

# Access Controller

## User Manual

V1.01

# Contents

About This Manual.....	1
1 Defaults.....	2
2 Login.....	2
3 Common.....	3
3.1 Basic Info.....	3
3.2 Network Basic Config.....	4
3.2.1 Ethernet.....	4
3.2.2 Port.....	5
3.2.3 Port Mapping.....	6
3.3 External Device.....	6
3.3.1 485 Serial Port Configuration.....	6
3.3.2 Wiegand Interface.....	8
3.3.3 QR Code.....	10
3.4 Server.....	10
4 Security.....	10
4.1 Network Security.....	10
4.1.1 HTTPS.....	10
4.1.2 Authentication.....	11
4.1.3 ARP Protection.....	12
4.1.4 IP Address Filtering.....	12
4.1.5 Access Policy.....	13
4.2 Registration Info.....	13
5 System.....	14
5.1 Time.....	14
5.1.1 Time.....	14
5.1.2 DST.....	15
5.2 User.....	15
5.3 Maintenance.....	16
6 Network.....	17
6.1 Basic.....	17
6.2 Advanced Setting.....	17
6.2.1 DNS.....	17
6.2.2 DDNS.....	18
6.3 EZCloud.....	18
7 Access Control.....	19
7.1 Device Parameter Config.....	19
7.2 Door Parameter Config.....	20
7.3 Check Template.....	21
7.4 Door Verification Config.....	22

7.5 Event Input Configuration.....	24
7.6 External Device.....	24
<b>8 Advanced.....</b>	<b>25</b>
8.1 Normally Open/Closed.....	25
8.2 Multi-Door Interlocking.....	26
<b>9 Alarm.....</b>	<b>27</b>
9.1 Linkage Configuration.....	27
9.2 Alarm Function Configuration.....	29

# About This Manual

---

This manual describes the features and operations of access controller, including single-door, two-door, and four-door access controllers.

## Copyright Statement

©2024-2025 Zhejiang Uniview Technologies Co., Ltd. All rights reserved.

No part of this manual may be copied, reproduced, translated or distributed in any form or by any means without prior consent in writing from Zhejiang Uniview Technologies Co., Ltd (hereinafter referred to as Uniview or us).

The product described in this manual may contain proprietary software owned by Uniview and its possible licensors. Unless permitted by Uniview and its licensors, no one is allowed to copy, distribute, modify, abstract, decompile, disassemble, decrypt, reverse engineer, rent, transfer, or sublicense the software in any form by any means.

## Disclaimer




Due to such reasons as product version upgrade or regulatory requirement of relevant regions, this manual will be periodically updated.

This manual is only for informational purpose, and all statements, information, and recommendations in this manual are presented without warranty.

The illustrations in this manual are for reference only and may vary depending on the version or model. The screenshots in this manual may have been customized to meet specific requirements and user preferences. As a result, some of the examples and functions featured may differ from those displayed on your monitor.

## Safety Symbols

The symbols in the following table may be found in this manual. Carefully follow the instructions indicated by the symbols to avoid hazardous situations and use the product properly.

Symbol	Description
	NOTE! Indicates useful or supplemental information about the use of product.
	CAUTION! Indicates a situation which, if not avoided, could result in damage, data loss or malfunction to product.
	WARNING! Indicates a hazardous situation which, if not avoided, could result in bodily injury or death.

# 1 Defaults

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

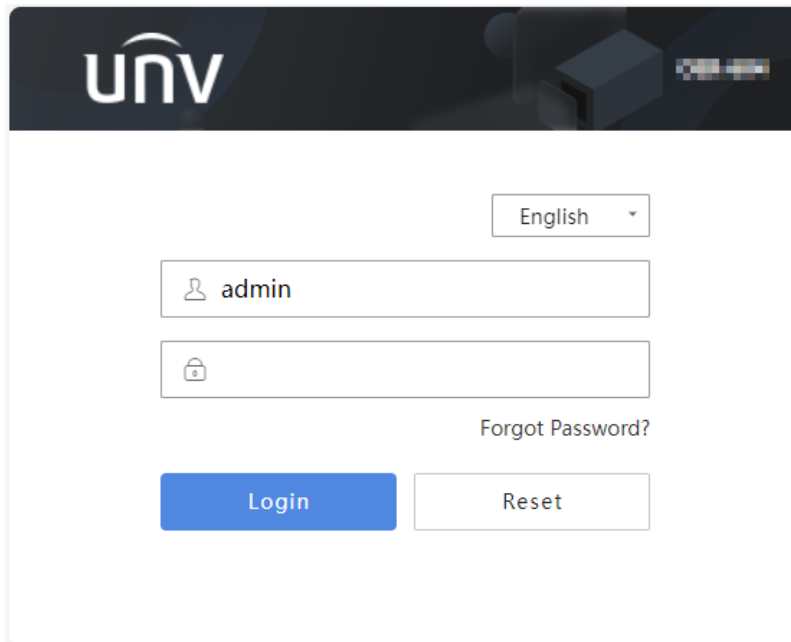
## 2 Login

### 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) Please 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, make sure the device has an email address registered, otherwise contact the local technical support to reset the password.

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

## Retrieve Password

Please scan the QR code to obtain the security code (for admin only):

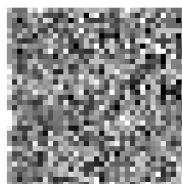
- Scan with WeChat

• %s:

Path 1: Me > Tool > Forget Device Password

Path 2: Scan (in the added devices)

- %s: Me > General > Forget Device Password



We will send the security code to: Email not set

Security Code

Cancel Next

2. Obtain a security code according to the on-screen instructions.
3. Enter the security code, and click **Next** to retrieve the password. Please note this new password.







## Logout

Click ... in the upper-right corner of the interface, choose **Logout**, and click **OK** to log out from the current user.

## Customer Service

Click ... in the upper-right corner of the interface, choose **Customer Service**, and you may view the customer service hotline, official account QR code, and technical support information.

Customer Service ×

 Customer Service Hot Line  400-655-2828	 Official Account(QQ)   4006552828	 UNV Dealer Official Account   WeChat	 Technical Support  Tel: 0571-26896060(workday) service@uniview.com
--	---	--	---

# 3 Common

Configure commonly used functions.

## 3.1 Basic Info

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

Go to **Common > Basic Info**.

Basic Info

Model

Product Config

Firmware Version

Hardware Version

Boot Version

Serial No.

Network

MAC Address

Factory time

Status

System Time

Operation Time

Refresh

Common Configuration

Ethernet

Time

User

Common Configuration: Click the icon or text to quickly access the common functions, including [Ethernet](#), [Time](#), and [User](#).

## 3.2 Network Basic Config

### 3.2.1 Ethernet

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

Obtain IP Address

Static

IPv4

IP Address

Subnet Mask

Default Gateway

IPv6

IPv6 Mode

1

IPv6 Address

Prefix Length

64

Default Gateway

MTU

1500

Port Type

FE Port

Operating Mode

Auto-negotiation

Save

- Configure Ethernet parameters.

Parameter		Description
IPv4	Obtain IP Address	<ul style="list-style-type: none"> <li>Static: Configure a static public network IP address for the device manually. Set <b>Obtain IP Address</b> to <b>Static</b>, and enter the IP address, subnet mask, and default gateway.</li> <li>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.</li> <li>PPPoE: Configure PPPoE (Point to Point Protocol over Ethernet) to assign the device a dynamic IP address to establish network connection. Set <b>Obtain IP Address</b> to <b>PPPoE</b>, and enter the username and password.</li> </ul>
IPv6	Mode	<p>IPv6 has a lot more IP addresses than IPv4, and is faster and safer than IPv4 in terms of data transfer.</p> <p>The IPv6 mode includes <b>DHCP</b> and <b>Manual</b>. The default mode is <b>DHCP</b>.</p>
Parameter	MTU	<p>Maximum transmission unit, the maximum packet size supported by the device in bytes.</p> <p>Range: [576-1500], integer only. Default: 1500.</p> <p>The greater the value, the higher the communication efficiency, the higher the transmission delay.</p>
	Operating Mode	<ul style="list-style-type: none"> <li>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.</li> <li>Rate + Full Duplex: At the set rate, the port can receive and send data at a given time, eliminating the physical transmission distance limitation of half duplex.</li> <li>(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.</li> </ul>

3. Click **Save**.

### 3.2.2 Port

Set the port to access the device via network.

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

HTTP Port	<input type="text" value="80"/>
HTTPS Port	<input type="text" value="443"/>
RTSP Port	<input type="text" value="554"/>

Note: Modifying the RTSP port number will cause the device to restart.

**Save**

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, a message "**Port conflicts. Please try again.**" will appear. 23, 81, 82, 85, 3260, and 49152 have been assigned for other purposes and cannot be used. In addition to the above port numbers, the system can also dynamically detect other port numbers that are already in use.

- HTTP/HTTPS Port: If you change the HTTP/HTTPS port number, then 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: Real-Time Streaming Protocol port. Enter an available port number.

3. Click **Save**.

## 3.2.3 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**.

Port Mapping ☐

Mapping Type Automatic

Port Type	External Port	External IP Address	Status
HTTP Port	80	0.0.0.0	Inactive
RTSP Port	81	0.0.0.0	Inactive
Server Port	554	0.0.0.0	Inactive
HTTPS Port	443	0.0.0.0	Inactive

**Save**

2. Enable **Port Mapping**.

3. Set the mapping type, including **Automatic** and **Manual**. It is **Automatic** by default.

- 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

### 3.3.1 485 Serial Port Configuration

The RS485 interface can be used to connect external card readers for authentication.

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

You can click the title to show or hide the tab.

Click **Save** after the following parameters are configured.

## RS485\_1, RS485\_2

### RS485\_1

Baud Rate	115200
Data Bits	8
Stop Bits	1
Parity	None
Flow Control	None

### RS485\_2

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 Config

Set the parameters of the external card reader connected to the access controller through the RS485 serial interface.

External Device

<input type="checkbox"/> RS485 Address	External Device Name	Serial Port ID	Port Mode	Format	Tamper Detection	Operation
<input type="checkbox"/> 8	485CardReader1	-	Disabled	Ascending Order	Disable	
<input type="checkbox"/> 9	485CardReader2	-	Disabled	Ascending Order	Disable	
<input type="checkbox"/> 10	485CardReader3	-	Disabled	Ascending Order	Disable	
<input type="checkbox"/> 11	485CardReader4	-	Disabled	Ascending Order	Disable	
<input type="checkbox"/> 12	485CardReader5	-	Disabled	Ascending Order	Disable	
<input type="checkbox"/> 13	485CardReader6	-	Disabled	Ascending Order	Disable	
<input type="checkbox"/> 14	485CardReader7	-	Disabled	Ascending Order	Disable	
<input type="checkbox"/> 15	485CardReader8	-	Disabled	Ascending Order	Disable	

Save

- Select the card reader you want to edit, and click to change the card reader parameters.

**Edit**

Card Reader Name

Port Mode

Format

Tamper Detection ☐

Copy To ☐ Select All

☐ 485CardReader1 ☐ 485CardReader2 ☐ 485CardReader4

☐ 485CardReader5 ☐ 485CardReader6 ☐ 485CardReader7

☐ 485CardReader8

- Select multiple card readers, click **External Device**, and change the following parameters of the selected card readers as needed.

**Edit(1,2)**

Port Mode

Format

Tamper Detection ☐

Parameter	Description
Card Reader Name	It can be customized and must be unique.
Port Mode	<ul style="list-style-type: none"> <li>• Disable: Disable the RS485 address.</li> <li>• IC Card Reader: Bind the device to the IC card reader.</li> <li>• QR Code Card Reader: Bind the device to the QR code card reader.</li> </ul>
Serial Port ID	It is a required item and must be unique when the port mode is set to <b>QR Code Card Reader</b> .
Format	<ul style="list-style-type: none"> <li>• Ascending Order: Show the same sequence of the card number as the number read by the card reader.</li> <li>• Descending Order: Show the opposite sequence of the card number as the number read by the card reader.</li> </ul>
Tamper Detection	When enabled, an alarm will be triggered if the card reader is detected to be disassembled.
Copy	To apply the current settings to other card readers, select the desired card reader and then click <b>Copy</b> .

### 3.3.2 Wiegand Interface

The Wiegand interface can be used to connect external card readers for authentication.

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

Wiegand Interface						
<input type="checkbox"/>	Wiegand Port	Card Reader Name	Protocol	Format	Tamper Detection	Operation
<input type="checkbox"/>	0	WiegandReader1	Wiegand 34	Ascending Order	Disable	
<input type="checkbox"/>	1	WiegandReader2	Wiegand 34	Ascending Order	Disable	
<input type="checkbox"/>	2	WiegandReader3	Wiegand 34	Ascending Order	Disable	
<input type="checkbox"/>	3	WiegandReader4	Wiegand 34	Ascending Order	Disable	
<input type="checkbox"/>	4	WiegandReader5	Wiegand 34	Ascending Order	Disable	
<input type="checkbox"/>	5	WiegandReader6	Wiegand 34	Ascending Order	Disable	
<input type="checkbox"/>	6	WiegandReader7	Wiegand 34	Ascending Order	Disable	
<input type="checkbox"/>	7	WiegandReader8	Wiegand 34	Ascending Order	Disable	

- Select the card reader you want to edit, and click to change the card reader parameters.

Edit

Card Reader Name

WiegandReader2

Protocol

Wiegand 34

Format

Ascending Order

Tamper Detection

☐

Copy To

☐ Select All

☐ WiegandReader1

☐ WiegandReader3

☐ WiegandReader4

☐ WiegandReader5

☐ WiegandReader6

☐ WiegandReader7

☐ WiegandReader8

Cancel

OK

- Select multiple card readers, click **Wiegand Interface**, and change the following parameters of the selected card readers as needed.

Edit(2,3)

Protocol

Wiegand 34

Format

Ascending Order

Tamper Detection

☐

Cancel

OK

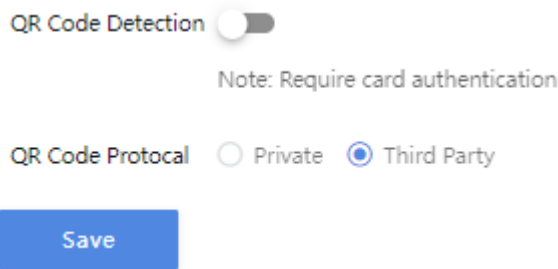
Parameter	Description
Card Reader Name	It can be customized and must be unique.
Protocol	<ul style="list-style-type: none"> <li>• Wiegand 26: Read 3-byte card numbers via the Wiegand 26 protocol.</li> <li>• Wiegand 34: Read 4-byte card numbers via the Wiegand 34 protocol.</li> <li>• Custom Wiegand: You can customize the Wiegand protocol.</li> </ul>
Format	<ul style="list-style-type: none"> <li>• Ascending Order: Show the same sequence of the card number as the number read by the card reader.</li> <li>• Descending Order: Show the opposite sequence of the card number as the number read by the card reader.</li> </ul>

Parameter	Description
Tamper Detection	When enabled, an alarm will be triggered if the card reader is detected to be disassembled.
Copy	To apply the current settings to other card readers, select the desired card reader and then click <b>Copy</b> .


### 3.3.3 QR Code

When the authentication mode is set to **Card**, you can open the door using the QR code generated by the card number.

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



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

 **Note:** It is required to set the authentication mode to **Card** in [Check Template](#) and bind the template in [Door Verification Config](#).

3. Click **Save**.

## 3.4 Server

You can view the server that connected to the access controller.

Go to **Common > Server**, and the server page shows the server address, port number, type, etc.

Subscription List

No.	Subscription ID	Server IP	Port No.	Type	Remaining Time(s)
1	0	172.20.88.128	0	Alarm Subscription	3079

## 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**.

HTTPS



SSL Certificate

Browse...

Upload

Note: Include RSA public and private keys in one pem file and import.

Steps:

1. Open the key file and cert file.
2. Create a blank file.
3. Copy contents of the key file to the blank file.
4. Copy contents of the cert file below contents of the key file in the blank file.
5. Save the blank file as ssl\_cert.pem.

Example:

```
-----BEGIN RSA PRIVATE KEY-----  
MIIE...  
-----END RSA PRIVATE KEY-----  
-----BEGIN CERTIFICATE-----  
MIID...  
-----END CERTIFICATE-----
```

Save

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**.

RTSP Authentica... Digest

HTTP Authentica... Digest

**Save**

2. Choose an authentication mode.

Parameter	Description
RTSP Authentication	Choose an authentication mode, including <b>None</b> , <b>Basic</b> , and <b>Digest</b> . <ul style="list-style-type: none"> <li>• None: Transmits data without authentication.</li> <li>• Basic: Authentication information is transferred in plaintext without encryption, which imposes serious security risks.</li> <li>• Digest: Authentication information is encrypted to provide higher security.</li> </ul>
HTTP Authentication	Choose an authentication mode, including <b>None</b> and <b>Digest</b> .

3. Click **Save**.

### 4.1.3 ARP Protection

ARP attack mainly exists in local area network, 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**.

**ARP**

ARP Protection ☐

Gateway

Gateway MAC Ad...

**Save**

2. Enable **ARP Protection**.
3. Enter the gateway and gateway's 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**.

#### IP Address Filtering

IP Address Filtering ☐

Filtering Mode ☒ Whitelist ☐ Deny Access

No.	IP Address	+

Save

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 **+**, and 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**.

#### Access Policy

MAC Authenticati... ☒

Save

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

### 4.2 Registration Info

You can set to hide vendor information of the access controller from the server.

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

Hide Vendor Info ☐

Save

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**.

Sync Mode

Time Zone

System Time

Save

2. You can set the device time manually or sync it with a server.

- Set manually in the **Set 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) Select the sync mode.

Parameter	Description
Sync with System Configuration	The device uses the time provided by the system's built-in time module.
Sync with Management Server(ONVIF)	The device regularly syncs time with the management server connected via Onvif.
Sync with Latest Server Time	Default sync mode. The device regularly syncs time with all the connected servers.
Sync with NTP Server	<p>NTP Server: A server used to sync time with the distributed server and client via the NTP protocol.</p> <p>To sync the server time, you need to configure the following parameters.</p> <ul style="list-style-type: none"><li>• NTP Server Address: Enter the NTP server address and click <b>Test</b> to check the network communication. A message will appear if the NTP is verified successfully.</li><li>• Port: Range: [1-65535], integer only, default: 123.</li><li>• Update Interval (s): Range: [30-86400], integer only, default: 600.</li></ul>

- (2) Set the time zone as needed.


- (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**.

### DST

DST



Save

2. Enable **DST**.

### DST

DST



Start Time

Apr

First

Sun

02:00

End Time

Oct

Last

Sun

02:00

DST Bias

60mins


Save

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 access controller has an admin user only, which can be edited only.


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

No.	Username	User Type	Operation
1	admin	Admin	

< 1 >

1

Total 1 item(s) 1/1 Page

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

Edit



Username

admin

User Type

Admin

Old Pass...

Password

Weak

Medium

Strong

Confirm

OK Cancel

## 5.3 Maintenance

System maintenance includes software upgrade, system configuration, diagnosis information, and device restart.



### Note:

- The device will be restarted if you perform operations such as software upgrade, device restart, restoring default settings, importing configurations, and importing person library.
- Restarting the device will interrupt the ongoing services. Please handle with caution.

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

### Software Upgrade

Local upgrade and cloud upgrade are available.



### 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.

#### Software Upgrade

Local Upgrade ☐ Upgrade Boot Program

Cloud 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.
  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.

### Configuration Management

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

#### Config Management

Default ☐ Restore all settings to defaults without keeping current network,user settings,face library and record data.

Importing


Exporting

Storage Medium

- Default: Clicking **Default** will restore the current network, user settings, face library, and record data to the defaults, and then the device will automatically restart.

To restore all settings to factory defaults, select **Restore all settings to defaults without keeping current network, user settings, face library and record data**.

- 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 personnel and record data, or click **Record Clear** to clear the record data only.

## Diagnosis Info

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


### | Diagnosis Info

Export Diagnosis ...

Export

## Device Restart

You can choose to restart the device manually or automatically.

 **Note:** Restarting the device will interrupt the ongoing services.

### | Device Restart

Restart device

Restart

Enable Auto Restart



- Restart manually: Click **Restart**, and then confirm to restart the device.
- Restart automatically:
  1. Enable **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

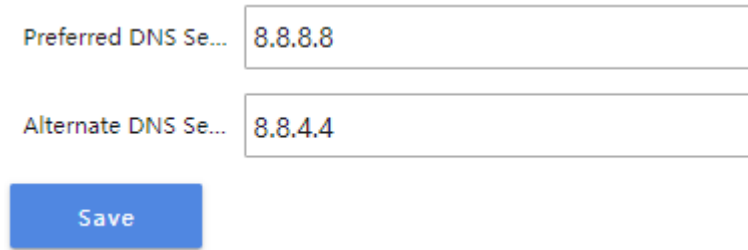
See [Ethernet](#) for details.

## 6.2 Advanced Setting

### 6.2.1 DNS

The DNS server can automatically translate the domain name address into an IP address so as to access the access controller.

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



Preferred DNS Se... 8.8.8.8

Alternate DNS Se... 8.8.4.4

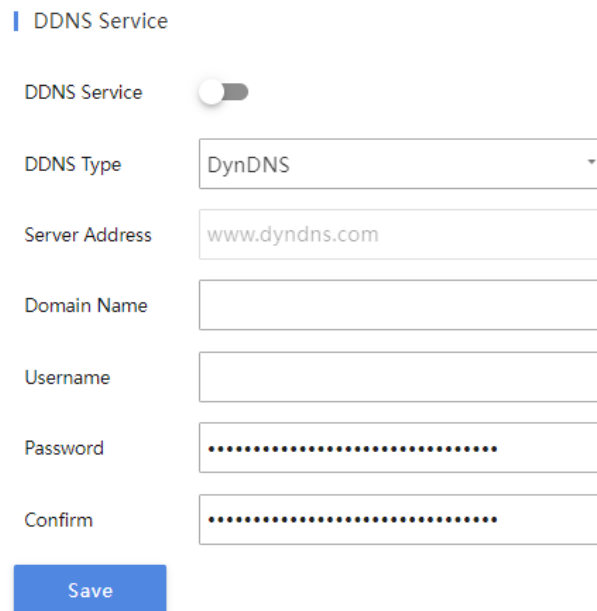
Save

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

## 6.2.2 DDNS

DDNS (Dynamic Domain Name Server) can map the dynamic IP address of the device to a fixed domain name, which is designed to help other devices on the public network access the network with the fixed domain name. With DDNS, users can access the private network device for remote control with the public IP address.

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



DDNS Service

DDNS Type DynDNS

Server Address www.dyndns.com

Domain Name

Username

Password

Confirm

Save


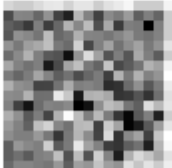
2. Enable **DDNS Service**.
3. Select the DDNS type.
  - DynDNS/No-IP: Enter the domain name, username, and password, and confirm the password.
    - Domain name: Domain name assigned by your DDNS service provider, for example, www.dyndns.com.
    - Username and password: The corresponding username/password for your DDNS account, for example, www.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**.

EZCloud	<input checked="" type="checkbox"/>
No registration	<input checked="" type="checkbox"/>
Address	<a href="http://ezcloud.uniview.com">ezcloud.uniview.com</a>
Register Code	
Device Status	Offline
Scan	
<input type="button" value="Save"/>	

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

 **Note:** The number of channels, Wiegand card readers, and RS485 card readers displayed on the interface may vary with device model. The following takes the four-door access controller as an example.

### 7.1 Device Parameter Config

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

#### Record Upload Settings

Reporting Type	<input type="text" value="Upload All"/>
Storage Mode	<input type="radio"/> Stop Recording <input checked="" type="radio"/> Overwrite Recording
Card Type	<input checked="" type="checkbox"/> General IC Card <input type="checkbox"/> MIFARE Card
<input type="button" value="Save"/>	

2. Select a reporting type.
  - Upload All: The device reports all authentication records including success and failure to the [Server](#).
  - Upload Success Record: The device only reports authentication success records to the [Server](#).

3. Select a storage mode.
  - Stop Recording: When the local recording capacity is full, recording stops automatically.
  - Overwrite Recording: When the local recording capacity is full, the oldest recordings are overwritten automatically.
4. Select a card type. The two cards cannot be selected simultaneously.
  - General IC Card: The device can read general IC cards.
  - MIFARE Card: Inductive smart IC card.
5. Click **Save**.

## 7.2 Door Parameter Config

Configure door opening and closing parameters, as well as the door-connected lock, door magnet, and button.

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

2. Configure door parameters for the door 1.

Parameter	Description
Door Name	You can set the door name as needed. The names of doors bound to the same access controller must be unique.
Door Opening Duration	Duration of single door opening. If the duration exceeds the set time, the door will lock automatically.
Exit Button Type	Keep the <b>N.O.</b> setting.
Door Opening Timeout	If the door remains open longer than the set time, an alarm will be triggered. 0 means no alarm.
Auto Door Lock Upon Closing	Even if the door lock action time is not reached, the door will still lock immediately upon closing.
Door Magnet Type	Keep the <b>N.C.</b> setting.

Parameter	Description
Authentication Over Limit	If the number of consecutive failed card swipe attempts reaches the set value, an alarm will be triggered.  0 means no alarm. If <a href="#">Linkage Configuration</a> is set, the corresponding alarm will be triggered.
Super Password	Entering the password will unlock the door, regardless of the verification method. Do not disclose the password.
Duress Code	In case of duress, you can input the code to unlock the door, and meanwhile, the device will report a duress event to the platform.



**Note:** The super password, duress code, and person password cannot be the same.

- Repeat the previous step to configure the parameters for other doors respectively. You can copy the door 1 parameters to other doors.
- Click **Save**.

## 7.3 Check Template

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

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

The screenshot shows the 'Check Template' configuration page. On the left, a sidebar lists templates, with 'default' selected. The main panel shows a table for configuring time intervals and authentication methods. The first interval is set to '00:00:00 - 23:59:59' with 'Card, Password' authentication. The other seven intervals are set to 'Please select'. Below the table, there are checkboxes for 'Copy To' for each day of the week (Mon, Tue, Wed, Thu, Fri, Sat, Sun) and a 'Copy' button. A 'Save' button is at the bottom left.

### Add

- Click +, an empty template appears on the right.

\*Template Name

The content cannot be empty.

Mon Tue Wed Thu Fri Sat Sun

Time Interval1	<input type="text" value="00:00:00 - 23:59:59"/>	<input type="text"/>
Time Interval2	<input type="text" value="Please select"/>	<input type="text"/>
Time Interval3	<input type="text" value="Please select"/>	<input type="text"/>
Time Interval4	<input type="text" value="Please select"/>	<input type="text"/>
Time Interval5	<input type="text" value="Please select"/>	<input type="text"/>
Time Interval6	<input type="text" value="Please select"/>	<input type="text"/>
Time Interval7	<input type="text" value="Please select"/>	<input type="text"/>
Time Interval8	<input type="text" value="Please select"/>	<input type="text"/>

Copy To ☐ Select All


☒ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat ☐ Sun

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 on the left you want to edit, change the template information, and click **Save**.

### Delete

Click the template on the left you want to delete, click , and confirm the deletion.





## 7.4 Door Verification Config

Configure the verification card reader bound to the door.

By default, each door has been assigned two card reader channels, including an entry channel and an exit channel.

Go to **Setup > Access Control > Door Verification Config**. Configure the door verification parameters for the four doors respectively.

Door Channel	+ Add	Delete	Refresh
Access Control Controller 01			
DoorChannel1			
DoorChannel2			
DoorChannel3			
DoorChannel4			

<input type="checkbox"/>	Card Reader Channel Name	Direction	Check Template	Card Reader	Operation
<input type="checkbox"/>	ReaderChannel1	Enter	default	WiegandReader1,485CardReader1	 
<input type="checkbox"/>	ReaderChannel2	Exit	default	WiegandReader2,485CardReader2	 

### Add

The card reader should be physically connected to the access controller's Wiegand interface/485 interface.

1. Click **Add**.

**Basic Info**

Card Reader Cha...

Direction ☒ Enter ☐ Exit

Check Template ...


**Card Reader binding**

<input type="checkbox"/>	Card Reader	Protocol	Port Mode	Format	Tamper Detection	Operation
<input type="checkbox"/>						

- Set the card reader channel name and direction, and select a check template (set in [Check Template](#)).
- Click **Bind**, choose the desired card reader interface, and click **OK**.

**Bind**

Card Reader bind...

- (Optional) Select the card reader you want to edit, and click  to edit the card reader name, protocol type, format, and enable/disable tamper detection.

**Edit**

Card Reader Name

Protocol

Format

Tamper Detection ☐

Copy To ☐ Select All

☐ WiegandReader2 ☐ WiegandReader3 ☐ WiegandReader4

☐ WiegandReader5 ☐ WiegandReader6 ☐ WiegandReader7


☐ WiegandReader8 ☐ 485CardReader1 ☐ 485CardReader2

☐ 485CardReader3 ☐ 485CardReader4 ☐ 485CardReader5


☐ 485CardReader6 ☐ 485CardReader7 ☐ 485CardReader8

- Click **Save**.

## Edit

Select the card reader you want to edit, and click  to edit the device information, change the card reader, or edit the card reader parameters.

## Delete


Select the card reader you want to delete, and click .

## 7.5 Event Input Configuration

After connecting the alarm detector to the access controller, 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 controller is open, and no signal is transmitted to the controller. The signal will only be transmitted when an alarm event is detected.
- N.C.: In the default state, the circuit between the alarm detector and the controller is closed, and the signal will continuously be transmitted to the controller. 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**.

 **Note:** The number of interfaces may vary depending on the model of the access controller. Please refer to the actual UI for configuration.

**Event Input Configuration**

Emergency Port

Event Input Port 1

Event Input Port 2

Event Input Port 3

Event Input Port 4

Event Input Port 5

Event Input Port 6

Event Input Port 7

Event Input Port 8

## 7.6 External Device

See [External Device](#) for details.

## 8 Advanced

### 8.1 Normally Open/Closed

The door lock can be remotely controlled through the access controller to maintain a Normally Open (N.O.) or Normally Closed (N.C.) state.

- N.O.: Control the door lock to remain in a normally open state.

If a remote close signal is received during the effective period, the door will close, and it will remain closed until the next door-opening action (verification/button press), after which it will return to the normally open state.


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

- N.C.: Control the door lock to remain in a normally closed state.

If a remote open signal is received during the effective period, the door 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 door lock will remain open.

- Default: Enables N.O./N.C. without setting a weekly plan or holiday plan. The door lock 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 channel 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  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.

No.	Start Time	End Time	Status
1	<input type="text"/>	<input type="text"/>	Default
2	<input type="text"/>	<input type="text"/>	Default
3	<input type="text"/>	<input type="text"/>	Default
4	<input type="text"/>	<input type="text"/>	Default
5	<input type="text"/>	<input type="text"/>	Default
6	<input type="text"/>	<input type="text"/>	Default
7	<input type="text"/>	<input type="text"/>	Default
8	<input type="text"/>	<input type="text"/>	Default

Copy To ☐ Select All

☒ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat ☐ Sun 02872w

(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.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
---	---	---	---	---	---	---	---	---	---	----	----	----	----	----	----	----	----	----	----	----

(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**.

## 8.2 Multi-Door Interlocking

Link the open/closed states of multiple doors.

When doors are interlocked, all doors within the interlocking combination remain closed. Verification can only be performed on one door at a time, and once the verification is successful, the door must be closed before verification can proceed on the other doors. If the door is not properly closed, the other doors will remain closed until the initially opened door is securely shut.

This feature is commonly used in areas requiring high security, such as bank vaults, data centers, and laboratories, to prevent unauthorized access.

### Note:

- Only dual-channel and four-channel access controllers support this feature.
- Interlocked doors cannot be set to normally open.
- Administrators using a super password are not subject to interlock restrictions and can open the door directly.

## Add

1. Go to **Setup > Advanced Setting > Multi-Door Interlocking**.

Interlocking Combination	DoorChannel1	DoorChannel2	DoorChannel3	DoorChannel4
6C:4B:90:B5:C0:31, z02872*	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

2. Click **Multi-Door Interlocking**.
3. Select the door channel numbers that you want to enable interlocking (at least two).

**Add**

Please select at least two access control points for interlocking.

☐ DoorChannel1

☐ DoorChannel2

☐ DoorChannel3

☐ DoorChannel4

**Cancel** **OK**

4. Click **Save**.

## Delete

Select the interlocking combinations to delete, and then click **Delete**.

# 9 Alarm

The alarm-triggered 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 access controller to sound a buzzer or unlock the door.

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

Linkage Type	Event Type	Event Name	Linkage Target	Operation
<input type="checkbox"/> Event Linkage	Device Alarm	Fire Alarm	Access Control Point	<a href="#">Edit</a> <a href="#">Delete</a>
<input type="checkbox"/> Event Linkage	Device Alarm	Fire Alarm Cleared	Access Control Point	<a href="#">Edit</a> <a href="#">Delete</a>
<input type="checkbox"/> Event Linkage	Door Alarm	Door Opening Timeout Alarm_DoorChannel4	Access Control Point	<a href="#">Edit</a> <a href="#">Delete</a>

Total 3 item(s) < 1 > item(s) 1/1 Page Jump To 1 Page

## Add

A maximum of 30 linkage configurations can be added (including 2 default configurations: fire alarm triggers the door to keep open; fire alarm cleared triggers the door to close).

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

Event Source

Linkage Type ☒ Event Linkage ☐ Card Number Linkage

\*Event Type  \*Alarm Type

Linkage Target

Buzzer Alarm Output Access Control Point

Access Control... ☐ On ☐ Off ☒ Not Link

Card Reader Bu...

Linkage Name	Linkage Status	Buzzer Duration
WiegandReader1	<input type="radio"/> On <input type="radio"/> Off <input checked="" type="radio"/> Not Link	<input type="text" value="1"/> s
WiegandReader2	<input type="radio"/> On <input type="radio"/> Off <input checked="" type="radio"/> Not Link	<input type="text" value="1"/> s
WiegandReader3	<input type="radio"/> On <input type="radio"/> Off <input checked="" type="radio"/> Not Link	<input type="text" value="1"/> s
WiegandReader4	<input type="radio"/> On <input type="radio"/> Off <input checked="" type="radio"/> Not Link	<input type="text" value="1"/> s
WiegandReader5	<input type="radio"/> On <input type="radio"/> Off <input checked="" type="radio"/> Not Link	<input type="text" value="1"/> s

Cancel OK

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

Event Type	Alarm Type	Description
Device alarm	Alarm triggered by the access control itself.	
	Device tamper alarm	The access controller has been tampered with.
	Fire alarm	Fire-related anomalies such as smoke or fire detection.
	Device tamper alarm cleared	The device tamper alarm has stopped.
	Fire alarm cleared	The fire alarm has stopped.
Door alarm	Alarm triggered by the door connected to the access controller. After selecting this type, you also need to select the specific door channel. To configure alarm linkages for multiple channels, you need to add them one by one.	
	Abnormal door opening alarm	Alarm triggered by an unconventional door opening signal.
	Door open timeout alarm	Alarm triggered when the door remains open beyond the preset timeout period (see <a href="#">Door Parameter Config</a> )
	Normal door magnet opening	Alarm triggered by the door magnet detecting a normal door opening.
	Normal door magnet closing	Alarm triggered by the door magnet detecting a normal door closing.
	Authentication over limit alarm	Alarm triggered after the set number of failed card swipe attempts is reached.
Card reader alarm	Alarm triggered by the card reader connected to the access controller. After selecting this type, you also need to select the specific card reader and event input interface. To configure alarm linkages for multiple readers and event input interfaces, you need to add them one by one.	
	Card reader tamper alarm	The card reader has been tampered with.
	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).
	Card reader tamper alarm cleared	The card reader tamper alarm has stopped.

- 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 access controller itself or an external card reader to emit a buzzer sound.

Access Control... ☐ On ☐ Off ☒ Not Link

Card Reader Bu...	Linkage Name	Linkage Status	Buzzer Duration
	WiegandReader1	<input type="radio"/> On <input type="radio"/> Off <input checked="" type="radio"/> Not Link	1 s
	WiegandReader2	<input type="radio"/> On <input type="radio"/> Off <input checked="" type="radio"/> Not Link	1 s
	WiegandReader3	<input type="radio"/> On <input type="radio"/> Off <input checked="" type="radio"/> Not Link	1 s
	WiegandReader4	<input type="radio"/> On <input type="radio"/> Off <input checked="" type="radio"/> Not Link	1 s
	WiegandReader5	<input type="radio"/> On <input type="radio"/> Off <input checked="" type="radio"/> Not Link	1 s

- Access controller buzzer: The access controller itself emits a buzzer sound. The built-in buzzer will sound 30 times, and the buzzer duration cannot be configured.
- Card reader buzzer: The card reader physically connected to the access controller emits a buzzer sound. If **Linkage Status** is set to **On**, the buzzer duration must be configured.
- Alarm output: If an output device like alarm lamp is connected, you can set alarm output linkage.

Alarm Output

Linkage Name	Linkage Status	Duration
Alarm Output 1	<input type="radio"/> On <input type="radio"/> Off <input checked="" type="radio"/> Not Link	1 s
Alarm Output 2	<input type="radio"/> On <input type="radio"/> Off <input checked="" type="radio"/> Not Link	1 s
Alarm Output 3	<input type="radio"/> On <input type="radio"/> Off <input checked="" type="radio"/> Not Link	1 s
Alarm Output 4	<input type="radio"/> On <input type="radio"/> Off <input checked="" type="radio"/> Not Link	1 s
Alarm Output 5	<input type="radio"/> On <input type="radio"/> Off <input checked="" type="radio"/> Not Link	1 s
Alarm Output 6	<input type="radio"/> On <input type="radio"/> Off <input checked="" type="radio"/> Not Link	1 s

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

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


Access Control ...

Linkage Name	Linkage Status
DoorChannel1	<input type="radio"/> On <input type="radio"/> Off <input type="radio"/> N.O. <input type="radio"/> N.C. <input type="radio"/> Restore Keeping Open/Closed <input checked="" type="radio"/> Not Link
DoorChannel2	<input type="radio"/> On <input type="radio"/> Off <input type="radio"/> N.O. <input type="radio"/> N.C. <input type="radio"/> Restore Keeping Open/Closed <input checked="" type="radio"/> Not Link
DoorChannel3	<input type="radio"/> On <input type="radio"/> Off <input type="radio"/> N.O. <input type="radio"/> N.C. <input type="radio"/> Restore Keeping Open/Closed <input checked="" type="radio"/> Not Link
DoorChannel4	<input type="radio"/> On <input type="radio"/> Off <input type="radio"/> N.O. <input type="radio"/> N.C. <input type="radio"/> Restore Keeping Open/Closed <input checked="" type="radio"/> Not Link

- Click **Save**.

## 9.2 Alarm Function Configuration

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

 **Note:** Prerequisites:


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

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

Linkage Type	Alarm Type	Event Type	Enable	When enabled, the corresponding alarm event will be reported to the platform.
Linkage Configuration	Device Alarm	Device Tamper Alarm	<input type="checkbox"/>	
Linkage Configuration	Device Alarm	Fire Alarm	<input checked="" type="checkbox"/>	
Linkage Configuration	Device Alarm	Device Tamper Alarm Cleared	<input type="checkbox"/>	
Linkage Configuration	Device Alarm	Fire Alarm Cleared	<input checked="" type="checkbox"/>	

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.

 **Note:** Fire alarms and fire alarm cleared are reported by default and cannot be disabled.

Linkage Type	Alarm Type	Event Type	Enable	When enabled, the corresponding alarm event will be reported to the platform.
Linkage Configuration	Device Alarm	Device Tamper Alarm	<input type="checkbox"/>	
Linkage Configuration	Device Alarm	Fire Alarm	<input checked="" type="checkbox"/>	
Linkage Configuration	Device Alarm	Device Tamper Alarm Cleared	<input type="checkbox"/>	
Linkage Configuration	Device Alarm	Fire Alarm Cleared	<input checked="" type="checkbox"/>	

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

Linkage Type	Alarm Type	Event Type	Enable	When enabled, the corresponding alarm event will be reported to the platform.
Linkage Configuration	Door Alarm	Abnormal Door Opening Alarm	<input checked="" type="checkbox"/>	
Linkage Configuration	Door Alarm	Door Opening Timeout Alarm	<input checked="" type="checkbox"/>	
Linkage Configuration	Door Alarm	Normal Door Magnet Opening	<input type="checkbox"/>	
Linkage Configuration	Door Alarm	Normal Door Magnet Closing	<input type="checkbox"/>	
Linkage Configuration	Door Alarm	Authentication Over Limit Alarm	<input checked="" type="checkbox"/>	

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

Access Control Device

DoorChannel1

WiegandReader1

485CardReader1

WiegandReader2

485CardReader2

DoorChannel2

WiegandReader3

WiegandReader4

485CardReader4

DoorChannel3

WiegandReader5

485CardReader5

WiegandReader6

485CardReader6

DoorChannel4

WiegandReader7

485CardReader7

WiegandReader8

485CardReader8

Linkage Type	Alarm Type	Event Type	Enable	When enabled, the corresponding alarm event will be reported to the platform.
Linkage Configuration	Card Reader Alarm	Card Reader Tamper Alarm	<input type="checkbox"/>	6C:4B:90:B5:C0:3
Linkage Configuration	Card Reader Alarm	Duress Card/Code Entry	<input checked="" type="checkbox"/>	
Linkage Configuration	Card Reader Alarm	Unauthorized List Alarm	<input checked="" type="checkbox"/>	
Linkage Configuration	Card Reader Alarm	Card Reader Tamper Alarm Cleared	<input type="checkbox"/>	