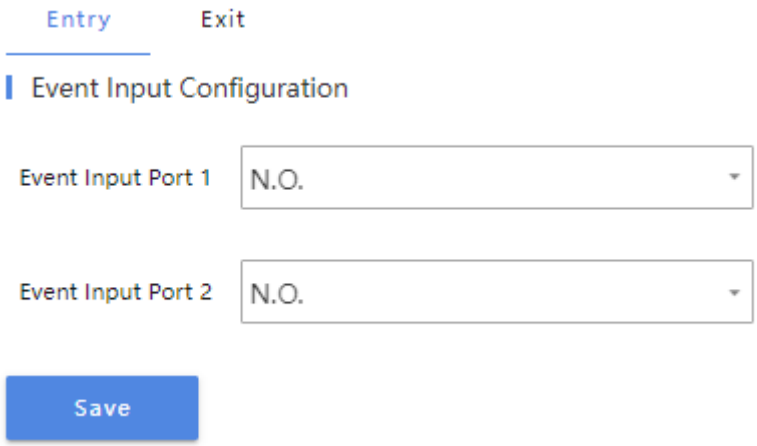
7.5 Event Input Configuration

After connecting the alarm detector to the speed gate, you can configure the event input interface status according to the detector's operating mode.

- N.O.: In the default state, the circuit between the alarm detector and the speed gate is open, and no signal is transmitted to the speed gate. The signal will be transmitted only when an alarm event is detected.
- N.C.: In the default state, the circuit between the alarm detector and the speed gate is closed, and the signal will continuously be transmitted to the speed gate. When an alarm event is detected, the signal transmission will be cut off.

Go to **Setup > Access Control > Event Input Configuration**. Configure the status of each interface in sequence, and then click **Save**.

If an alarm detector is installed at the entry direction of the speed gate, the corresponding parameters need to be configured; the same applies to the exit direction.



7.6 External Device Configuration

See **Common > External Device Configuration**.

8 Advanced Settings

8.1 Normally Open/Closed

The barrier of the speed gate can be remotely controlled to maintain a Normally Open (N.O.) or Normally Closed (N.C.) state.

- N.O.: Control the barrier to remain in a normally open state. All people can pass through directly without verification or credentials.

  If a remote close signal is received during the effective period, the barrier will close, and it will remain closed until the next barrier-opening action, after which it will return to the normally open state.

  If a manual normally closed signal is received during the effective period, the barrier will remain closed.

- N.C.: Control the barrier to remain in a normally closed state. No one can pass through.

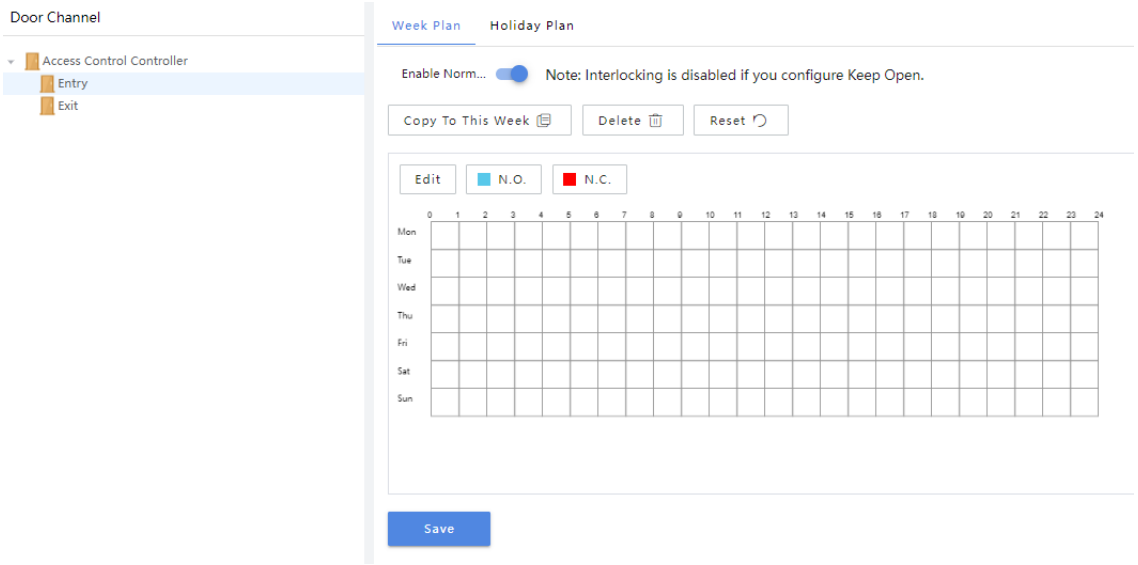
  If a remote open signal is received during the effective period, the barrier will open; and after closing, it will continue to remain in the normally closed state.

  If a manual normally open signal is received during the effective period, the barrier will remain open.

- Default: Enables N.O./N.C. without setting a weekly plan or holiday plan. The barrier will open or close according to the received signals.

Note: Setting a time period to N.O. will cause interlocking to be ineffective during this time period.

1. Go to **Setup > Advanced > Normally Open/Closed**.



2. In the left-side list, select the entry or exit direction to configure. The parameters are displayed on the right side.
3. Turn on **Enable Normally Open/Closed** under **Week Plan**. By default, it operates on a weekly cycle.
4. Set the effective period. Two methods are supported:

   - Filling color: Each grid represents 1 hour. means Normally Open/Closed is disabled for the corresponding time period; means Normally Open is enabled for the corresponding time period; ; means Normally Closed is enabled for the corresponding time period.

     The following describes how to set Normally Open. Setting Normally Closed is similar.

     (1) Click 常开 to enable Normally Open.

     (2) Click a grid or drag. If it turns blue, it means the corresponding period is set to Normally Open.

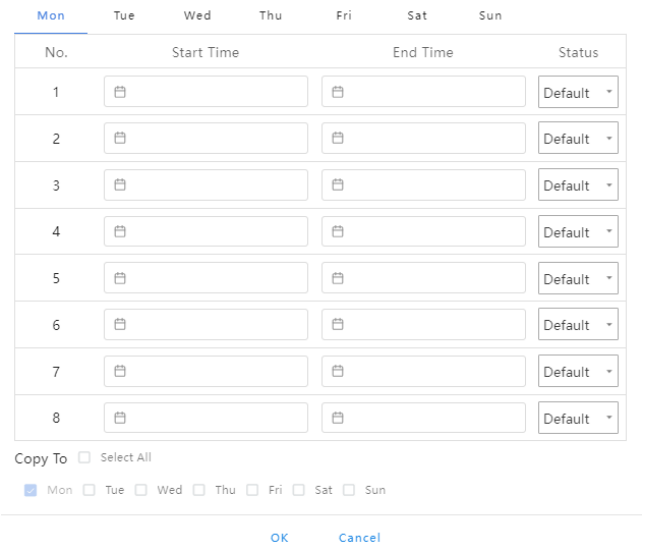
     Click a grid, then click **Copy to This Week**. This will set the same period of every day of the week to Normally Open.

Click **Delete**, then click a grid or drag. If it turns white, it means the corresponding period is set to neither N.O. nor N.C..

Click **Reset** to disable Normally Open/Normally Closed for the entire week.

- Edit time periods: You can set up to 8 time periods per day, and the time periods must not overlap.

  (1) Click **Edit**. A window as shown below appears.

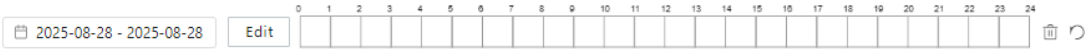


  (2) Set the start and end times for each period of the day.

  (3) Repeat the previous step to set time periods for the remaining days of the week. If the settings are the same, you can select the desired days of the week and click **Copy**.

5. Switch to the **Holiday Plan** tab to set exceptions. You can set different N.O. or N.C. plans for specific dates.

   (1) Click **Add** to add a holiday.



   (2) Set N.O. or N.C. time periods in the same way you set for the weekly plan. The delete/reset options are described as follows:

   - Reset all holiday plans: Click **Reset** at the top.
   - Delete/reset a specific holiday plan: Scroll to the right of the plan and click the corresponding / .

6. Repeat the above steps to complete the settings for the remaining channels. If the settings are the same, select the corresponding channels and click **Copy**.
7. Click **Save**.

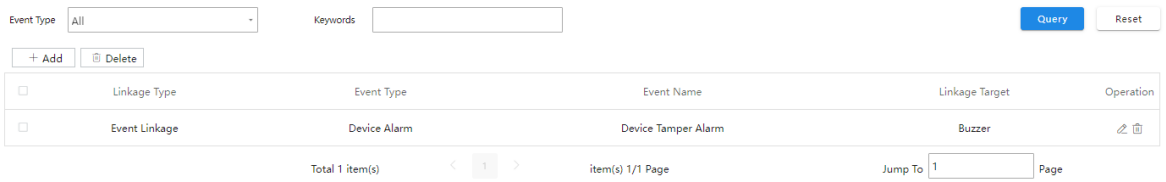
9 Alarm Configuration

The alarm linkage actions supported may vary with device model.

9.1 Linkage Configuration

Configure actions that will be triggered after an alarm occurs. For example, when an alarm is triggered, it can activate the speed gate to sound a buzzer or open the gate.

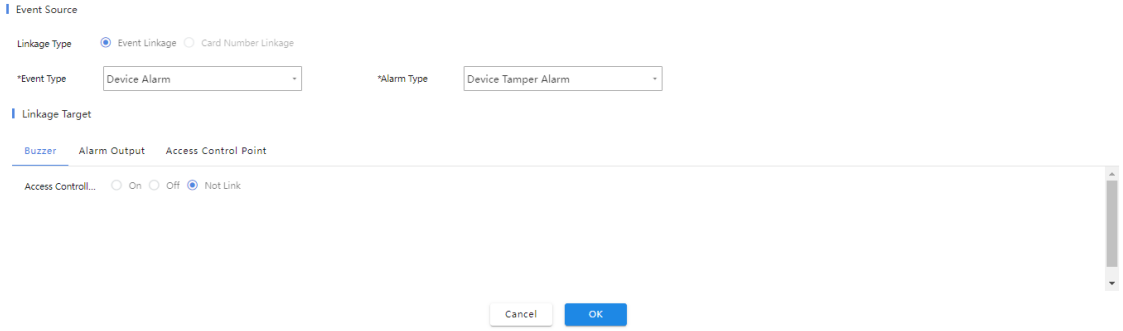
Go to **Setup > Alarm > Linkage Configuration**.



Add

A maximum of 30 linkage configurations can be added.

1. Click **Add** to enter the configuration page. The **Event Linkage** type is currently supported.

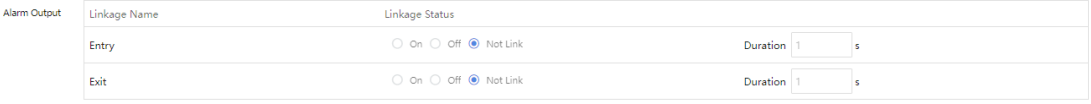


2. Select the event type and the corresponding alarm type.

Event Type	Alarm Type	Description
Device alarm	Alarm triggered by the speed gate itself.	
	Device tamper alarm	The speed gate has been tampered with.
	Device tamper alarm cleared	The device tamper alarm has stopped
Case input alarm	An alarm was triggered by an external device connected to the speed gate, causing the speed gate to trigger this alarm After selecting this type, you also need to select the port for the physical connection to the speed gate. To configure multiple alarm linkages, you need to add them one by one.	
	Event input alarm	The external device triggered an alarm
	Event input alarm cleared	The external device stops the alarm
Door Alarm	Alarm triggered by the door connected to the speed gate. After selecting this type, you also need to select the direction (entry or exit). To configure alarm linkages for both entry and exit directions, you need to add them one by one.	
	Authentication over limit alarm	Alarm triggered after the set number of failed authentication attempts is reached.
Card reader alarm	Alarm triggered by the card reader connected to the speed gate.	
	Duress alarm	In case of duress, the duress code can be entered to open the door, and meanwhile, the device will report a duress event to the platform.
	Unauthorized list alarm	The card swipe information is not in the authorized list (the list is configured in the UMS).

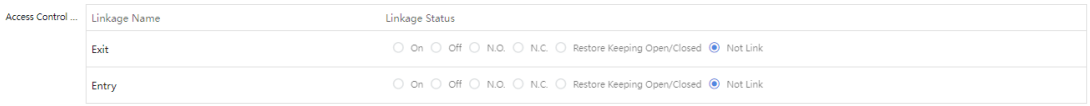
3. Set linkage targets. On: Trigger linkage when an event occurs. Off: Trigger to stop the linkage after an event occurs. Not Link: Default setting, not controlled by event linkage.

   - Buzzer: Can trigger the speed gate itself to emit a buzzer sound. The default duration is 30 seconds (unconfigurable)
   - Alarm output: If an output device like alarm lamp is connected, you can set alarm output linkage.



   When **Linkage Status** is set to **On**, you must set the alarm output duration.

   - Doors: Trigger actions like opening/closing the gate, keeping the gate open/closed, cancelling keeping the gate open/closed



4. Click **Save**.

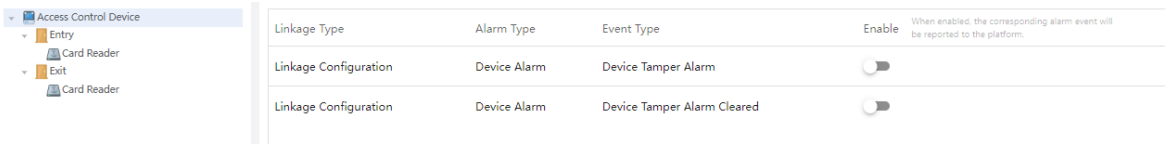
9.2 Alarm Function Configuration

You can enable/disable the reporting of each linkage to the UNV Guard platform/UNV-Link app individually.

Note: Prerequisites:

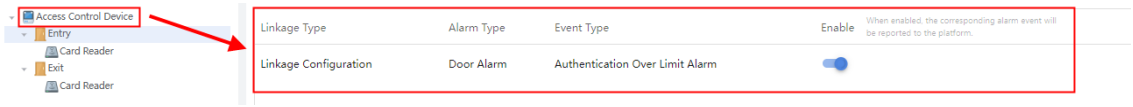
- Reporting to the UNV Guard platform: Please subscribe to the device on the UNV Guard platform first.
- Reporting to the UNV-Link app: Please bind the device on the app first.

Go to **Setup > Alarm > Alarm Function Configuration**.

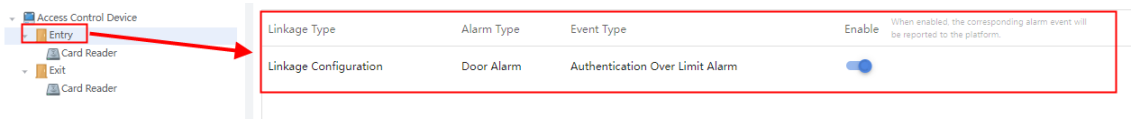


Click to enable reporting. Click to disable reporting.

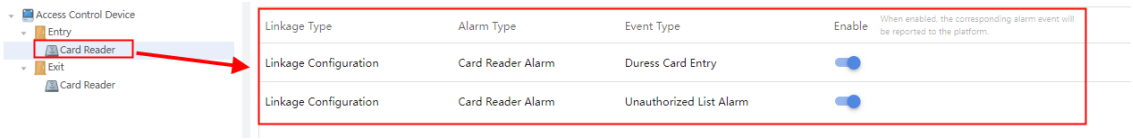
- Click **Access Control Device** in the left-side list to display linkage information of the device alarm type.



- Click the door channel name to display linkage information of the door alarm type.

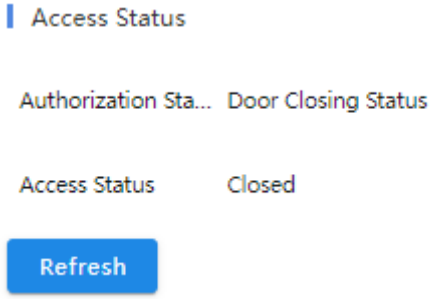


- Click a card reader under the door channel to display linkage information of the card reader alarm type.



10 Device Status

Access Status

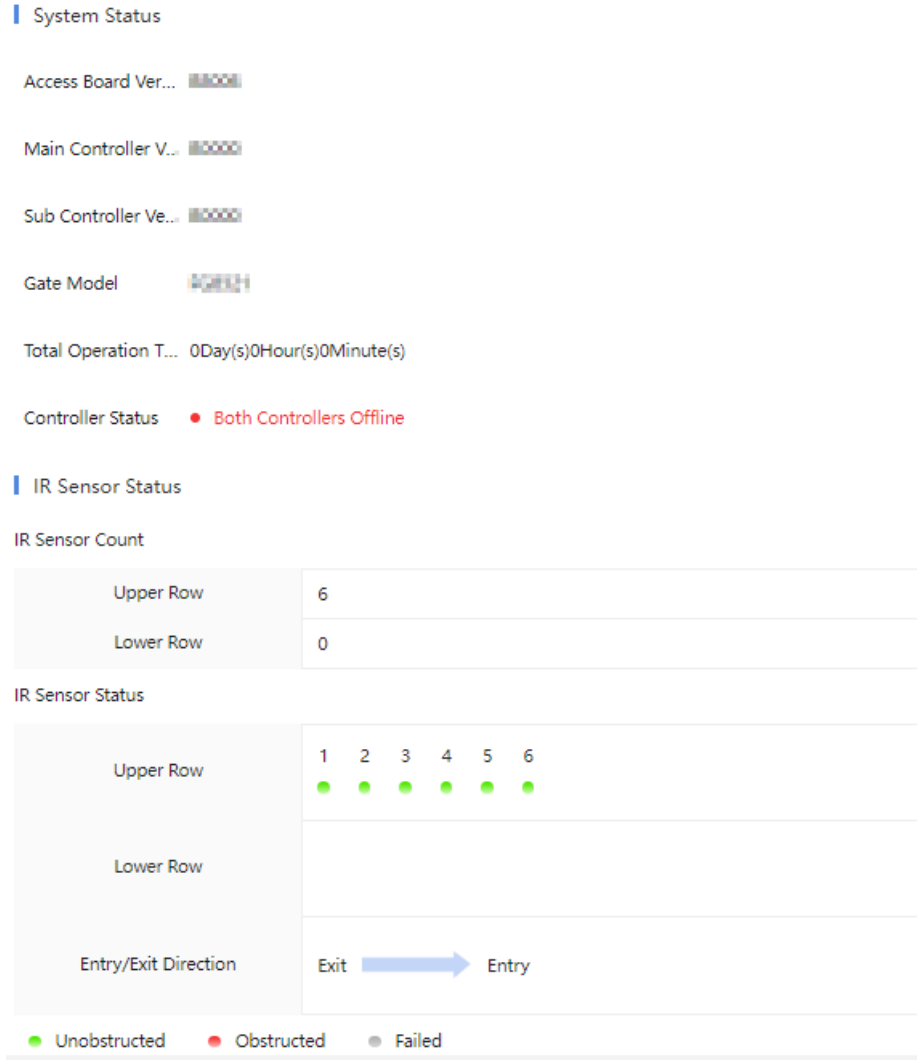


Click **Refresh** to update the status.

Parameter	Description
Authorization Status	Commands sent by the speed gate, including: • Door Closing Status: Close the gate

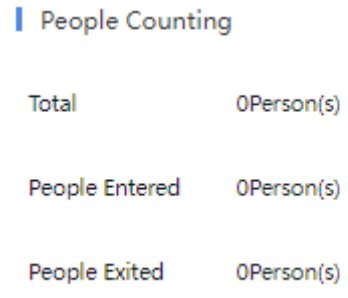
Parameter	Description
	• Protection Action: Keep the gate open. If the person remains in the lane beyond the configured entry/exit timeout period, causing the gate to close, the speed gate will send the command to stop gate closing to prevent the person from being trapped. • Entry Open: Open the gate for entry. • Exit Open: Open the gate for exit.
Access Status	Gate barrier status, including Closed, Opening, Closing, Entry Open, Exit Open.

System Status



Display the version information of the main circuit boards, the status of the controller, and the status of the IR sensors.

People Counting



View the total number of people who have passed through the speed gate since power-up, including the total number of people entering and the total number of people exiting.