DS-K262XX Series Access Controller

User Manual

Regulatory Information

FCC Information

Please take attention that changes or modification not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
FCC compliance: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
—Reorient or relocate the receiving antenna.
—Increase the separation between the equipment and receiver.
—Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
—Consult the dealer or an experienced radio/TV technician for help
This equipment should be installed and operated with a minimum distance 20cm between the radiator and your body.
FCC Conditions
This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:
1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

EU Conformity Statement

CE

This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed

under the EMC Directive 2014/30/EU, RE Directive 2014/53/EU,the RoHS Directive 2011/65/EU

2012/19/EU (WEEE directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information see: www.recyclethis.info

2006/66/EC (battery directive): This product contains a battery that cannot be disposed of as unsorted municipal waste in the European Union. See the product documentation for specific battery information. The battery is marked with this symbol, which may include lettering to indicate cadmium (Cd), lead (Pb), or mercury (Hg). For proper recycling, return the battery to your supplier or to a designated collection point. For more information see:www.recyclethis.info

Industry Canada ICES-003 Compliance

This device meets the CAN ICES-3 (B)/NMB-3(B) standards requirements.
This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions:

1. this device may not cause interference, and
2. this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radioexempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

1. l'appareil ne doit pas produire de brouillage, et
2. l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that necessary for successful communication.
Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peut fonctionner avec une antenne d'un type et d'un gain maximal (ou inférieur) approuvé pour l'émetteur par Industrie Canada. Dans le but de réduire les risques de brouillage radioélectrique à l'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que la puissance isotrope rayonnée équivalente (p.i.r.e.) ne dépasse pas l'intensité nécessaire à l'établissement d'une communication satisfaisante.
This equipment should be installed and operated with a minimum distance 20cm between the radiator and your body.

Cet équipement doit être installé et utilisé à une distance minimale de 20 cm entre le radiateur et votre corps.

Safety Instruction

These instructions are intended to ensure that user can use the product correctly to avoid danger or property loss.

The precaution measure is divided into Dangers and Cautions:

Dangers: Neglecting any of the warnings may cause serious injury or death.

Cautions: Neglecting any of the cautions may cause injury or equipment damage.

⚠	⚠
Dangers: Follow these safeguards to prevent serious injury or death.	**Cautions:** Follow these precautions to prevent potential injury or material damage.

⚠ Danger:

- If the device supports wall mounting or ceiling mounting, the mounting surface shall be able to withstand the additional force of three times the weight of the device but not less than 50 N. The device and its associated mounting means shall remain secure during the installation. After the installation, the device, including any associated mounting plate, shall not be damaged.
- In the use of the product, you must be in strict compliance with the electrical safety regulations of the nation and region.

⚠ Cautions:

- The interface varies with the models. Please refer to the product datasheet for details.
- Provide a surge suppressor at the inlet opening of the device under special conditions such as the mountain top, iron tower, and forest.
- + identifies the positive terminals of the device which is used with, or generates direct current, and - identifies the negative terminal(s) of the device which is used with, or generates direct current.

Available Model

Product Name	Model
Access Controller	DS-K2621X Series Access Controller
	DS-K2622X Series Access Controller
	DS-K2624X Series Access Controller

Contents

Chapter 1 Appearance

1.1 Device Appearance and Interface

Open the case by the key.

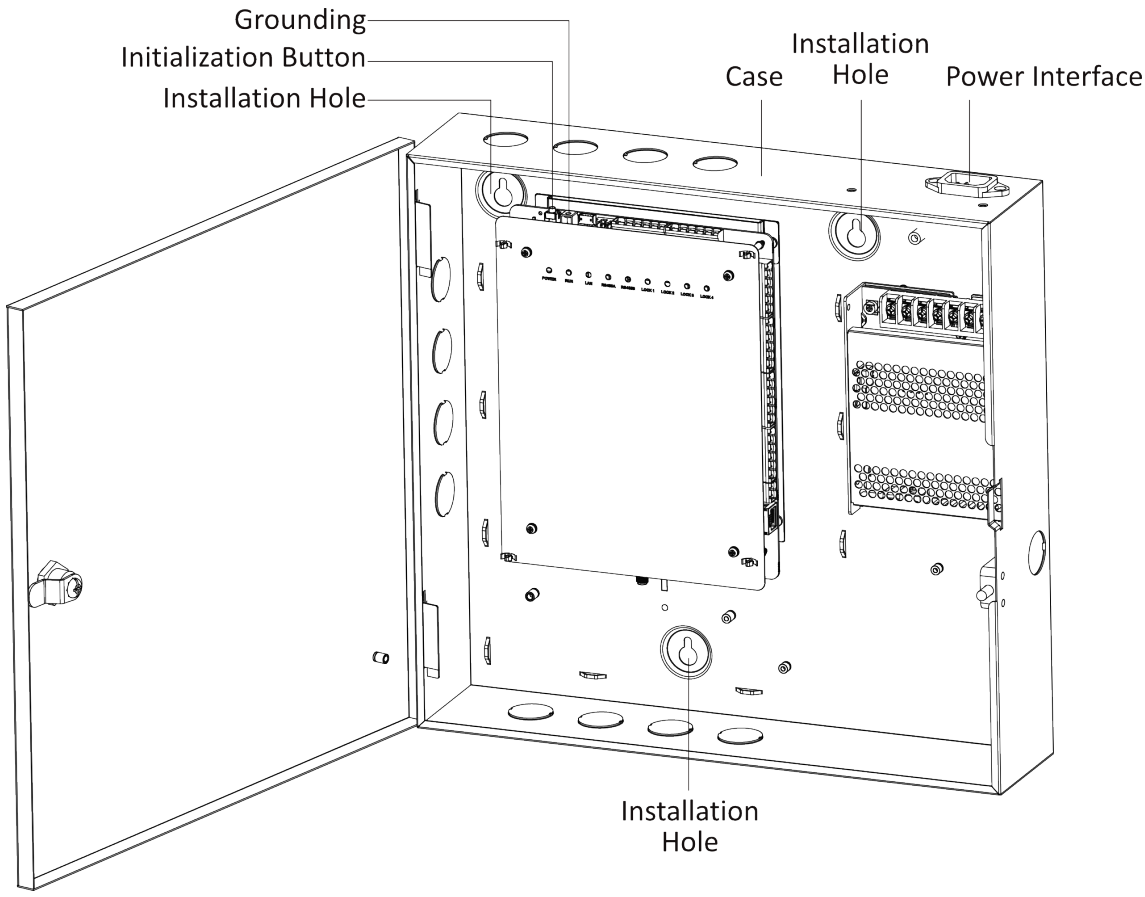


Figure 1-1 Device Component and Interface

1.2 Indicator Description

Introduction of the indicator of 1-Door, 2-Door, and 4-Door controller.

Device Name	Indicator Details
1-Door controller	6 indicators: 1 Power indicator, 1 Operating Status indicator, 1 Network indicator, 2 RS-485 indicators, 1 Door Contact indicator
2-Door controller	7 indicators: 1 Power indicator, 1 Operating Status indicator, 1 Network indicator, 2 RS-485 indicators, 2 Door Contact indicators
4-Door controller	9 indicators: 1 Power indicator, 1 Operating Status indicator, 1 Network indicator, 2 RS-485 indicators, 4 Door Contact indicators

Note

When the Operating Status indicator is red, the device is powered on; when the indicator turns green, the device is added to the platform. When the Door Contact indicator is on, the door is opened; when the indicator is off, the door is closed. When the other indicators are on, the device is connected; when the indicators are off, the device is unconnected.

Chapter 2 Terminal Wiring

Terminal Wiring Description of the Access Controller.

2.1 4-Door Controller Wiring Description

Remove the 4 screws on the controller and remove the decoration sheet. Here taking 4-door controller as an example.

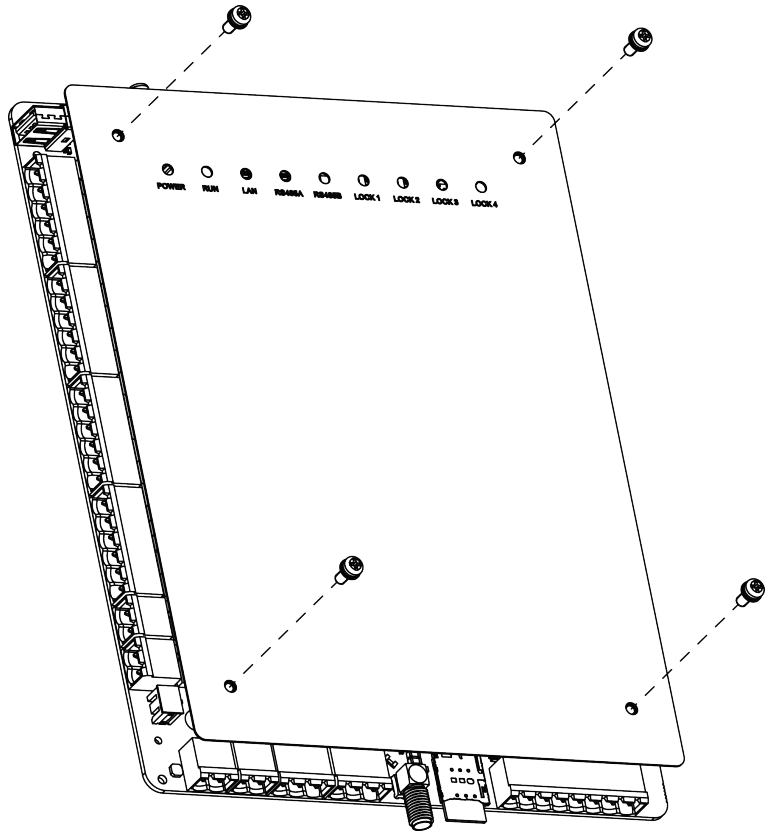


Figure 2-1 Unscrew the Control Box

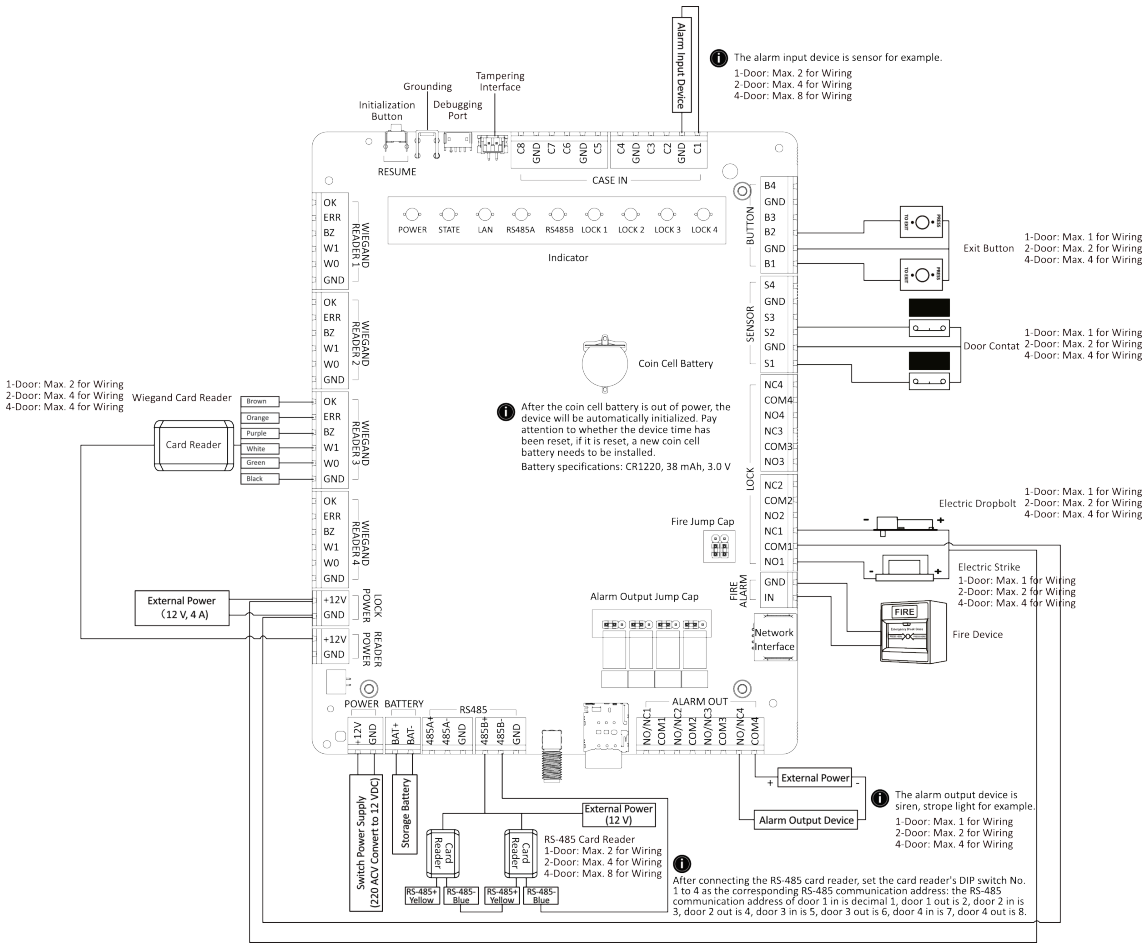


Figure 2-2 Wiring Diagram of the Access Controller

Note

- The recommended specification for the accumulator (optional) is 12 V, 7 Ah.
- The working temperature of the accumulator is 0 °C to 40 °C.
- Recommended specifications of cable: door lock power supply: AWG18; Card reader power supply: AWG20; Other cables: AWG22.

2.2 Wiegand Card Reader Wiring

You can view the Wiegand card reader wiring diagram.

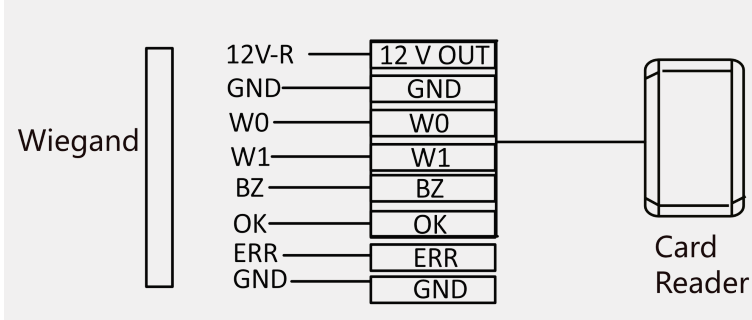


Figure 2-3 Wiegand Card Reader Wiring Diagram

Note

You must connect the OK/ERR/BZ, if using access controller to control the LED and buzzer of the Wiegand card reader.

2.3 RS-485 Card Reader Wiring

You can view the RS-485 card reader wiring diagram.

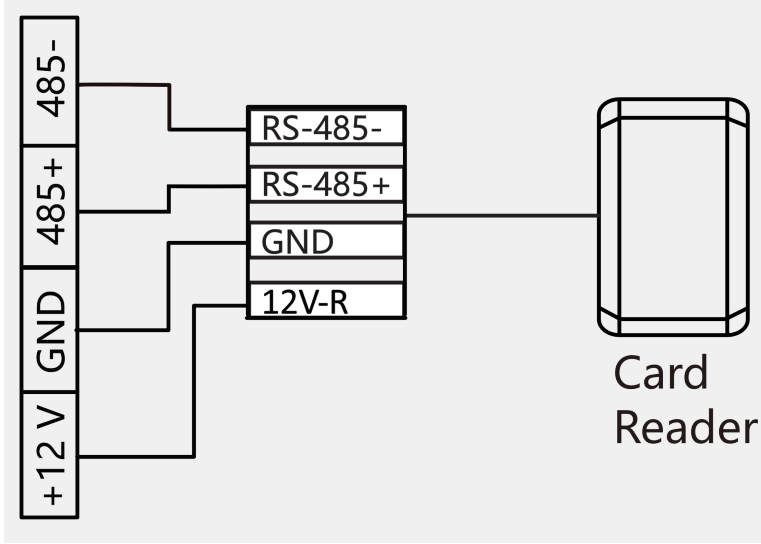


Figure 2-4 RS-485 Card Reader Wiring Diagram

Note

- If the card reader is installed too far away from the access controller, you can use an external power supply.
- It is recommended to use hand-in-hand wiring to connect the RS-485 card reader.

2.4 Door Lock Wiring

You can view the door lock wiring diagram.

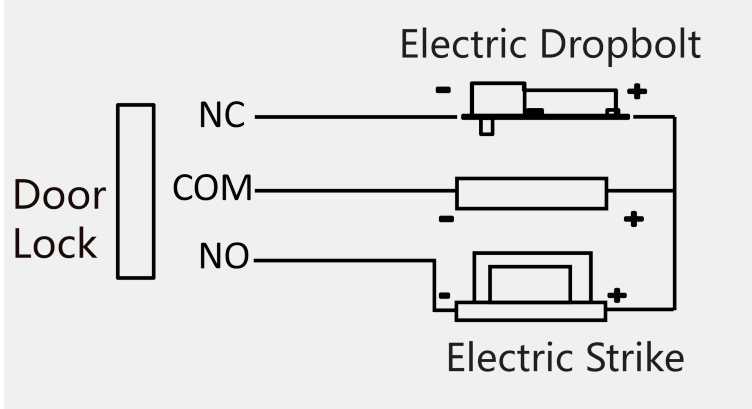


Figure 2-5 Wiring Diagram of Door Lock

2.5 Alarm Wiring

You can view the alarm wiring diagram.

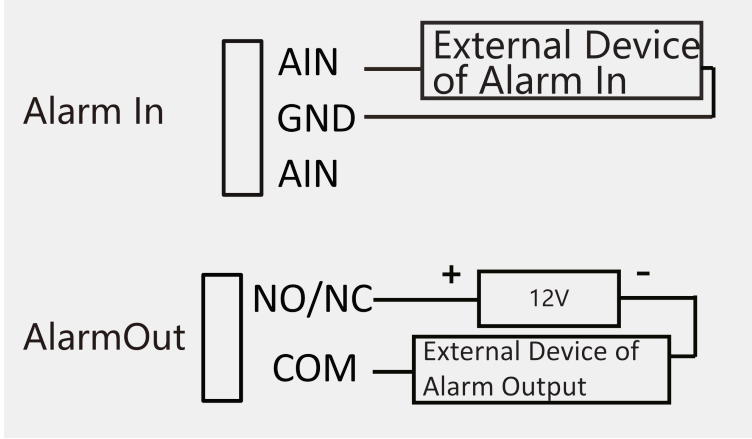


Figure 2-6 Alarm Wiring

2.6 Exit Button Wiring

You can view the exit button wiring diagram

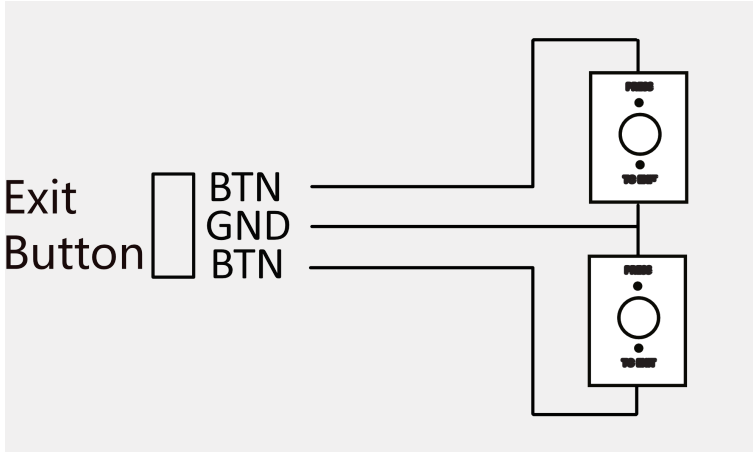


Figure 2-7 Exit Button Wiring

2.7 Door Contact Wiring

You can view the door contact wiring diagram.

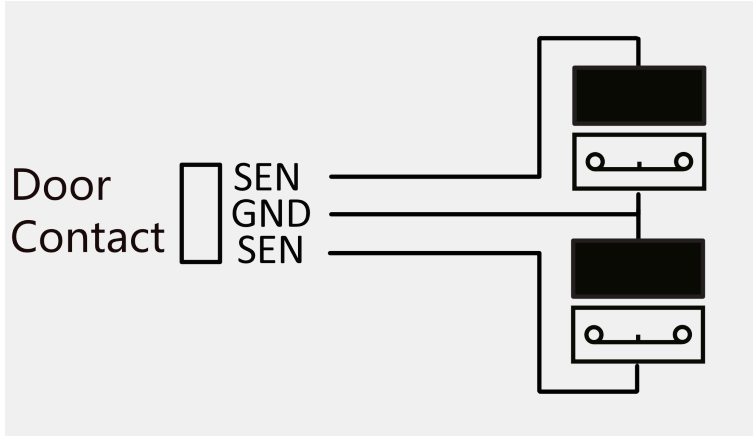


Figure 2-8 Door Contact Wiring

2.8 1-Door/ 2-Door Board

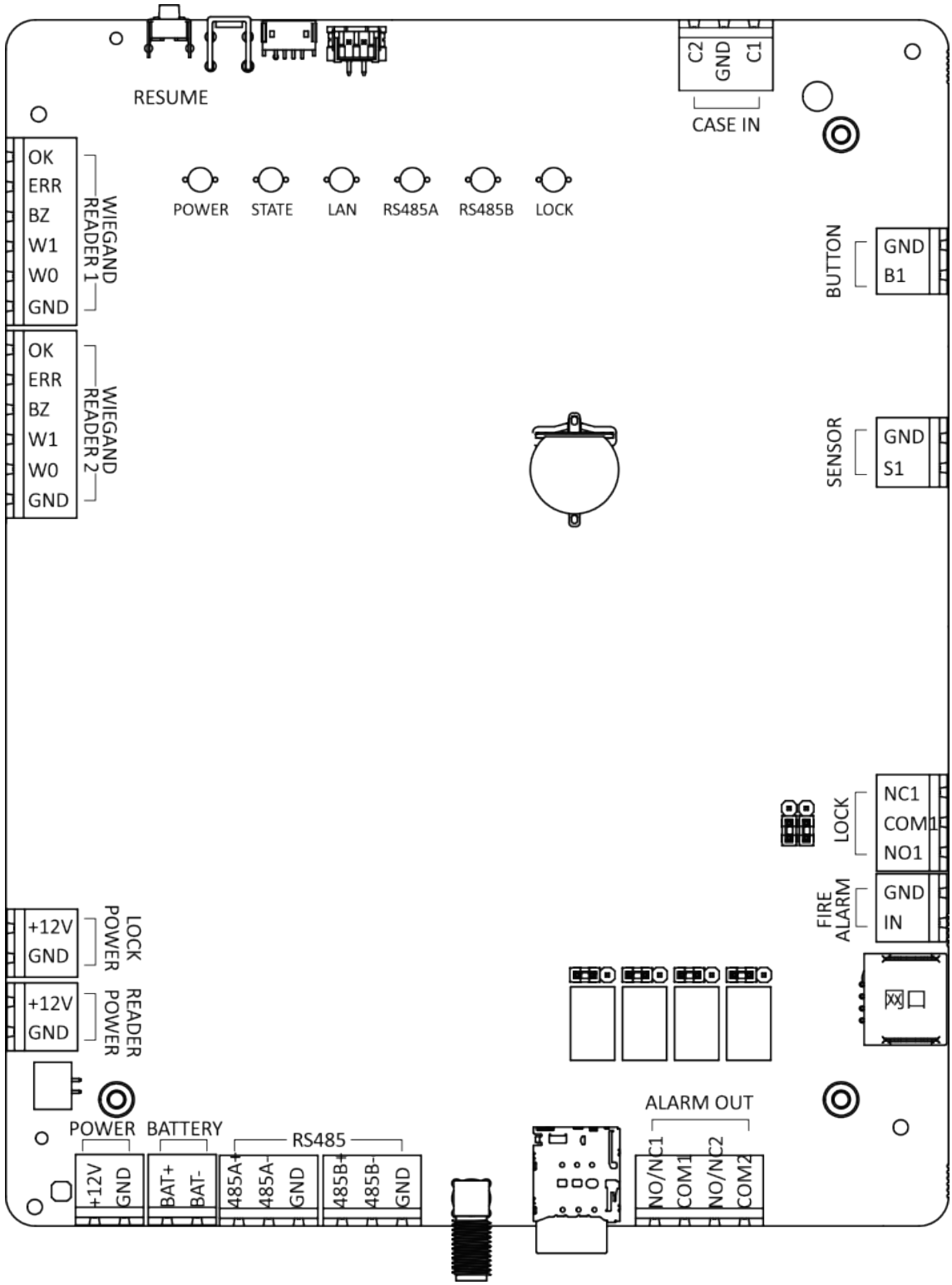


Figure 2-9 1-Door Board

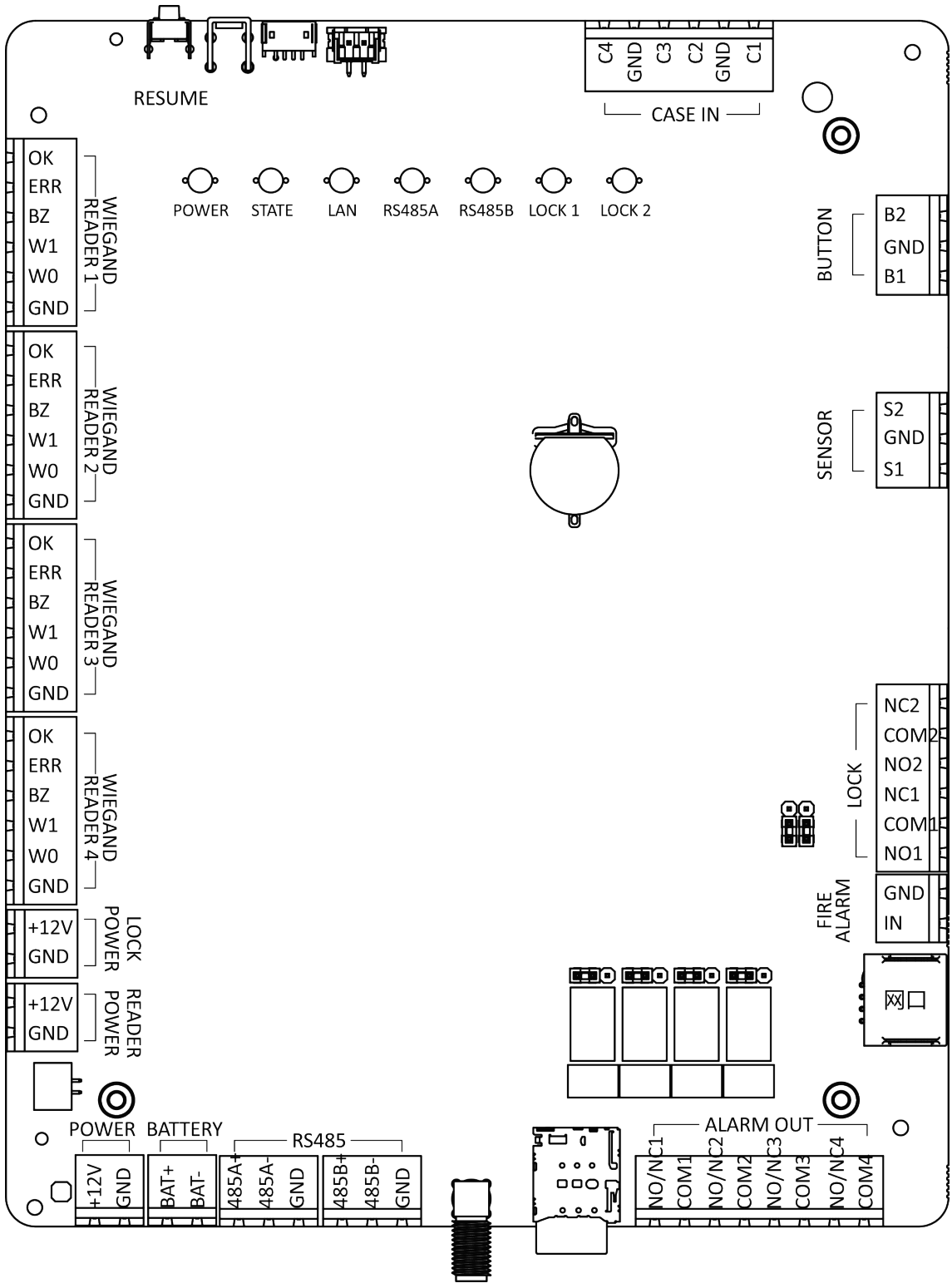


Figure 2-10 2-Door Board

Chapter 3 Installation

The case of the access controller can be screwed to the wall。

Steps

Note

- The device can be installed indoors.
- The wall holding the case should be able to support wight three times of the device steadily with no damages to the equipment itself.
- Here taking 4-Door controller as an example.

1. Fix 3 SC-KA4X45 screws to the wall, and 3 to 5 mm thread should be reserved on the top of the screw (to facilitate subsequent hanging of the case).

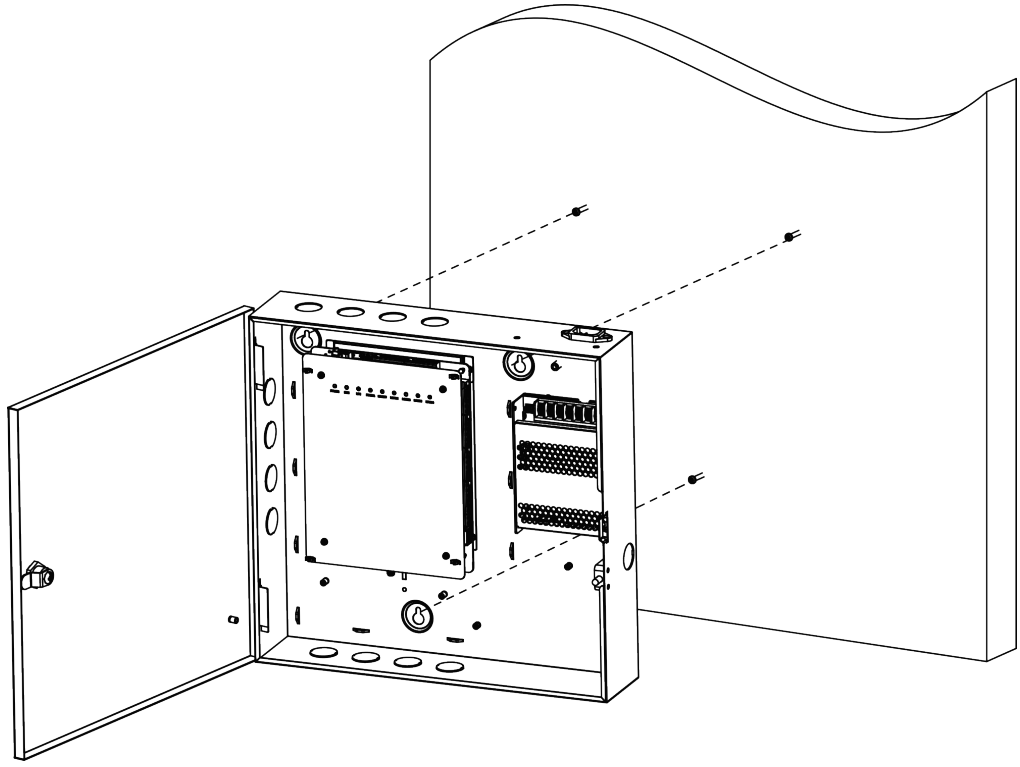


Figure 3-1 Fix Access Controller

2. Open the case door and align the installation holes on the case with the screws reserved on the wall. Then attach the case from top to bottom onto the screws.

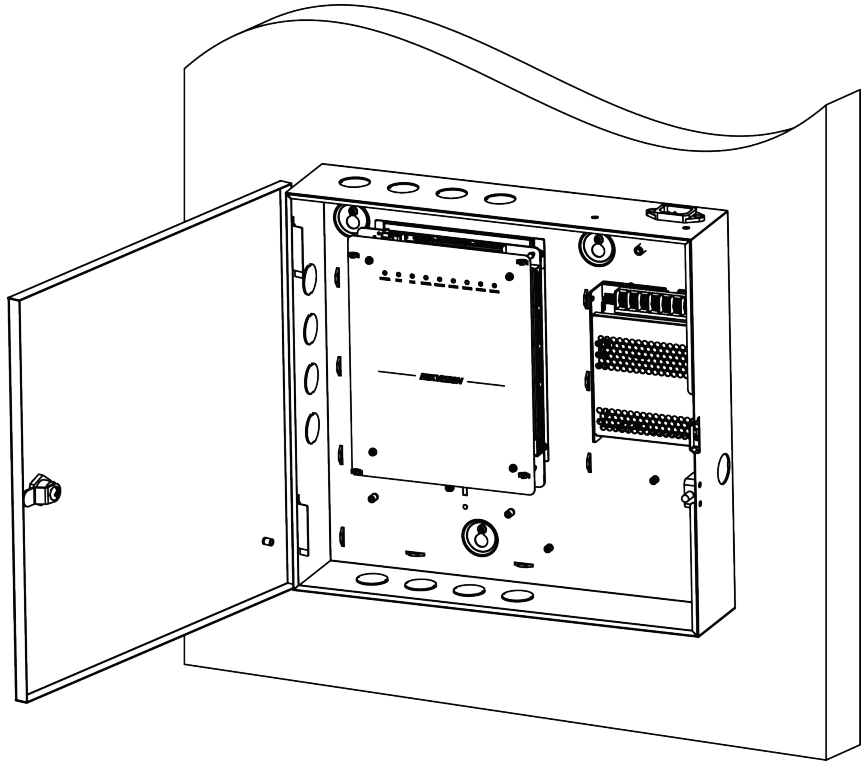


Figure 3-2 Hang Access Controller

3. Close the case door and complete the installation.

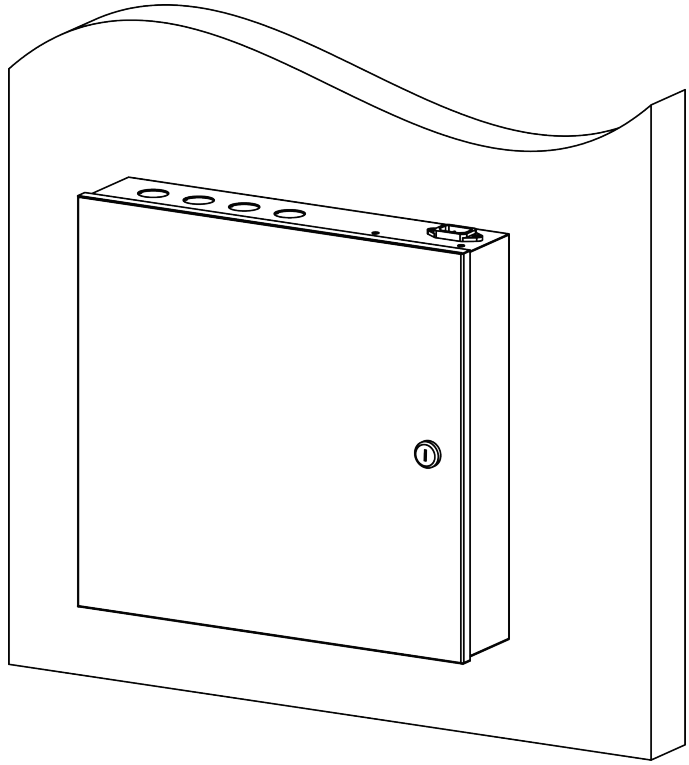


Figure 3-3 Installation completed

Chapter 4 Device Debugging

Device Initialization

Hold the initialization button for 5 s to initialize.

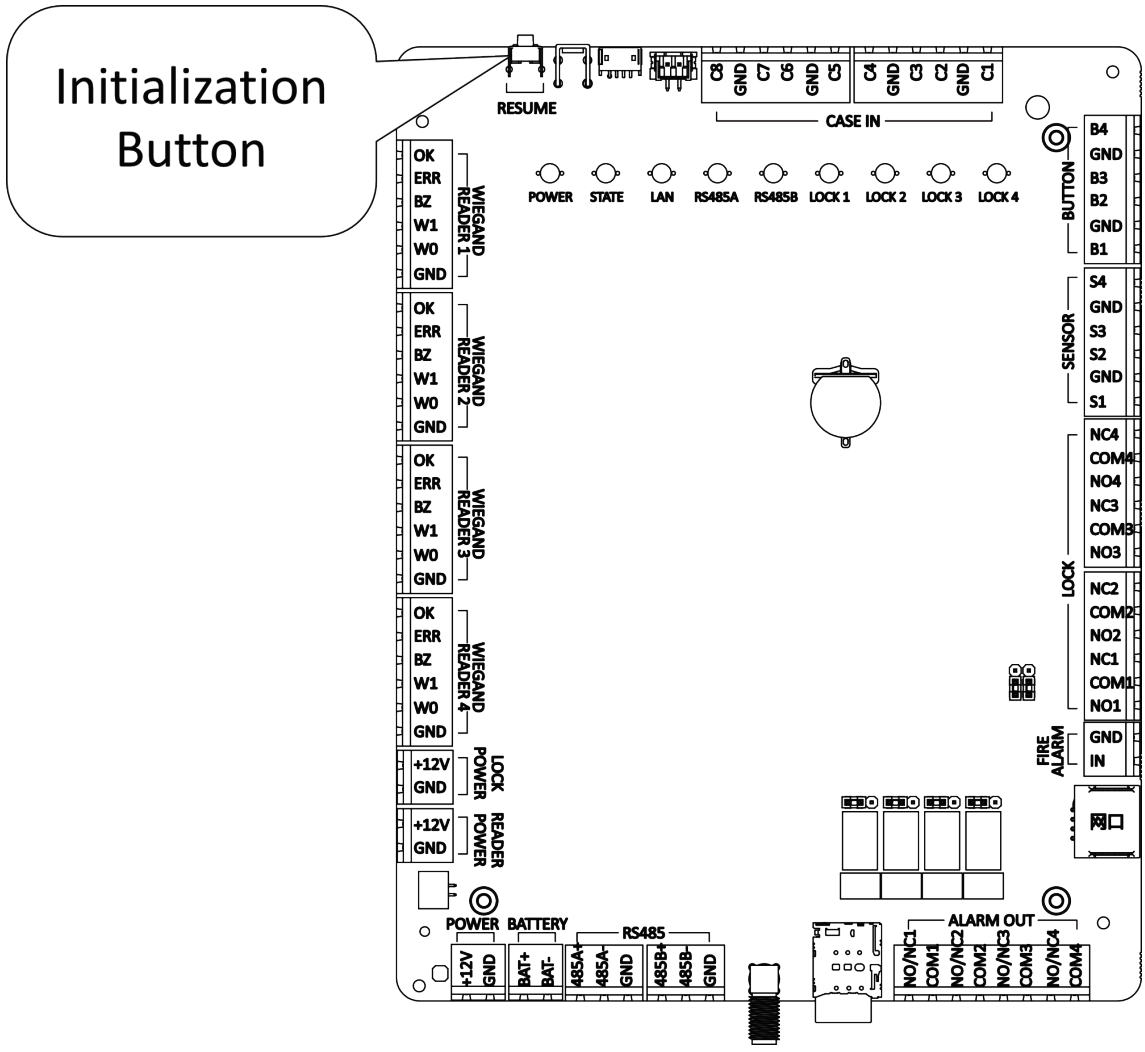


Figure 4-1 Device Initialization

Fire Relay Remain Open/Close Selection

Note

This operation requires disassembling the upper shell of the device, which is recommended to set by a professional.

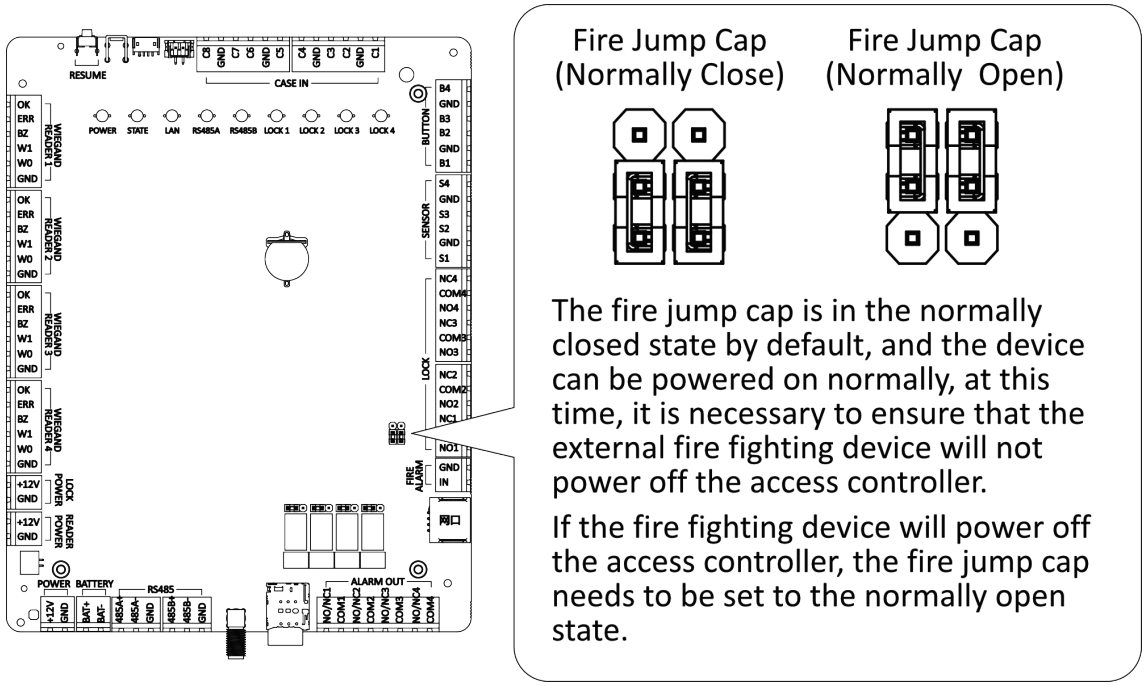
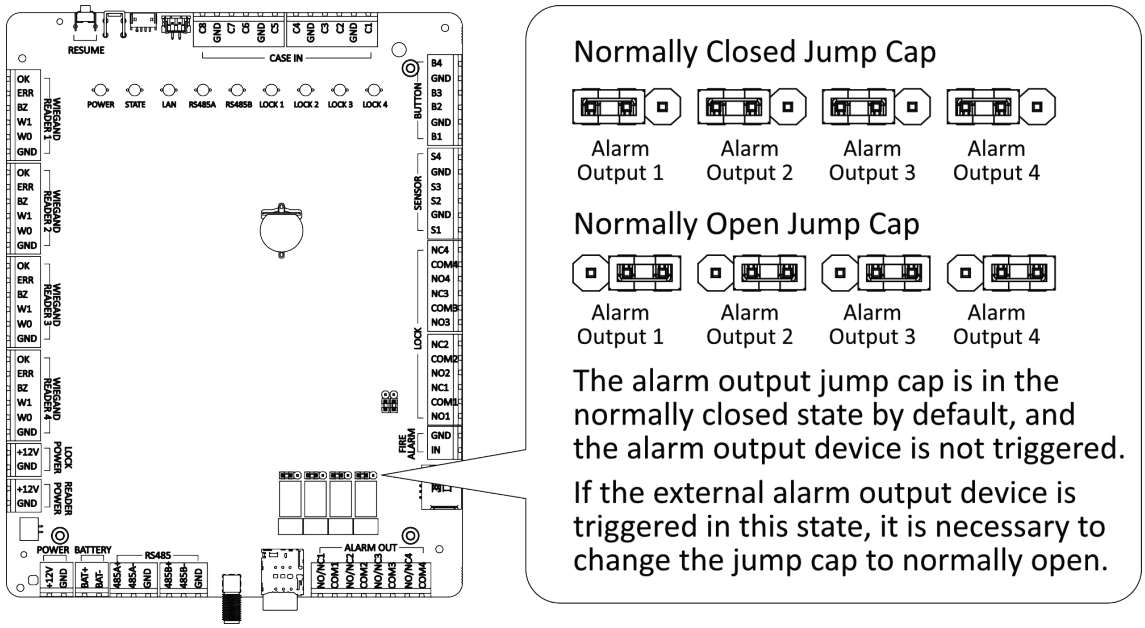


Figure 4-2 Fire Relay Remain Open/Close Selection

Alarm Output Jump Cap Selection (Taking 4-Door as an Example)



This operation requires disassembling the upper shell of the device, which is recommended to set by a professional.

Figure 4-3 Alarm Output Jump Cap Selection (Taking 4-Door as an Example)

Chapter 5 Typical Application

Typical application of access controller, door lock and platform.

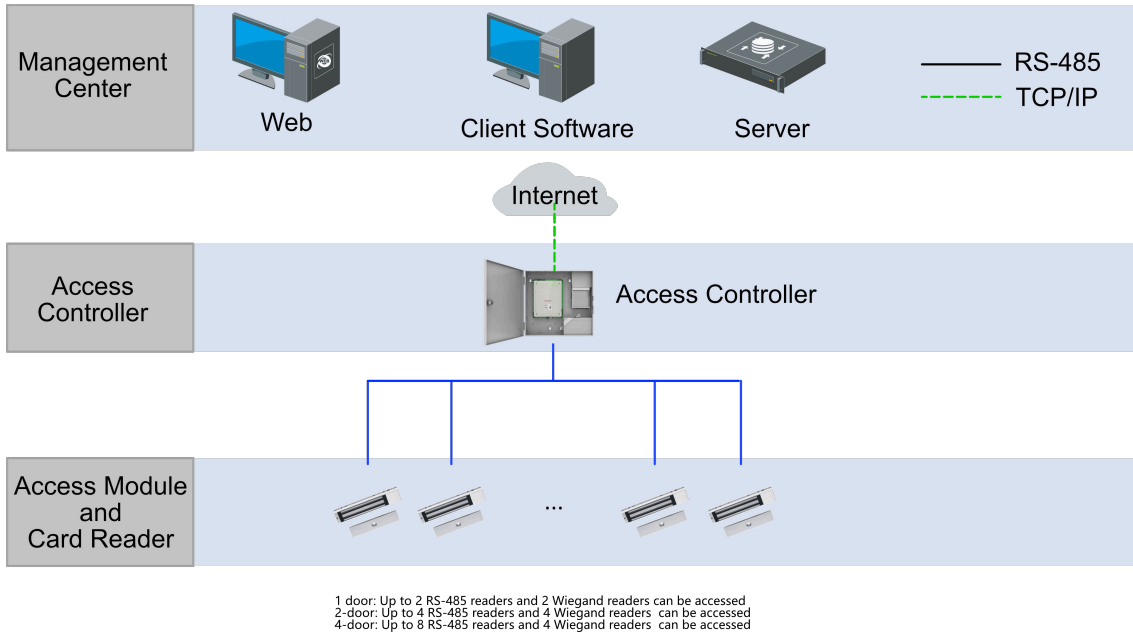


Figure 5-1 Typical Application Example

Chapter 6 Activation

You should activate the device before the first login. After powering on the device, the system will switch to Device Activation page.

Activation via the device, SADP tool and the client software are supported.

The default values of the device are as follows:

- The default IP address: 192.0.0.64
- The default port No.: 8000
- The default user name: admin

6.1 Activate via Web Browser

You can activate the device via the web browser.

Steps

1. Enter the device default IP address (192.0.0.64) in the address bar of the web browser, and press **Enter**.

   Note

   Make sure the device IP address and the computer's should be in the same IP segment.

2. Create a new password (admin password) and confirm the password.

   Caution

   - The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.
   - Proper configuration of all passwords and other security settings is the responsibility of the service provider and/or end-user.
   - Do not contain following characters in the password: the user name, 123, admin (case-insensitive), 4 or more continuously increasing or decreasing digits, or 4 or more consecutively repeated characters.
   - Password cannot contain words such as hik, hkws, and hikvision (case insensitive).

3. Click **Activate**.
4. Edit the device IP address. You can edit the IP address via the SADP tool, the device, and the client software.

6.2 Activate via SADP

SADP is a tool to detect, activate and modify the IP address of the device over the LAN.

Before You Start

- Get the SADP software from the supplied disk or the official website ***http://www.hikvision.com/en/*** , and install the SADP according to the prompts.
- The device and the PC that runs the SADP tool should be within the same subnet.

The following steps show how to activate a device and modify its IP address. For batch activation and IP addresses modification, refer to *User Manual of SADP* for details.

Steps

1. Run the SADP software and search the online devices.
2. Find and select your device in online device list.
3. Input new password (admin password) and confirm the password.

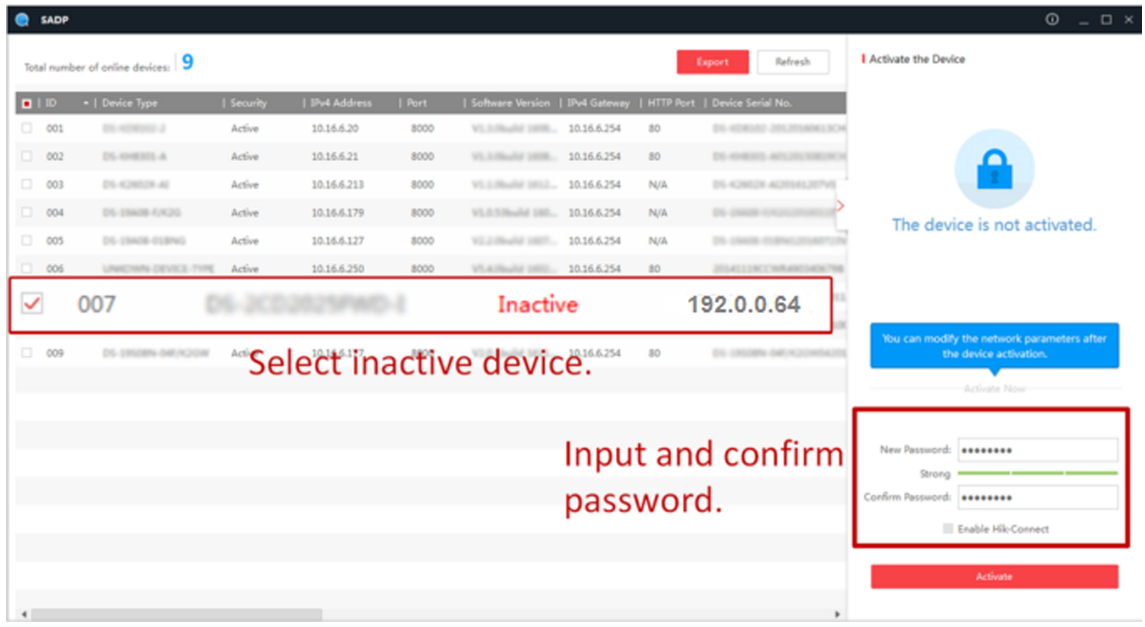
Caution

STRONG PASSWORD RECOMMENDED-We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

Note

Characters containing admin and nimda are not supported to be set as activation password.

4. Click **Activate** to start activation.



Status of the device becomes **Active** after successful activation.

5. Modify IP address of the device.
   1) Select the device.
   2) Change the device IP address to the same subnet as your computer by either modifying the IP address manually or checking **Enable DHCP**.
   3) Input the admin password and click **Modify** to activate your IP address modification.

Chapter 7 Operation via Web Browser

7.1 Login

You can login via the web browser or the remote configuration of the client software.

Note

- Make sure the device is activated. For detailed information about activation, see Activation Chapter.
- It is recommended to log in through the Chrome browser.

Login via Web Browser

Enter the device IP address in the address bar of the web browser and press **Enter** to enter the login page.
Enter the device user name and the password. Click **Login**.

Login via Remote Configuration of Client Software

Download and open the client software. After adding the device, click to enter the Configuration page.

7.2 Forget Password

If you forget the password when logging in, you can change the password by email address or security questions.

On the login page, click **Forget Password**.

Select **Verification Mode**.

Security Question Verification

Answer the security questions.

E-mail Verification

1. Export the QR code and send it to ***pw_recovery@hikvision.com*** as attachment.
2. You will receive a verification code within 5 minutes in your reserved email.
3. Enter the verification code into the verification code field to verify your identification.

Click **Next**, create a new password and confirm it.

7.3 Download Web Plug-In

Both non-Plug-in live view and live view after downing plug-in are available. For better live view, downloading plug-in for live view is recommended.

Click → **Download Web Pug-In** to download the pulg-in to the local.

7.4 Help

7.4.1 Open Source Software Licenses

You can view open source software licenses.

Click → **Open Source Software Statement** on the upper-right corner to view the licenses.

7.4.2 View Online Help Document

You can view the help document for Web configuration.

Click → **Online Document** on the upper right of the Web page to view the document.

7.5 Logout

Log out the account.

Click **admin → Logout → OK** to logout.

7.6 Quick Operation via Web Browser

7.6.1 Set Security Question

If you forget the device activation password, you can change the password via security questions and E-mail. Set the security questions before configuration.

Click in the top right of the web page to enter the **Change Password** page.

Security Question Verification

Answer the security questions.

E-mail Verification

1. Export the QR code and send it to ***pw_recovery@hikvision.com*** as attachment.
2. You will receive a verification code within 5 minutes in your reserved email.
3. Enter the verification code into the verification code field to verify your identification.

click **Next**. Or you can click **Skip** to skip the step.

7.6.2 Select Language

You can select a language for the device system.

Click in the top right of the web page to enter the **Device Language Settings** page. You can select a language for the device system from the drop-down list.

By default, the system language is English.

Note

After you change the system language, the device will reboot automatically.

7.6.3 Time Settings

Click in the top right of the web page to enter the wizard page.

Time Zone

Select the device located time zone from the drop-down list.

Time Sync.

NTP

You should set the NTP server's IP address, port No., and interval.

Manual

By default, the device time should be synchronized manually. You can set the device time manually or check **Sync. with Computer Time** to synchronize the device time with the computer's time.

Server Address/NTP Port/Interval

You can set the server address, NTP port, and interval.

DST

You can view the DST start time, end time and bias time.

7.7 Operation Process

Log in to Web to operate access control, people management, and maintenance management.

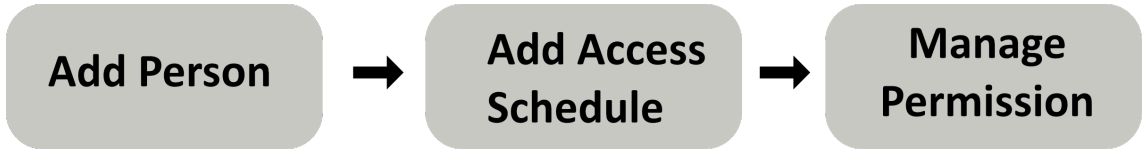


Figure 7-1 Configuration Process

7.8 Add Person

Add the person's information, including the basic information, certificate, authentication and settings.

Add Basic Information

Click **Person Management → Add** to enter the Add Person page.
Add the person's basic information, including the employee ID, the person's name, organization, gender, and person type.

Note

- If you select **Visitor** as the person type, you can set the visit times.
- Letters are allowed in the employee ID. Up to 32 bits are allowed.
- Up to 128 bits are allowed in the name.

Click **Add** to save the settings.
Click **Save and Continue** to save the settings and continue to add next person.

Set Permission Time

Click **Person Management → Add** to enter the Add Person page.
Enable **Long-Term Effective User**, or set **Start Time** and **End Time** and the person can only has the permission within the configured time period according to your actual needs.
Click **Add** to save the settings.
Click **Save and Continue** to save the settings and continue to add next person.

Add Card

Click **Person Management → Add** to enter the Add Person page.
Click **Configuration**. If select the Collection Device as **Card Enrollment Station**, you should select the device model, card type, set buzzing, M1 card encryption, and sector. Click **OK** to save.

Note

If select the Collection Device as **Card Enrollment Station**, click **Download** to download the plug-in to view the device status. During the installation, you should close the web page.

If select the Collection Device as **Card Reader**, you should select the card reader from the drop-down list. Click **OK** to save.
Click **Add Card**, enter the **Card No.** and select the **Property**, and click **OK** to add the card.
Click **Add** to save the settings.
Click **Save and Continue** to save the settings and continue to add next person.

Add Fingerprint

Note

Only devices supporting the fingerprint function can add the fingerprint.

Click **Person Management → Add** to enter the Add Person page.
Click **Configuration**. If you select**USB Fingerprint Recorder**, you can click **Download**to download the plug-in and view the status. Or select **Fingerprint and Card Reader** and select a card reader from the drop-down list. Click **OK** to save.

Note

During the installation, you should close the web page.

Click **Add Fingerprint**, and press your finger on the fingerprint module of the device to add your fingerprint.
Click **Add** to save the settings.
Click **Save and Continue** to save the settings and continue to add next person.

Note

The plugin for adding card or fingerprint via USB is only available in Windows.

Add PIN

Before configuring PIN, it is necessary to clarify whether the PIN is a device-set personal PIN or a platform-applied personal PIN. If it is a device-set personal PIN, it can be created or edited on the device or on the web, and cannot be set on other platforms; If it is a platform-applied personal PIN, it can be created or edited on the platform, and issued to the device before it can be used. It cannot be set on the device or on the web.
Make sure you have already set the PIN mode as **Device-Set Personal PIN** in . Click **PIN Mode** on the page to go to configure.
Click **Person Management → Add** to enter the Add Person page.
Set the PIN. Or click **Auto Generate** to generate a PIN automatically.
Click **Add** to save the settings.
Click **Save and Continue** to save the settings and continue to add next person.

Authentication Settings

Click **Person Management → Add** to enter the Add Person page.
Set the authentication type.
Click **Add** to save the settings.
Click **Save and Continue** to save the settings and continue to add next person.

Permission Management

Before you start:

- You have already add the device. For details, see ***Device Management*** .
- You have already complete access point management. For details, see .
- You have already complete the access permission management. For details, see ***Permission Management*** .

Click **Person Management → Add** to enter the Add Person page.
Set the permission parameters.

Permission Type

By Permission Group

Click **Allocate** and select an added access permission. The person will contain the checked access permission. If you have not added the access permission in advance, you can click **Add Access Permission** to add. For details, see ***Permission Management*** . Click **OK**.

By Access Point

Click **Allocate** and select the access schedule. Click**Add** to add the access points. The person will contain the permissions of the access point within the access schedule. Click **OK**.

Extend Door Opening

The person related door will close after the configured time duration. You should go to to set the **Extended Open Duration**. Click **Door Parameters** to go to the configuration page.

Click **Add** to save the settings.
Click **Save and Configure** to save the settings and continue to add next person.

Edit/Delete/Search Person

Click **Person Management** to enter the page.
Select a person and click to edit the person's information.
Select a person and click to delete the person information.
Select multiple person, click **Delete** can delete person in batch.
Click **Import** or **Export**.
Click **Clear All** to delete all person information.
Click or to switch the viewing method.
Enter the person's employee ID and select the credential status and click **Filter** to search. Click **Reset** to reset all conditions.
Check **Show Sub Organization**, all persons in the sub organizations will be displayed.

7.9 Device Management

7.9.1 Search Not Added Device

The system can automatically search for not added modules that have been connected to the access controller.

Click **Device Management → Search Not Added Device** . The searched not added modules will be displayed in the list of the page.

Click + in the action bar to add module to the access controller.

7.9.2 Add IO Module

Add IO module manually.

Before You Start

Make sure that the area has been added. For more details, see .

Steps

1. Click **Device Management** to enter the settings page.
2. Select IO module.
3. Select the dial address of the IO module, and set the DIP switch of the IO module to be consistent with the one shown in the picture.

   Note

   After adding or modifying the dialing address of the IO module, you need to reboot the IO module to take it effect.
4. Set alarm input and out parameters.

   Alarm Input

   Set the alarm input No. and name.

   Alarm Output

   Set the alarm output No. and name. You can set **Alarm Duration**.

   Continuous Alarm

   The alarm output device will continuously in the alarm status.

   Custom Alarm Duration

   You should set the custom duration. The alarm output device will be in the alarm status for the configured time duration.

   Note

   Range: from 1 to 5999s.
5. Click **OK**.
6. **Optional:** Other Operations

Icon	Description
	You can edit the IO module.
	You can delete the IO module.
	You can restart the IO module.

You can restore the IO module to the factory settings.

You can upgrade the IO module. Select a local upgrade package to upgrade.

7.10 Access Control Management

7.10.1 Overview

You can control the door status, view the device status, view the event, view the alarm data, view the person information, network status, basic information, and device capacity. You can also enter the page from quick start part.

Login the web browser and enter the **Access Control → Overview** .

Remote Unlock

/ / /

Set the door status as unlock, closed, remain open, or remain closed.

Quick Start

Click **Add Person**, **System Settings**, or **Maintenance** on the upper-right of the page to quick enter the page to configure parameters.

Event

You can view the event Employee ID, Name, Card No., Door, and Event Types.

You can also click **View More** to enter the search conditions, including the event type, major type, sub type, employee ID, the name, the card No., the start time, and the end time, and click **Search**. The results will be displayed on the right panel.

Device Status

View the other linked devices' status.

Person Information

View the person number, card number, fingerprint No.

Network Status

You can view the connected and registered status of wired network, wireless network, ISUP and cloud service.

Basic Information

You can view the model, serial No. and firmware version.

Device Capacity

You can view the person, card, fingerprint, and event capacity.

7.10.2 Search Event

Click **Access Control → Event Search** to enter the Search page.

Enter the search conditions, including the event type, the employee ID, the name, the card No., the start time, and the end time, and click **Search**.

Note

The searched name should be up to 32 bits.

The results will be displayed on the right panel.

7.10.3 Permission Management

You can set access permission schedule template, holiday schedule template, and set access permission.

Configure Schedule Template

Add Access Schedule Template

Access schedule template is used to set the allowed passing time for people to entry and exit. The system disk provides 3 default access schedule templates: All-Day Template, Workday Template and Weekday Template. The user can also add customized template according to needs.

Steps

1. Click **Access control → Permission Management → Access Plan Management → +Add**.

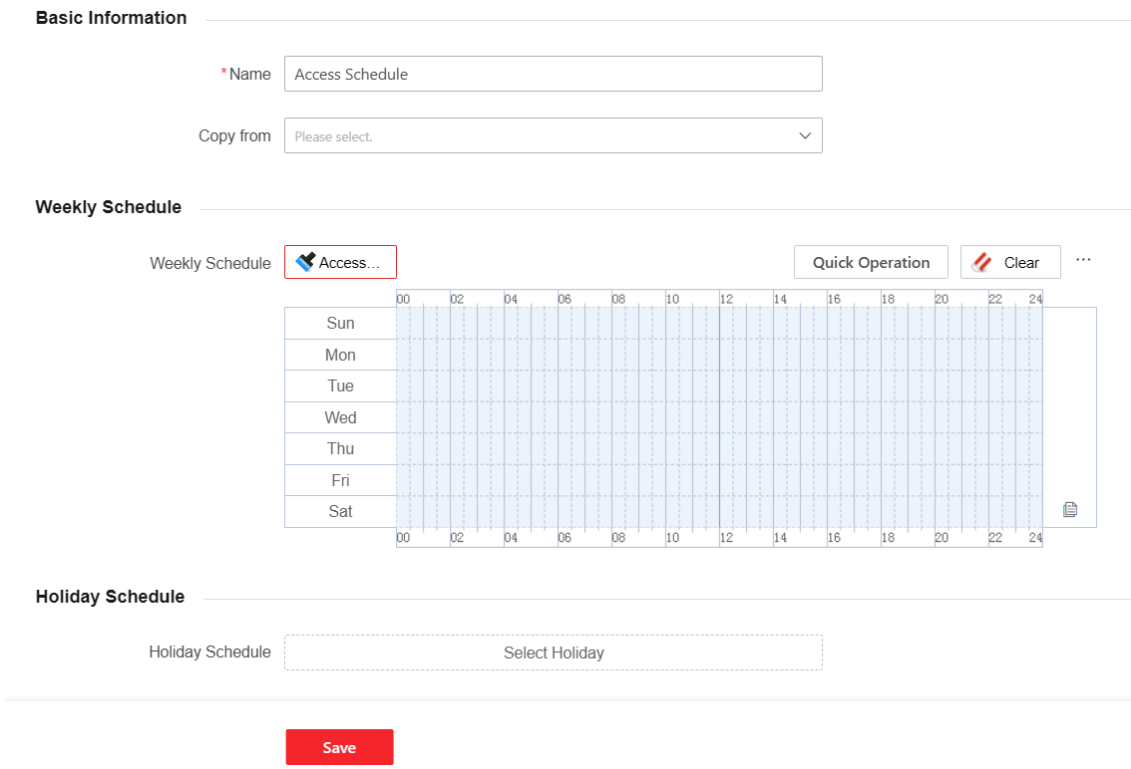


Figure 7-2 Add Access Schedule Template

2. Set basic information.

   Name

   Set basic information.

   Copy from

   The user can select an existing template. After selected, the chosen one will be duplicate to your current template. The user can make adjustments based on this template.

3. On Weekly Schedule, click **Access Time Period**, then you can drag your cursor on the timestamp to map your access time.

   Note

   A maximum of 8 period is allowed per day.

4. **Optional:** Click **Clear**, then drag your cursor. The overlapping part can be erased. You can also click a certain time period then adjust it manually.
5. **Optional:** Select Holiday Schedule.

   Note

   If the chosen Holiday schedule has conflict with Weekly Schedule, the Weekly Schedule will be prioritized.

1) Click **Select Holiday**.
2) Select existing holiday schedule or click **Add**. Enter Holiday Name, Date and Access Time Period.

Note

A maximum of 8 period is allowed per day.

3) Click **OK**.
4) The user can then check the allowed access time period during the holiday.

6. Click **Save**.

Holiday Schedule Template

Set official holidays or specified dates as holidays. The access level of set holidays is higher than the other basic access level.

Steps

1. Click **Access control → Permission Management → Access Plan Management → +Add**.
2. Enter holiday name in the right column.
3. **Optional:** Enable **Repeat Annually** according to actual demand. Once enabled, the template will take effect every year. No need to set again. Applicable to set official holidays.
4. Set Start Date and End Date.
5. Drag cursor on corresponding timestamp to map valid access period. People can access during valid access period.
6. **Optional:** Click **Clear** to adjust chosen time period. You can also click a certain time period then adjust it manually.
7. Click **Save**.

Access Control Management

Access permission can be customized or classified based on access point.

Steps

1. Click **Access control → Permission Management → +Add**.

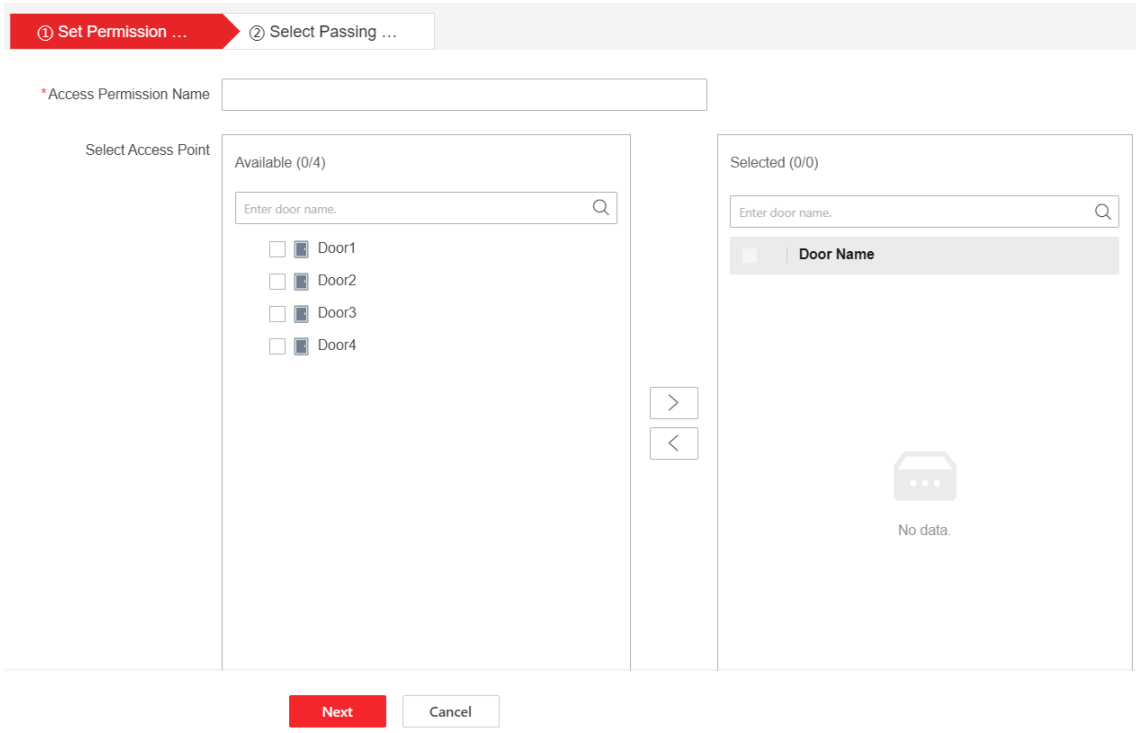


Figure 7-3 Access Control Management

2. Enter **Access Permission Name**.
3. Select **Access Schedule** Template. Click **View Licenses** on the right side to check the access time period of different templates.
4. Click **+Add**. Select access point. Click Save.
5. Click **Save**.

7.10.4 Access Control Application

Open Door with First Person

After a set person (the first person) get verified via credential (such as card, fingerprint, face picture). The others can enter directly or can use credential to get through. Usually apply to mass transit scene.

Steps

1. Click **Access Control → Access Control Application → Open Door with First Person → Settings → +Add**.

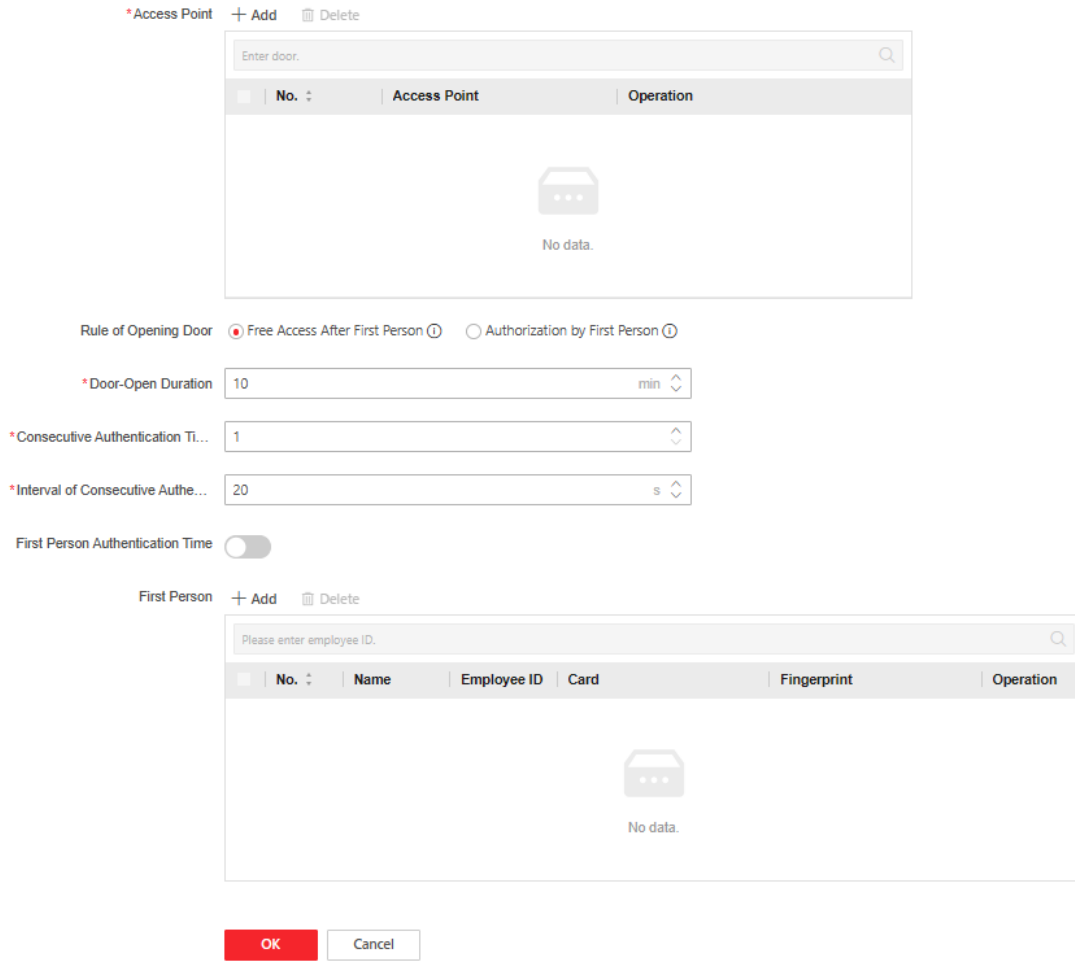


Figure 7-4 Open Door with First Person

2. Click **+Add**.Select access point.
3. Set parameters for Open Door with First Person.

Rule of Opening Door

Free Access After First Person

The mode is applicable for the passing of groups of persons, such as visitors entering the scenic spots. After the set person passes through, the door will open for a set time and other persons can pass through without authentication. Door-Open Duration.

Authorization by First Person

The mode is applicable to places with high security requirements. Only after the person configured with access permission passes through, other persons can pass through after authenticating with credentials.

Consecutive Authentication Times

Numbers of successful authentication during consecutive authentication.

Interval of Consecutive Authentication

The permitted length of interval of consecutive authentication for a same person. Repeated authentication for the same person during the interval is not valid.

First Person Authentication Time

Set **Rules Takes Effect at** and **Authentication Period**.

4. Add First Person Click **+Add** to choose person.
   1) Click **+Add**.
   2) Select a person.
   3) Click **OK**.
5. Click **OK**.
6. **Optional:** Select persons you want to delete from the list. Click **Delete**.

Multi-Factor Authentication Settings

Only after authenticating according to the multi-factor authentication rule, can persons in multi-factor authentication groups open the door.

Before You Start

- Please refer to ***Permission Management*** for completed configuration information and detailed configuration method.

Steps

1. Click **Access Control → Access Control Application → Multi-Factor Authentication → Set**.

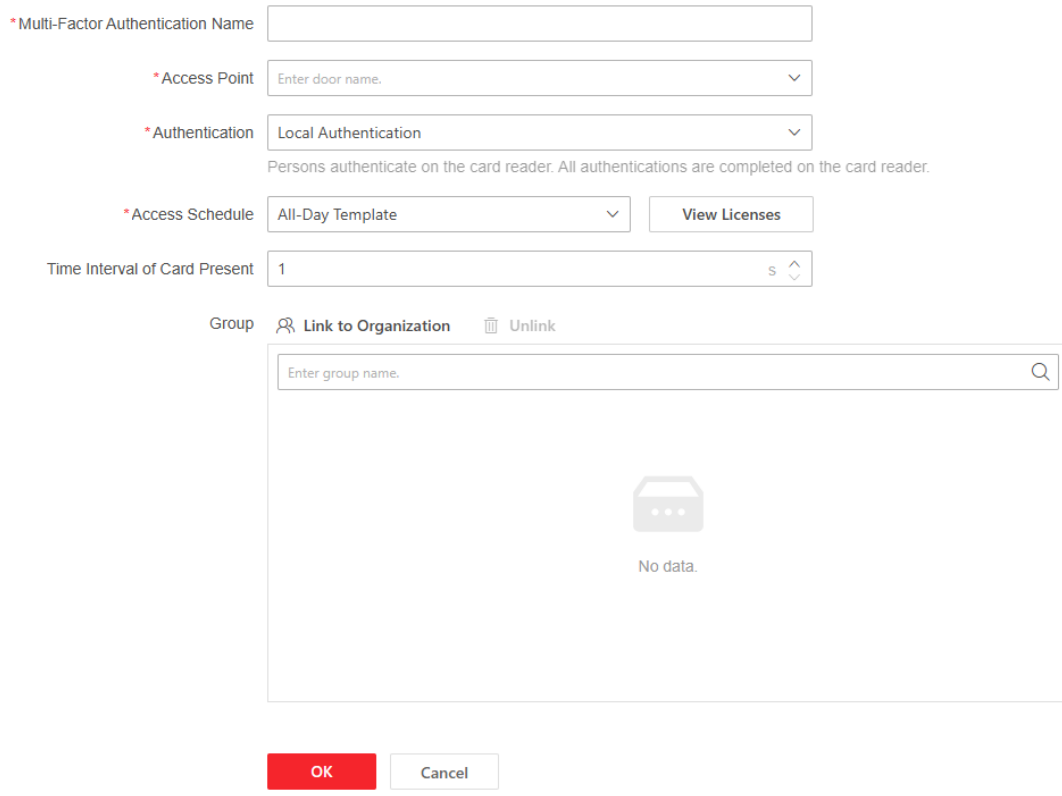


Figure 7-5 Multi-Factor Authentication Settings

2. Click **Group Management** to configure group.
1) Click **+** on the left, then enter group name.
2) Click **+Add** and select persons you want to add to this group. Click **OK**.
3) Click **OK**. The added groups will be showed in the left column. Information of group members will be showed at the right side of the page.
4) **Optional:** Choose one group, then click **+Add** on the right to add more group members. Select and click **OK**.

3. Add Multi-Factor Authentication Rule.
1) Click **+Add** at the interface of Multi-Factor Authentication.
2) Set Facial Recognition Parameters.

Multi-Factor Authentication Name

Enter Multi-Factor Authentication Name.

Access Point

Select access point which needs multi-factor authentication from the drop-down list.

Authentication Mode

Local Authentication

Persons can open the door only after they complete authentications following rules on the card reader.

Local Authentication + Remotely Opening Door

Persons should authenticate on the device first and the authentication will be confirmed remotely on client.

Local Authentication + Super Credential

Authenticate on the card reader. If the card reader is offline, authenticate by super credential.

Access Schedule

Select access schedule which need multi-factor authentication. Click **View Licenses** to check the chosen schedule template in details.

Time Interval of Card Present

Time interval between configuration for two different persons.

Group

Click **Link to Organization** to choose the group. Adjust the sequence of the chosen groups by dragging ☰ in the action bar. Before opening the door, please refer to sequence in the list and **No.** of people needed to be verified to do actual verification.

3) **OK**.

4. **Optional:** Select multi-factor authentication not needed, then click **Delete**.
5. Click 🗎 to check access schedule in details.

Multi-Door Interlocking Settings

Set the multi-door interlocking between multiple doors of the same access control device. To open one of the doors, other doors must keep closed.

Steps

1. Click **Access Control → Access Control Application → Multi-Door Interlocking → Set**.

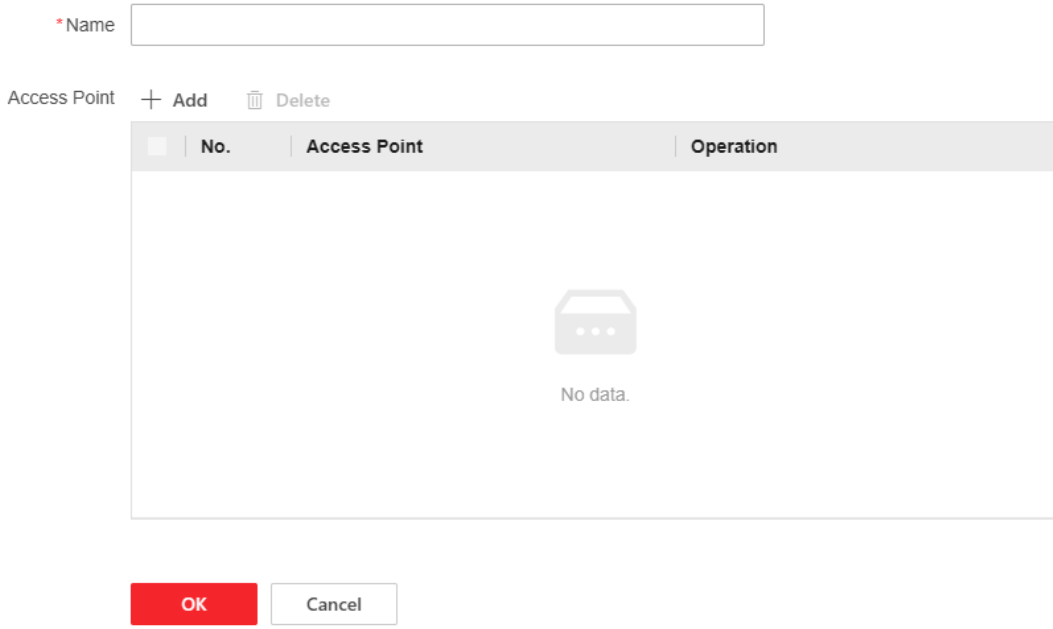


Figure 7-6 Multi-Door Interlocking Settings

2. Enter Name.
3. Click **+Add**, select access point to form a multi-door interlocking group.
4. It is recommended to delete unnecessary access point in the area.
   - Select access points not needed. Click **Delete** to delete in batches.
   - Click to delete single access point.
5. Click **OK**.
6. To edit or delete existing multi-door interlock.
   - Select one multi-door interlock. Click to edit.
   - Select one multi-door interlock. Click to delete.
   - Select multiple multi-door interlocks. Click **Delete** to delete in batches.

Anti-Passback Settings

People can only pass through access points according to the set sequence. If not followed the set path, the door will not open. If one swipe card without going through, he or she will be blocked the next time she or she wants to come in. Vise versa.

Steps

1. Click **Access Control → Access Control Application → Anti-Passback**.

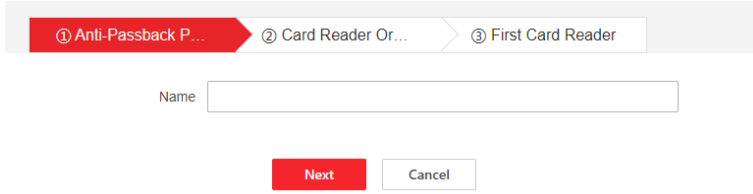


Figure 7-7 Anti-Passback Settings

2. Add Anti-Passback Route.
   1) Enter name of Anti-Passback Parameter. Click **Next**.
   2) Card reader Order. Click **Add**. Select a card reader needed.
   3) Click ⊕ to add the next card reader.
   4) Repeat sub step 3 to add more card readers.
   5) **Optional:** Click card reader to replace or delete.
   6) Click **Next Step**.
   7) First Card Reader

      Disable

      - If the card reader one pass through last time doesn't have anti-passback, or the person is a new user. Anti-passback access granted.
      - If the card reader one pass through last time have anti-passback and the current card reader is its subsequent card reader in its anti-passback route, anti-passback access granted; if the current card reader is not its subsequent card reader, anti-passback access denied.

      Select one card reader as the First Card Reader

      - Access granted whenever a person swipe his or her card at the First Card Reader
      - If the card reader one pass through last time have anti-passback and the current card reader is its subsequent card reader in its anti-passback route, anti-passback access granted; if the current card reader is not its subsequent card reader, anti-passback access denied.

Note

- If you violated the anti-passback rule, you should swipe the card again from the first card reader.
- Superusers are exceptions.
- Anti-passback route can have maximum 64 doors.

3. **Optional:** Anti-Passback Parameter
   1) Click **Anti-Passback Parameter**.
   2) Enable **Forgive Anti-Passback** to configure schedule.

      Forgiving Mode

      Forgive Anti-Passback Regularly

Set time of **Forgive Anti-Passback Regularly**. The system will forgive anti-passback. Then person need to follow the anti-passback route to start from the the First Card Reader.

Delay Forgiving Anti-Passback

Set time of **Delay Forgive Anti-Passback**. The system will start timing and forgive anti-passback once reach the set delayed time. Then you should follow the anti-passback rule and start again from the first card reader.

Non Anti-Passback Period

Select **Effective Time**, then drag cursor on the time bar to map non anti-passback period. Anti-passback is invalid during the chosen period.

Click **Clear** and drag your cursor on the timestamp to delete certain time period.

Click ··· → **Clear All** to delete all time period chosen.

3) Click **Save**.

4. To edit or delete existing anti-passback.

- Select one anti-passback. Click to edit.
- Select one anti-passback. Click to delete.
- Select multiple anti-passbacks. Click **delete** to delete in batches.
- Select one anti-passback. Click to view anti-passback route.

Set Remain Open or Closed

Set the time period by week during which the door(s) remains locked/unlocked.

Steps

1. Click **Access Control → Access Control Application → Remain Open or Closed\ → Set**.

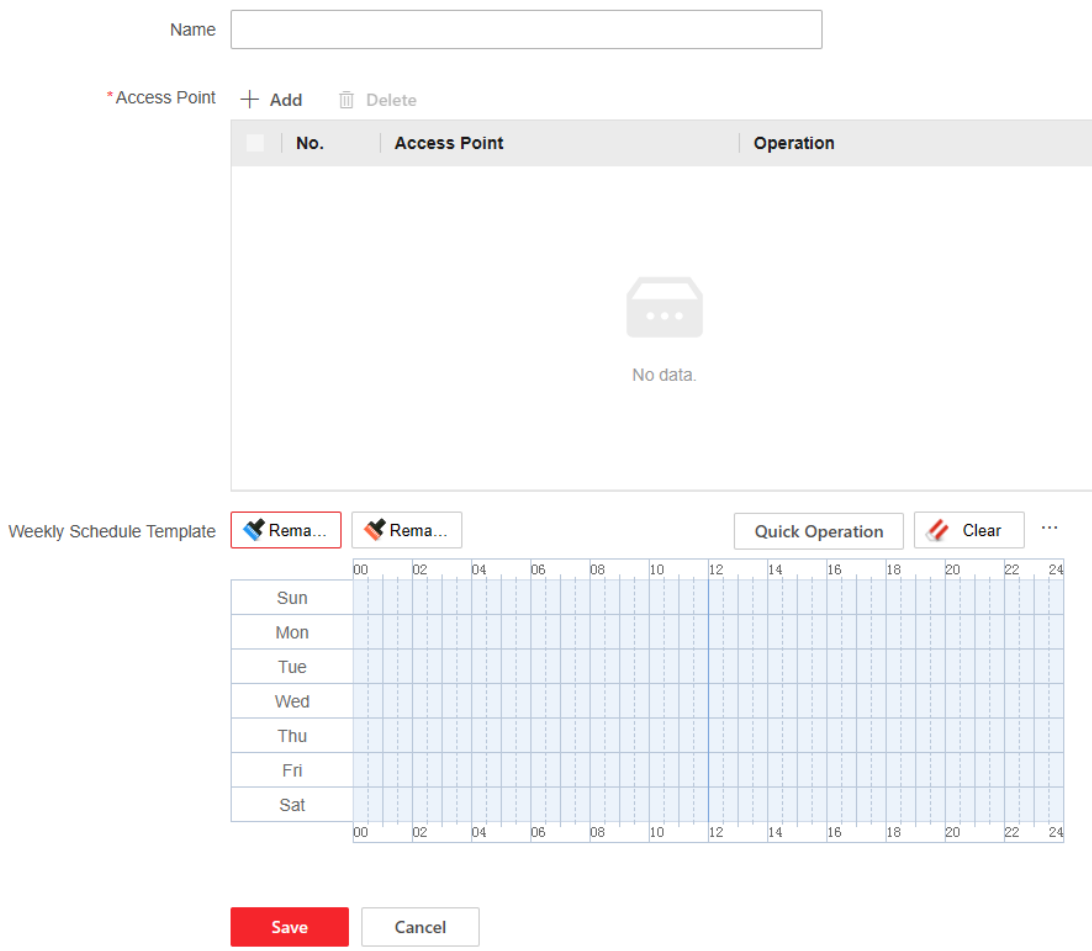


Figure 7-8 Remain Open or Closed

2. Click **+Add**.
3. Add Access Point.
   1) Click **+Add**.
   2) Select access point in the pop-up on the right. Click **OK**.
   3) Click to delete single access point or select multiple access points and then click **Delete** to delete in batches.
4. Weekly Schedule Template.
   1) Map the Remain Open or Closed time period.
   - Click **Remain open** or **Remain Closed**. Drag cursor on the timestamp to map the time period needed.
   - Click **Remain Open** or **Remain Closed**, then click **Quick Operation**. Choose **All-Day Schedule**, **Workday Schedule** or **Weekend Schedule**. The system will automatically draw the corresponding time period.

   1) **Optional:** Click **Clear** and drag your cursor on the timestamp to delete certain time period. Click ··· → **Clear All** to delete all time period chosen.

5. Click **Save**.

7.10.5 Door Parameter Configuration

Configure parameters for unlocking doors.

Select Door No.

Select a door to configure relative parameters.

Click **Access Control → Parameter Settings → Door Parameters** to enter the settings page.

Select **Door No.**. Usually, Door 1 is the door linked with the device and door 2 is the door linked with the secure door control unit.

Set other door parameters and click **Save**.

View Device Online Status

View and refresh the device status.

Click **Access Control → Parameter Settings → Door Parameters** to enter the settings page.

You can view the online status of the device. Click **Refresh** to refresh the status of the device.

Set Door Name

Create door name.

Click **Access Control → Parameter Settings → Door Parameters** to enter the settings page.

Set **Door Name** and click **Save**.

Set Open Duration via PC Web

You can set the time for the door lock to open after swiping the card.

Click **Access Control → Parameter Settings → Door Parameters** to enter the settings page.

Set the open duration, that is the action time after the door is unlocked. If the door is not opened within the set time, the door will automatically lock. Configurable time: 1 to 255 seconds.

Click **Save**.

Set Door Open Timeout Alarm via PC Web

If the door is not closed after reaching the lock action time, the access control point will sound an alarm.

Click **Access Control → Parameter Settings → Door Parameters** to enter the settings page.

Set **Door Open Timeout Alarm**. If the door is not closed after reaching the lock action time, the access control point will sound an alarm. When set as 0, alarm will not be enabled.

Click **Save**.

Set Door Lock Status via Web Page

Select door contact's status according to the door contact's wiring method.

Click **Access Control → Parameter Settings → Door Parameters**.

You can select Remain Open or Remain Closed according to your actual needs. By default, it is Remain Closed.

Click **Save**.

Set Passing Detection

If the function is enabled and door is not pushed open within unlocking duration, the event will be recorded as Passing Allowed (Door Not Used).

Click **Access Control → Parameter Settings → Door Parameters** to enter the settings page.

Enable **Passing Detection**.

Click **Save**.

Set Lock Door when Door Closed

If the function is enabled and door will be locked when door closed.

Click **Access Control → Parameter Settings → Door Parameters** to enter the settings page.

Enable **Lock Door when Door Closed**.

Click **Save**.

Set Exit Button via PC Web

Set the exit button as remain open or remain closed according to the actual wiring method.

Click **Access Control → Parameter Settings → Door Parameters** to enter the settings page.

Set **Exit Button Type**. By default, it is Remain Open (excluding special needs).

Click **Save**.

Set Extended Open Duration via PC Web

The door contact can be enabled with appropriate delay after person with extended access needs swipes her/his card.

Click **Access Control → Parameter Settings → Door Parameters** to enter the settings page.

Set **Extended Open Duration**. The door contact can be enabled with appropriate delay after person with extended access needs swipes her/his card.

Click **Save**.

Set Door Remain Open Duration with First Person via PC Web

After the first person is authorized, it allows multiple persons access the door or other authentication actions.

Click **Access Control → Parameter Settings → Door Parameters** to enter the settings page.

Set the door open duration when first person is in and click **Save**.

Set Duress Code via PC Web

After configuring duress code, when encountering duress, enter the code to open the door. At the same time, the access control system will report duress events.

Click **Access Control → Parameter Settings → Door Parameters** to enter the settings page.

Set duress code, and click **Save**.

Note

Duress code and super password can't be duplicated, usually consisting of 4 to 8 digits.

Set Super Password via PC Web

Administrator or designated person can enter the super password to open the door.

Click **Access Control → Parameter Settings → Door Parameters** to enter the settings page.

Set **Super Password**, the designated person can enter the super password to open the door.

Click **Save**.

Note

Duress code and super password can't be duplicated, usually consisting of 4 to 8 digits.

Set Dismiss Code via PC Web

The administrator or specified person can enter the dismiss code to dismiss the alarm.

Click **Access Control → Parameter Settings → Door Parameters**.

Create a **Dismiss Code**. When an alarm is triggered, you can enter the dismiss code to dismiss the alarm.

Click **Save**.

7.10.6 Card Reader Parameter Configuration

Set authentication parameter of the card reader based on real requirement.

Click **Access Control → Parameter Settings → Authentication Settings**. Select the card reader to finish configuration.

Tap **Save**. Click **Copy to** to copy the card reader's parameters to other card readers.

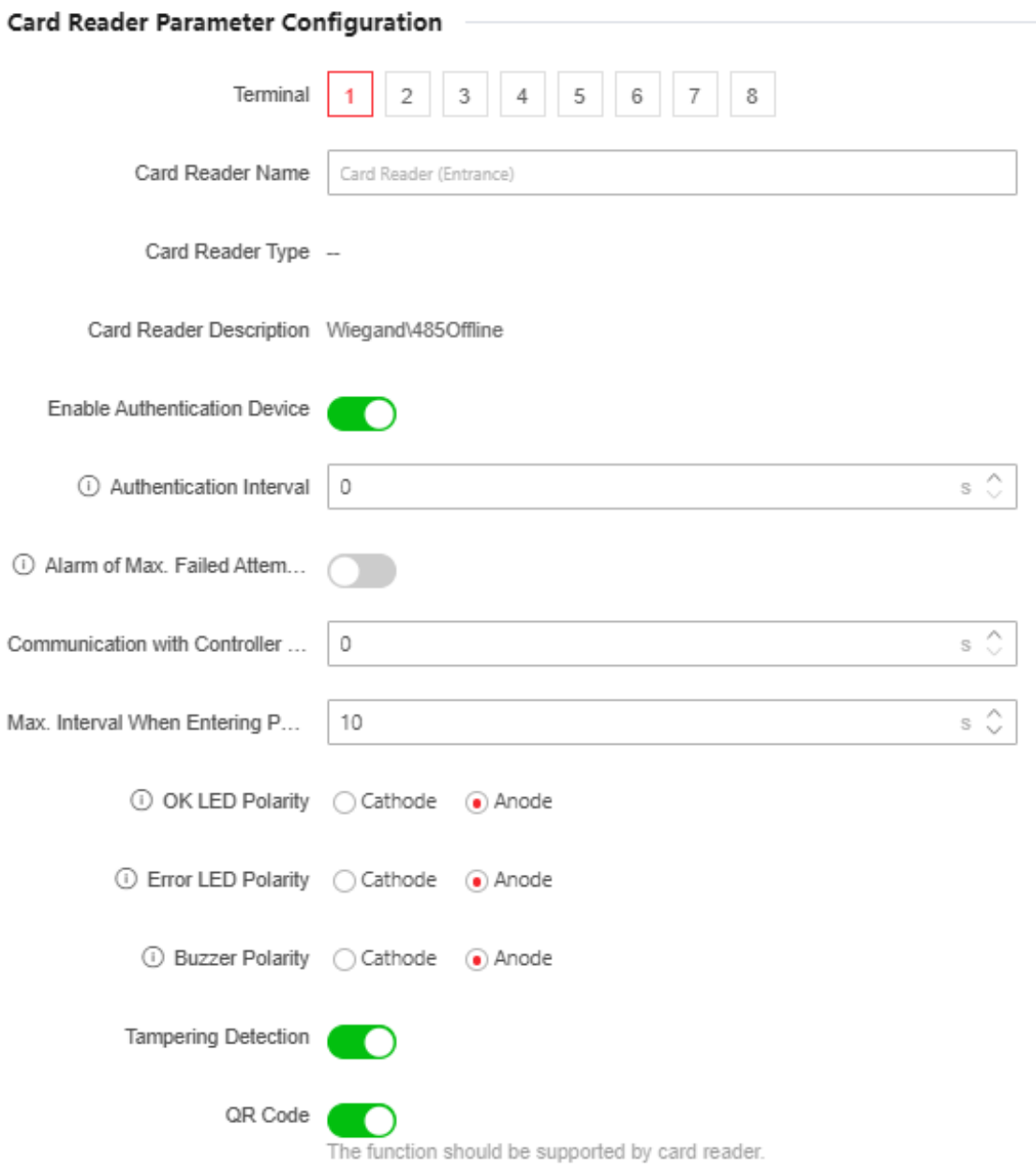


Figure 7-9 Authentication Parameter Configuration

Card Reader Parameter Configuration

Terminal

Select the No. of the card reader and configure the authentication parameter of it. After saving, the user can choose other No. for configuration.

Note

The No. here will be used as the dial address of RS-485. Select No. based on the dial address of the card reader.

Card Reader Name

Name the card reader.

Card Reader Type/ Description

Card Reader Description available.

Enable Authentication Device

Enable this function will enable the authentication device to work normally; vise versa.

Authentication Interval

The interval period of a person who pass the configured interval twice during the authentication. The same person can only authenticate once in the configured interval. If others authenticate during the configured interval, then the person can reauthenticate.

Alarm of Max. Failed Attempts

Enable **Alarm of Max. Failed Attempts** to configure Max. Authentication Failed Attempts. The device would report alarm when the failed attempts reach the set value.

Buzzer Polarity

Click **Access Control → Parameter Settings → Authentication Settings** to enter the settings page. Set **Buzzer Polarity**.

Note

The polarity is Anode in default.

Communication with Controller Every

If the card reader fail to contact the access controller during the set time, then card reader is disconnected.

Max. Interval When Entering Password

Set the maximum interval of entering two characters of the password. After entering one character, if the next character is not entered within the set interval, the entered characters will all be automatically cleared.

OK LED Polarity/ Error LED Polarity/ Buzzer Polarity

Select the polarity by actual demands.

Tampering Detection

The card reader will report lid opened alarm if the card reader is removed. Disable this feature to stop the alarm report.

QR Code

Enable this feature allows authentication via scanning the QR code.

Bluetooth Parameter Configuration

Enable Bluetooth

Start using bluetooth function.

Device Name/ Transmitting Power

The name and emissivity of the connected device can be edited.

Open Door via Bluetooth

Use Mobile Client to open door via bluetooth. Add the device to Mobile Client (property) to open door via bluetooth remotely. Once the property issues device permission, individuals can use Mobile Client (personal) to open door via bluetooth.

Open Door via Gesture Occlusion/Occlusion Times/Occlusion Detection Distance

After enabling, you can open door via gesture. You need set **Occlusion Times**and **Occlusion Detection Distance**.

Note

Continuously occluding detector is not allowed. The duration of each occlusion can not exceed 5 seconds.

Authentication Plan Configuration

Choose **Authentication Plan**. Place and drag the mouse on the timestamp to select valid authentication time. Click **Clear**, then drag your cursor. The overlapping part can be erased. Click ··· → **Clear All** to delete all time period chosen.

7.10.7 Set Facial Recognition Parameters

Set Facial Recognition Parameters.

Click **Access Control → Parameter Settings → Smart Settings** to enter the settings page.

Note

- Different models support different parameters. Please refer to the actual interface.
- Use general parameter configuration for the access controller. All card readers become effective after configuration.

Click **Save**.

Card reader

Select the No. of the card reader and configure the authentication parameter of it. After saving, the user can choose other No. for configuration.

Note

The No. here will be used as the dial address of RS-485. Select No. based on the dial address of the card reader.

Fingerprint Security Level

Fingerprint security level configuration. The higher the security level, the lower the False Acceptance Rate; the higher the False Rejection Rate.

Note

Only device with fingerprint module supports the fingerprint functions.

7.10.8 Card Settings

Enable/Disable NFC Protection via PC Web

After enabling, the device can read NFC card.

Click **Access Control → Parameter Settings → Card Settings** to enter the settings page.

Click to **Enable NFC Card** and click **Save**. After enabling, the device can read NFC card. If the data of access control devices is obtained by mobile devices, the situation of unauthenticated access may occur. To prevent this situation, you can disable NFC function.

Enable/Disable M1 Card via Web Client

After enabling, the device can recognize M1 card and users can swipe M1 card via the device.

Click **Access Control → Parameter Settings → Card Settings** to enter the settings page.

Click to **Enable M1 Card**.

M1 Card Encryption

Enable M1 Card Encryption can improve the security level of the entrance card. Therefore, the entrance card will be harder to be copied.

Sector

After enabling M1 Card Encryption, you will need to set the encrypted sector.

Note

You are advised to encrypt sector 13.

Click **Save**.

Enable/Disable EM Card via Web Client

After enabling, the device can recognize EM card and users can swipe EM card via the device.

Click **Access Control → Parameter Settings → Card Settings** to enter the settings page.

Click to **Enable EM Card** and click **Save**.

Note

If the peripheral card reader which can read EM card is connected, after enabling this function, you can also swipe EM card via this card reader.

Set DESFire Card

You can enable DESFire card and DESFire card read content.

Click **Parameter Settings → Card Settings** to enter the settings page.

Select **Enable DESFire Card** and **DESFire Card Read Content**and click **Save**.

Set FeliCa Card

You can enable FeliCa card.

Click **Parameter Settings → Card Settings** to enter the settings page.

Select **Enable FeliCa Card**.

Configure Card Authentication Mode via Web Browser

You can set the card number content that the device reads when authenticating by card number.

Click **Parameter Settings → Card Settings** to enter the settings page.

Select card authentication mode and click **Save**.

Full Card No.

All card No. will be read.

3 Byte

The device only read 3 bytes.

4 Byte

The device only read 4 bytes.

7.10.9 Event and Detection

When detected event is triggered, upload event information to the platform following the configuration.

Steps

1. Click **Access Control → Parameter Settings → Linkage Settings**.
2. Click **+**.
3. Event Source Configuration. Select from **Event Linkage**、 **Card linkage** or **Link Employee ID**.
   - Select **Event Linkage** from **Linkage Type**. Make selection based on your actual demands.

     Note

     If choose **Card Reader Event**, then you need to choose card reader.
   - If choose choose **Linkage Type** as **Card linkage**. You need to fill in **Card No.** and choose **Card Reader**.
   - If choose choose **Linkage Type** as **Link Employee ID**. You need to fill in **Link Employee ID** and choose **Card Reader**.
4. Set Linkage Action. The following actions are linkage actions of the previous events.

   Linked Access Controller Buzzing

   Select **Start Buzzing** or **Stop Buzzing**.

   Door Linkage

   After enabled, select linked door. Choose the action of door as **Unlock**, **Closed**,**Remain Open** or **Remain Closed**.

   Linked Alarm Output

   If the event source is **Card Linkage**. After enabling Linked Alarm Output, you can set it action as **Open** or **Disable**.

   Triggering Times Configuration

   If the event source is **Card Linkage**. After enabling Linked Alarm Output, you can choose to enable **Triggering Times Configuration** and set it as **Triggering Times (Enable)** or **Triggering Times (Disable)**.

   If set **Triggering Times (Enable)** as 3, **Triggering Times (Disable)** as 3. Then you can swipe your card 3 times to open/ disable the Linked Alarm Output.

   Note

   The configured alarm length will be applied to all the Linked Alarm output.
5. Click **Save** to enable the settings.
6. If you want to map the device linkage mode of a module to other modules, you can click **Copy To**, select or enter a device name, and click **OK**.

7.10.10 Privacy Settings

Event storage Settings.

Note

Different models support different functions, please refer to the specific device.

Click **Access Control → Parameter Settings → Privacy Settings** .

Choose from **Delete Old Event Periodically**, **Delete Old Event by Specified Time** or **Overwrite**.

Delete Old Events Periodically

Drag the slider to choose or you can enter the duration in the box directly. All events will be deleted according to the set duration.

Delete Old Events by Specified Time

All events will be deleted on the specified time chosen.

Overwrite

The earliest 5% events will be deleted when the system detects the stored events has been over 95% of the full space.

Set Event Storage Type via PC Web Browser

You can configure the event storage type.

Click **Access Control → Parameter Settings → Privacy Settings** to enter the settings page.

You can select **Event Storage Type** as **Delete Old Events Periodically**, **Delete Old Events by Specified Time** or **Overwriting**.

Delete Old Events Periodically

Drag the block or enter number to set the period for event deleting. All events will be deleted according to the configured time duration.

Delete Old Events by Specified Time

Set a time and all events will be deleted on the configured time.

Overwriting

The earliest 5% events will be deleted when the system detects the stored events has been over 95% of the full space.

Click **Save**.

Set PIN Mode via PC Web

Make sure the PIN is platform-applied personal PIN or device-set personal PIN before settings. If the PIN is device-set personal PIN, you can edit the PIN on the device or PC Web, but not set it on

the platform. If the PIN is platform-applied personal PIN, you should set the PIN on the platform, but not on the device or PC Web.

Go to **Access Control → Parameter Settings → Privacy Settings**.

In the PIN Mode module, you can set the following parameters. Click **Save** after parameters settings.

Platform-Applied Personal PIN

You can create the person PIN on the platform. You should apply the PIN to the device. You cannot create or edit the PIN on the device or PC Web.

Device-Set Personal PIN

You can create or edit the PIN on the device or PC Web. You cannot set the PIN on the platform.

Click **Save**.

7.11 System Configuration

7.11.1 View Device Information

View the device name, language, model, serial No., version, RS-485, alarm output, and device capacity, etc.

Click **System and Maintenance → System Configuration → System → System Settings → Basic Information** to enter the configuration page.

You can the device name, language, model, serial No., version, RS-485, alarm output, and device capacity, etc.

7.11.2 Set Time

Set the device's time zone, synchronization mode, server address, NTP port, and interval.

Click **System and Maintenance → System Configuration → System → System Settings → Time Settings** .

Click **Save** to save the settings after the configuration.

Time Zone

Select the device located time zone from the drop-down list.

Time Synchronization Mode

NTP

You should set the NTP server's IP address, port No., and interval.

Manual

By default, the device time should be synchronized manually. You can set the device time manually or check **Sync. with Computer Time** to synchronize the device time with the computer's time.

Server IP Address/NTP Port/Interval

You can set the server IP address, NTP port, and interval.

7.11.3 Change Administrator's Password

Steps

1. Click **System and Maintenance → System Configuration → System → User Management** .
2. Click .
3. Enter the old password and create a new password.
4. Confirm the new password.
5. Click **Save**.

Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.
Proper configuration of all passwords and other security settings is the responsibility of the service provider and/or end-user.

7.11.4 Account Security Settings

You can change the security questions and answers, or the email address for the device. After change the settings, once you forgot the device password, you should answer the new questions or use the new email address to reset the device password.

Steps

1. Click **System and Maintenance → System Configuration → System → User Management → Account Security Settings** .
2. Change the security questions or email address according your actual needs.
3. Enter the device password and click **OK** to confirm changing.

7.11.5 View Device Arming/Disarming Information

View device arming type and arming IP address.

Go to **System and Maintenance → System Configuration → System → User Management → Arming/Disarming Information** .

You can view the device arming/disarming information. Click **Refresh** to refresh the page.

7.11.6 Network Settings

Set Basic Network Parameters

Click **Configuration → Network → Network Settings → TCP/IP** .

Set the parameters and click **Save** to save the settings.

NIC Type

Select a NIC type from the drop-down list.

DHCP

If uncheck the function, you should set the IPv4 address, IPv4 subnet mask, IPv4 default gateway, IPv6 mode, IPv6 address, IPv6 subnet prefix length, IPv6 default gateway, Mac address, and MTU.

If you check the function, the system will allocate the IPv4 address, IPv4 subnet mask, the IPv4 default gateway, IPv6 mode, IPv6 address, IPv6 subnet prefix length, and IPv6 default gateway automatically.

DNS Server

Set the preferred DNS server and the Alternate DNS server according to your actual need.

Set Wi-Fi Parameters

Set the Wi-Fi parameters for device wireless connection.

Steps

Note

The function should be supported by the device.

1. Click **System and Maintenance → System Configuration → Network → Network Settings → Wi-Fi** .
2. Check **Wi-Fi**.
3. Select a Wi-Fi
   - Click of a Wi-Fi in the list and enter the Wi-Fi password.
   - Click **Add** and enter a Wi-Fi's name, password, and encryption type. Click **Connect**. When the Wi-Fi is connected, click **OK**.
4. **Optional:** Set the WLAN parameters.

1) Set the IP address, subnet mask, and default gateway. Or enable **DHCP** and the system will allocate the IP address, subnet mask, and default gateway automatically.

5. Click **Save**.

Set Port Parameters

Set the HTTP, HTTPS, HTTP Listening, RTSP and Server port parameters.

Click **System and Maintenance → System Configuration → Network → Network Service → HTTP(S)** .

HTTP

It refers to the port through which the browser accesses the device. For example, when the HTTP Port is modified to 81, you need to enter ***http://192.0.0.65:81*** in the browser for login.

HTTPS

Set the HTTPS for accessing the browser. Certificate is required when accessing.

HTTP Listening

The device can send alarm information to the event alarm IP address or domain name via HTTP protocol/HTTPS protocol. Edit the event alarm IP address or domain name, URL, port, and protocol.

Note

The event alarm IP address or domain name should support the HTTP protocol/HTTPS protocol to receive the alarm information.

Click **System and Maintenance → System Configuration → Network → Network Service → WebSocket(s)** .

View WebSocket and WebSockets port.

Enable/Disable HTTP

Enable the HTTP function to improve the broswer's visiting security.

Go to **System and Maintenance → System Configuration → Network → Network Service → HTTP(S)** .

Click**Save** after parameters are configured.

HTTP Port

When you log in with a browser, you need to add the modified port number after the address. For example, when the HTTP port number is changed to 81, you need to enter http://192.0.0.65：81 when you log in with a browser.

HTTPS Port

Set the HTTPS port for visiting browser. But certification is required.

HTTP Listening

The device will send the alarm information to the destination IP or domain name by HTTP protocol. The destination IP or domain name should support HTTP protocol. Enter the destination IP or domain name, URL and port. And select the protocol type.

View RTSP Port via PC Web

The RTSP port is the port of real-time streaming protocol.

Go to **System and Maintenance → System Configuration → Network → Network Service → RTSP** .
View the Port.

Set WebSocket(s) via PC Web

View WebSocket and WebSockets port.

Go to **System and Maintenance → System Configuration → Network → Network Service → WebSocket(s)** .
View WebSocket and WebSockets port.

SDK Service Settings

Set the SDK server port.

Steps

1. Go to **System and Maintenance → System Configuration → Network → Device Access → SDK Server**.
2. Set the SDK server port.
3. Click**Save**to enable the settings.

Set ISUP Parameters

Set the ISUP parameters for accessing device via ISUP protocol.

Steps

Note

The function should be supported by the device.

1. Click **System and Maintenance → System Configuration → Network → Device Access → ISUP** .

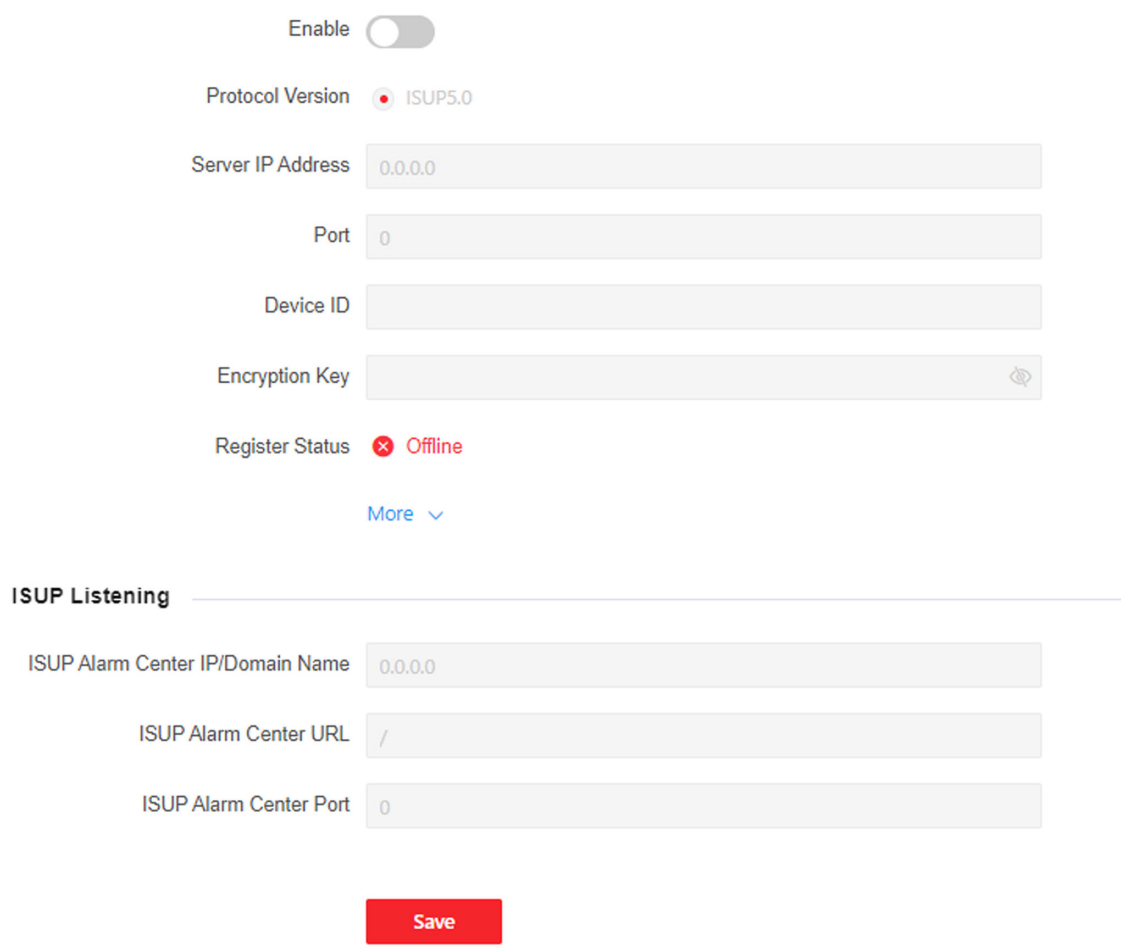


Figure 7-10 Set ISUP Parameters

2. Check **Enable**.
3. View the ISUP version, set server IP address, port, device ID, encryption key and view the ISUP status.
4. **Optional:** Click **More** to set the network connection priority.
   1) Enable **WLAN** or **Wired Network** according to your actual needs.
   1) Hold and drag ☰ to adjust the access priority.
5. Set the ISUP listening parameters, including ISUP alarm center IP address/domain name, ISUP alarm center URL, and ISUP alarm center port.
6. Click **Save**.

Platform Access

Platform access provides you an option to manage the devices via platform.

Steps

1. Click **System and Maintenance → System Configuration → Network → Device Access → Hik-Connect** to enter the settings page.

   Note

   Hik-Connect is an application for mobile devices. With the App, you can view live image of the device, receive alarm notification and so on.

2. Check **Enable** to enable the function.
3. **Optional:** Check **Custom**, and you can set the server address by yourself.
4. Enter the verification code.
5. **Optional:** View the register status. Click **Refresh** to refresh the status.
6. **Optional:** Click **More** to set the network connection priority.
   1) Enable **WLAN** or **Wired Network** according to your actual needs.
   1) Hold and drag ☰ to adjust the access priority.
7. Click **View** to view device QR code. Scan the QR code to bind the account.

   Note

   8 to 32 letters (a to z, A to Z) or numbers (0 to 9), case sensitive. You are recommended to use a combination of no less than 8 letters or numbers.

8. Click **Save** to enable the settings.
9. **Optional:** Click **Refresh** to refresh the binding status.
10. Click **Save**.

7.11.7 Alarm Settings via PC Web

Set the alarm output parameters.

Steps

1. Click **System and Maintenance → System Configuration → Event → Alarm Settings → Alarm Output** .
2. Set **Alarm Name** and mode of **Alarm Duration**.

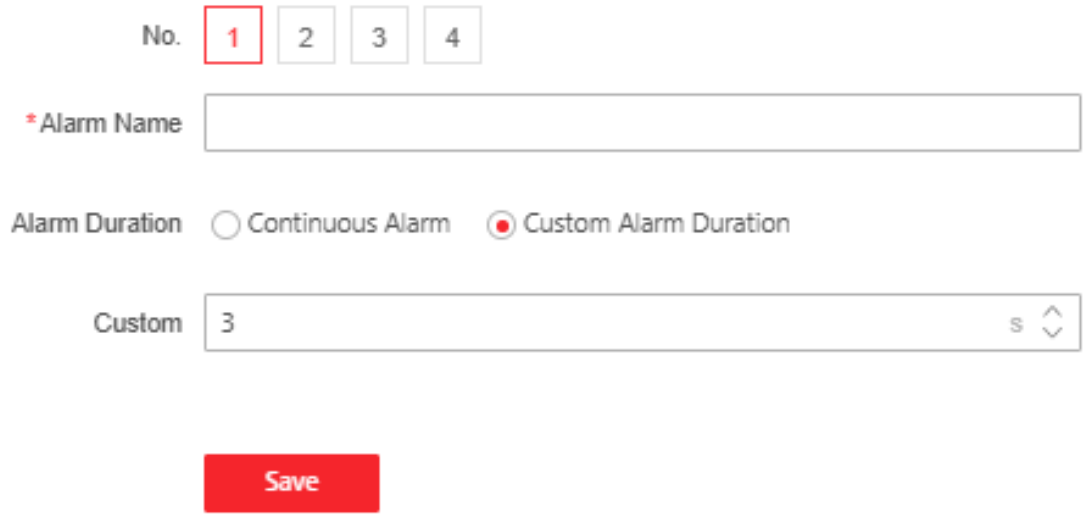


Figure 7-11 Alarm Settings

Continuous Alarm

When the alarm is triggered, it will alarm continuously.

Custom Alarm Duration

You can set **Alarm Duration** for the device when the alarm is triggered.

7.11.8 Alarm Input Settings

Set the device's alarm input parameters.

Click **System and Maintenance → System Configuration → Event → Alarm Settings → Alarm Input** .

Select the device, set No. and name. Click **Save**.

7.11.9 Access Configuration

RS-485 Configuration Parameters

RS-485 Configuration Parameters.

Click **System and Maintenance → System Configuration → Device Access → RS-485**, go to Configuration page.

Tap **Save**.

RS-485 Communication Backup

After enabled, the access controller and access module will communicate via double lines wiring methods.

RS-485 Protocol

Choose a partition from the drop-down list.

No.

Select the serial port No. of the card reader based on the tag reader configured.

Peripheral Type

Select peripheral type.

Baud Rate

Check baud rate when using RS-485 to communicate.

Serial Port Name

Check the name of physics serial port of the card reader used.

Set Wiegand Parameters

You can set the Wiegand transmission direction.

Steps

Note

Some device models do not support this function. Refer to the actual products when configuration.

1. Click **System and Maintenance → System Configuration → Access Configuration → Wiegand Settings** .
2. Select a access point from the list on the left.
3. Set Wiegand parameters.

   No.

   Select Wiegand No. for parameters settings.

   Wiegand

   select to enable the card reader's Wiegand function.

   Wiegand Direction

   By default, the direction is **Input**.

   Wiegand Mode

   Select the Wiegand mode and the card reader can communicate with the controller by Wiegand 26/34 or other protocol.

   Click **Auto Recognize**, enter card No. to recognize the Wiegand mode. Enter the Card No., and click **Start to Recognize**. Present the card on the related card reader. The system will show the Wiegand mode. Click **OK**.

If select **Custom**, you should set custom Wiegand parameters. Click **Custom Wiegand Settings**, and set the name, parity type, total length and Wiegand rule. Click **OK**.

Wiegand Mapping Card Reader

Select the Wiegand card reader related door and card reader direction.

4. Click **Save** to save the settings.

Note

If you change the peripheral, and after you save the device parameters, the device will reboot automatically.

Door Magnetic Contact Settings

Set the opening and closing door status of the door magnetic contact to match the actual wiring method.

Before You Start

The access controller has connected to the door magnetic contact.

Steps

1. Click **System and Maintenance → Maintenance → Device Access → Host Parameter** to enter the settings page.
2. Select the door magnetic contact status.

Barrier Open Status (Default)

The door magnetic contact is in open status in default. Access controller is connected to the door magnet contact through NO.

Door Closed Status

The door magnetic contact is in closed status in default. Access controller is connected to the door magnet contact through NC.

7.12 Maintenance and Security

7.12.1 Upgrade and Maintenance

Reboot device, restore device parameters, and upgrade device version.

Reboot Device

Click **System and Maintenance → Maintenance → Host** .
Click **Restart** to reboot the device.

Reboot Sub Device

Click **System and Maintenance → Maintenance → Sub-Device** .

Set the device, and click **Restart**.

Upgrade

Click **System and Maintenance → Maintenance → Upgrade** .
Select an upgrade type from the drop-down list. Click and select the upgrade file from your local PC. Click **Upgrade** to start upgrading.
If the device has been connected to Hik-Connect and network, when there is a new installation package in Hik-Connect, you can click **Upgrade** after Online Update to upgrade the device system.

Note

Do not power off during the upgrading.

Sub Device Upgrade

Click **System and Maintenance → Maintenance → Upgrade** .
Select an upgrade type from the drop-down list. Click and select the upgrade file from your local PC and click **Next**. Click **Upgrade** to start upgrading.

Restore Parameters

Click **System and Maintenance → Maintenance → Backup and Reset → Host** .

Restore All

All parameters will be restored to the factory settings. You should activate the device before usage.

Restore

The device will restore to the default settings, except for the device IP address and the user information.

Restore Sub-Device Parameters

Click **System and Maintenance → Maintenance → Backup and Reset → Sub-Device** .
Select the device, and click **Restore to Factory Settings**.

Import and Export Parameters

Click **System and Maintenance → Maintenance → Backup and Reset** .

Export

Click **Export** to export the device parameters.

Note

You can import the exported device parameters to another device.

Import

Click and select the file to import. Click **Import** to start import configuration file.

7.12.2 View Exception Diagnosis

Click **System and Maintenance → Maintenance → Exception Diagnosis** to enter the settings page.
You can view the exception diagnosis.

7.12.3 Device Debugging

You can set device debugging parameters.

Steps

1. Click **System and Maintenance → Maintenance → Device Debugging** .
2. You can set the following parameters.

Enable SSH

To raise network security, disable SSH service. The configuration is only used to debug the device for the professionals. You can click **Debug** to debug SSH.

Capture Network Packet

You can set the **Capture Packet Duration**, **Capture Packet Size**, and click **Start** to capture.

Enable/Disable SSH via Web Browser

You can enable SSH to perform remote debugging.

Click **System and Maintenance → Maintenance → Device Debugging → Log for Debugging**.

Enable SSH

SSH is used for remote debugging. When you don't need to use this service, it's recommended to disable SSH to improve security.

Print Device Log via PC Web

You can print out the device log.

Click **System and Maintenance → Maintenance → Log** to enter the settings page.
Click**Export** to print out the device log.

Capture Network Packet via PC Web

Set the capture packet duration and size and start caputre. You can view the log and debug according to the capture result.

Go to **System and Maintenance → Maintenance → Device Debugging → Log for Debugging** .
Set **Capture Packet Duration**,**Capture Packet Size**, and click **Start Capture**.

Test Protocol via PC Web

Select a protocol address, and enter the protocol to test. You can debug the device according to the response header and returned value.

Go to **System and Maintenance → Maintenance → Device Debugging → Protocol Testing**.

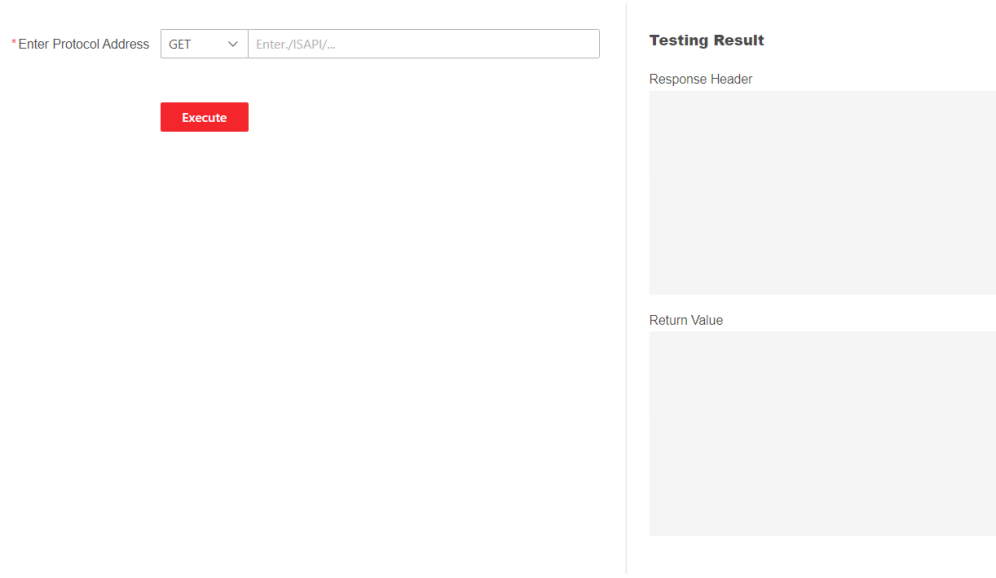


Figure 7-12 Protocol Testing

Select a protocol address, and enter the protocol. Click **Execute**.

Debug the device according to the response header and returned value.

Set Network Diagnosis

Enter the device IP address or domain name, you can perform PING settings. Debug the network according to the PING result.

Go to **Maintenance and Security → Maintenance → Network Diagnosis** .

Enter the device IP for PING operation, select the network connection mode, PING duration, and Ping data package size (default parameter is recommended.) Click **Diagnose**. The result will displayed in **PING Result**.

Set Network Penetration Service via PC Web

When the devcie is deployed in the LAN, you can enable the penetration service to realize device remote management.

Steps

1. Go to **System and Maintenance → Maintenance → Device Debugging → Network Penetration Service**.
2. Slide **Enable Penetration Service**.
3. Set **Server IP Address** and **Server Port**. Create **User Name** and **Password**.
4. **Optional:** You can set **Heartbeat Timeout**. The value range is 1 to 6000.
5. **Optional:** You can view the status of the penetration service. Click **Refresh** to refresh the status.
6. Click **Save**.

Note

The penetration service will auto disabled after 48 h.

7.12.4 Log Query

You can search and view the device logs.

Go to **System and Maintenance → Maintenance → Log** .

Set the major and minor type of the log type. Set the start time and end time for searching, and click **Search**.

The results will be displayed below, which including the No., time, the major type the minor type, the channel No., the local/remote user information, the remote host IP, etc.

7.12.5 Test Protocol via PC Web

Select a protocol address, and enter the protocol to test. You can debug the device according to the response header and returned value.

Go to **System and Maintenance → Maintenance → Device Debugging → Protocol Testing**.

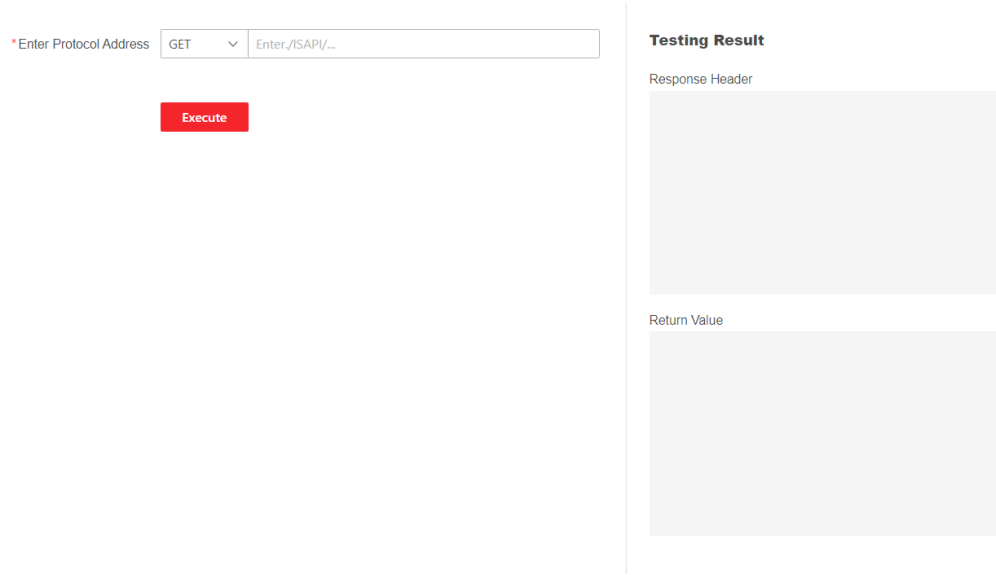


Figure 7-13 Protocol Testing

Select a protocol address, and enter the protocol. Click **Execute**.

Debug the device according to the response header and returned value.

7.12.6 Certificate Management

It helps to manage the server/client certificates and CA certificate.

Note

The function is only supported by certain device models.

Create and Import HTTPS Certificate

Steps

1. Go to **Maintenance and Security → Security → Certificate Management** .
2. In the **HTTPS Certificate** area, click **Create Certificate Request**.
3. Input certificate information and click **Save**.
   - Click **View** and the created certificate will be displayed.
   - The certificate will be saved automatically.
4. Download the certificate and save it to an asking file in the local computer.
5. Send the asking file to a certification authority for signature.
6. Import the signed certificate.
   1) In the **Import Key** area, select a certificate from the local, and click **Import**.
   2) In the **Import Communication Certificate** area, select a certificate from the local, and click **Import**.

Create and Import SYSLOG Certificate

Steps

1. Go to **Maintenance and Security → Security → Certificate Management** .
2. In the **SYSLOG Certificate** area, click **Create Certificate Request**.
3. Input certificate information and click **Save**.
   - Click **View** and the created certificate will be displayed.
   - The certificate will be saved automatically.
4. Download the certificate and save it to an asking file in the local computer.
5. Send the asking file to a certification authority for signature.
6. Import the signed certificate.
   1) In the **Import Key** area, select a certificate from the local, and click **Import**.
   2) In the **Import Communication Certificate** area, select a certificate from the local, and click **Import**.

Import CA Certificate

Before You Start

Prepare a CA certificate in advance.

Steps

1. Go to **Maintenance and Security → Security → Certificate Management** .
2. Create an ID in the **CA Certificate ID** area.

   Note

   The input certificate ID cannot be the same as the existing ones.
3. Upload a certificate file from the local.
4. Click **Import**.

Chapter 8 Quick Operation via Web Browser

8.1 Set Security Question

If you forget the device activation password, you can change the password via security questions and E-mail. Set the security questions before configuration.

Click in the top right of the web page to enter the **Change Password** page.

Security Question Verification

Answer the security questions.

E-mail Verification

1. Export the QR code and send it to ***pw_recovery@hikvision.com*** as attachment.
2. You will receive a verification code within 5 minutes in your reserved email.
3. Enter the verification code into the verification code field to verify your identification.

click **Next**. Or you can click **Skip** to skip the step.

8.2 Select Language

You can select a language for the device system.

Click in the top right of the web page to enter the **Device Language Settings** page. You can select a language for the device system from the drop-down list.

By default, the system language is English.

Note

After you change the system language, the device will reboot automatically.

8.3 Time Settings

Click in the top right of the web page to enter the wizard page.

Time Zone

Select the device located time zone from the drop-down list.

Time Sync.

NTP

You should set the NTP server's IP address, port No., and interval.

Manual

By default, the device time should be synchronized manually. You can set the device time manually or check **Sync. with Computer Time** to synchronize the device time with the computer's time.

Server Address/NTP Port/Interval

You can set the server address, NTP port, and interval.

DST

You can view the DST start time, end time and bias time.

Chapter 9 Configure the Device via the Mobile Web

9.1 Login

You can login via mobile browser.

Note

- Parts of the model supports Wi-Fi settings.
- Make sure the device is activated.
- Make sure the device and the mobile phone are in the same Wi-Fi.

Enter the device IP address in the address bar of the mobile browser and press **Enter** to enter the login page.

Enter the device user name and the password. Tap **Login**.

9.2 Overview

You can view the basic information, door status, real-time event, device status, network status and set person management, device management, event search, access control parameters, door parameters, etc. via shortcut entry.

Function Descriptions:

Door Status

/ / /

The door status is open/closed/remaining open/remaining closed. You can tap to select open/closed/remaining open/remaining closed status according to your actual needs.

Shortcut Entry

You can set person management, device management, event search, access control parameters, door parameters, etc. via shortcut entry.

Network Status

You can view the connected and registered status of network.

Real-Time Event

You can view real-time event details.

Device Status

You can view device status.

9.3 Forget Password

If you forget the password when logging in, you can change the password by email address or security questions.

On the login page, tap **Forget Password**.

Select **Verification Mode**.

Security Question Verification

Answer the security questions.

E-mail Verification

1. Export the QR code and send it to ***pw_recovery@hikvision.com*** as attachment.
2. You will receive a verification code within 5 minutes in your reserved email.
3. Enter the verification code into the verification code field to verify your identification.

Tap **Next**, create a new password and confirm it.

9.4 Configuration

9.4.1 View Device Information

View the device name, language, model, serial No., version, Mac address, local RS-485 number, alarm input number, alarm output number, device capacity, etc.

On the home page, tap → **System Settings** → **Basic Information** .

View the device name, language, model, serial No., version, Mac address, local RS-485 number, alarm input number, alarm output number, device capacity, etc.

Tap **Save**.

9.4.2 Time Settings

Set the time zone, time sync. mode, and displayed time.

Tap → **System Settings** → **Time Settings** to enter the settings page.

Tap **Save** to save the settings.

Time Zone

Select the time zone where the device is located from the drop-down list.

Time Sync. Mode

Manual

By default, the device time should be synchronized manually. You can set the device time manually.

NTP

Set the NTP server's IP address, port No., and interval.

9.4.3 Set DST

Steps

1. Tap → **System Settings** → **Time Settings** , to enter the settings page.

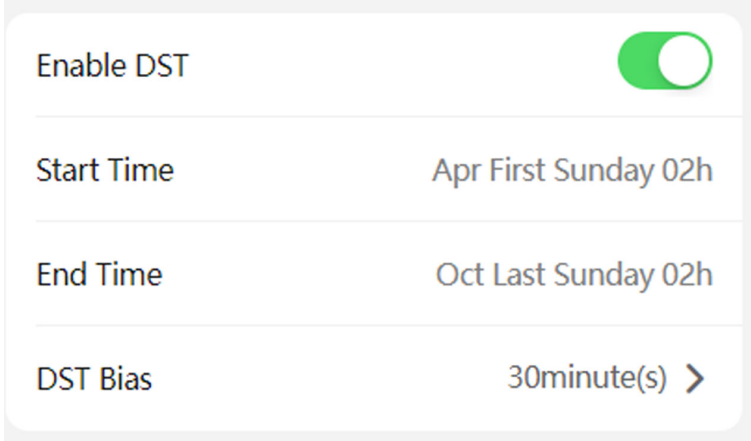


Figure 9-1 DST

2. Tap **Enable DST**.
3. Set the start time, end time, and DST bias.
4. Tap **Save**.

9.4.4 User Management

Steps

1. Tap → **User Management** → **User Management** → **admin** to enter the setting page.
2. Enter the old password and create a new password.
3. Confirm the new password.
4. Tap **Save**.

Note

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using 8-16 characters, including at least two kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you change your password

regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.

9.4.5 Network Settings

Wired Network

Set wired network.

Tap → **Network Settings** → **TCP/IP** to enter the configuration page.

DHCP

If you disable the function, you should set the IPv4 address, IPv4 subnet mask, IPv4 default gateway, IPv6 mode, IPv6 address, IPv6 subnet prefix length, IPv6 default gateway, Mac address, and MTU, Mac address, MTU.

If you enable the function, the system will allocate the IPv4 address, IPv4 subnet mask, the IPv4 default gateway, IPv6 mode, IPv6 address, IPv6 subnet prefix length, and IPv6 default gateway automatically.

DNS Server

Set the preferred DNS server and the Alternate DNS server according to your actual need.

Set Wi-Fi Parameters

Set the Wi-Fi parameters for device wireless connection.

Steps

Note

The function should be supported by the device.

1. Tap → **Network Settings** → **Wi-Fi** to enter the settings page.
2. Enable **Wi-Fi**.

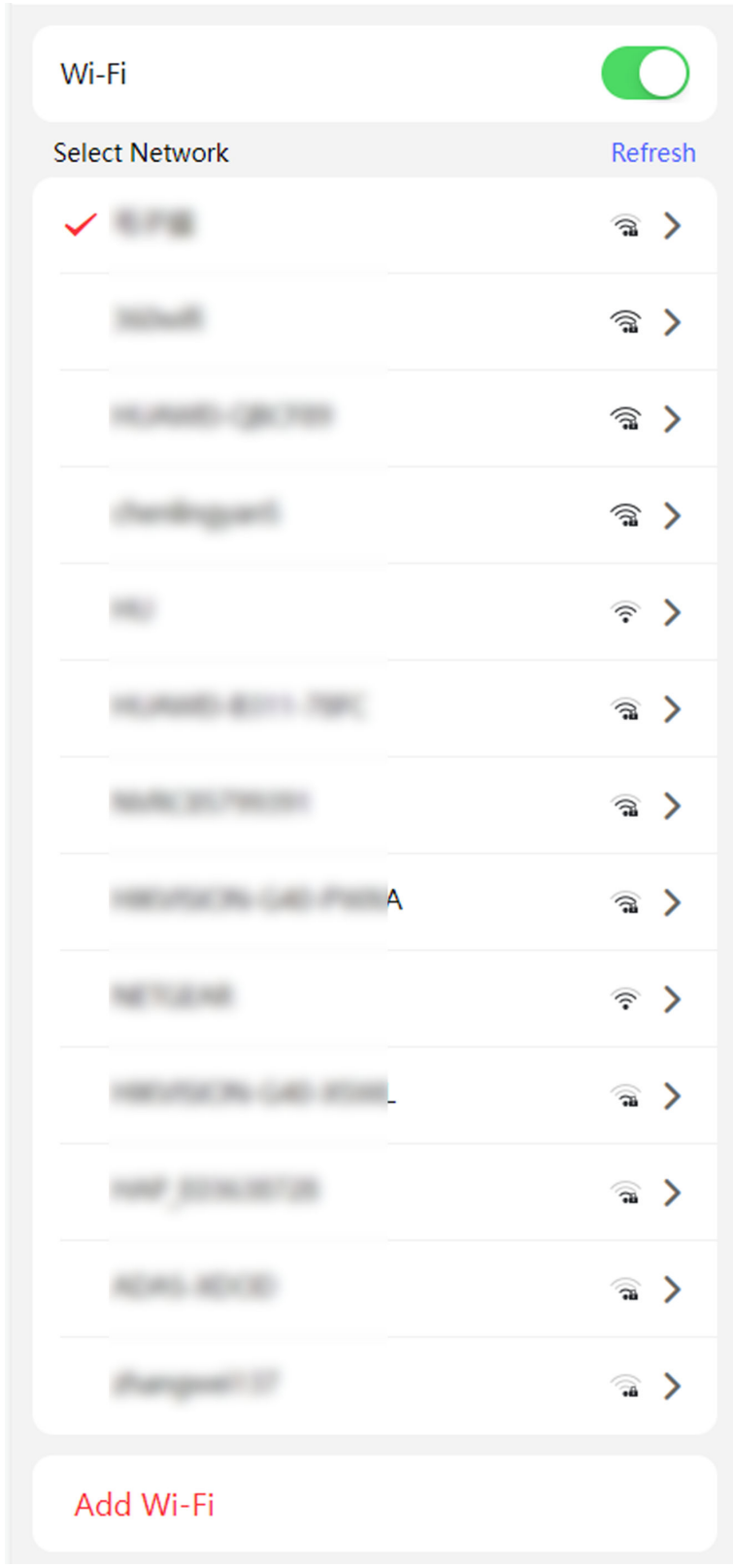


Figure 9-2 Wi-Fi

3. Add Wi-Fi.
   1) Tap **Add Wi-Fi**.
   2) Enter **Wi-Fi Name** and **Wi-Fi Password**, and select **Encryption Type**.
   3) Tap **Save**.
4. Select the Wi-Fi name, and tap **Connect**.
5. Enter the password and tap **Save**.

Set Device Hotspot

Set the device hotspot, and mobile phone can connect to the device to enter the mobile browser.

Steps

1. Tap → **Network Settings** → **Device Hotspot** .
2. You can enable device hotspot and view the hotspot name.

   Note

   By default, the hotspot name is the AP_Device Serial No.
3. Tap **Save**.

Set Port Parameters

You can set the HTTP, HTTPS and Websocket(s) according to actual needs when accessing the device via network.

Tap → **Network Service** → **HTTP(S)** , to enter the settings page.

HTTP

It refers to the port through which the browser accesses the device. For example, when the HTTP Port is modified to 81, you need to enter ***http://192.0.0.65:81*** in the browser for login.

HTTPS

Set the HTTPS for accessing the browser. Certificate is required when accessing.

Tap → **Network Service** → **Websocket(s)** , to enter the settings page.

You can view the Websocket(s) port No.

Platform Access

Platform access provides you an option to manage the devices via platform.

Steps

1. Tap → **Device Access** → **Hik-Connect** to enter the settings page.

Note

Hik-Connect is an application for mobile devices. With the App, you can view live image of the device, receive alarm notification and so on.

2. Check **Enable** to enable the function.
3. You can enable **Custom** to enter the server address.

Note

- 6 to 12 letters (a to z, A to Z) or numbers (0 to 9), case sensitive. You are recommended to use a combination of no less than 8 letters or numbers.
- The verification code cannot be ***123456*** or ***abcdef*** (case non-sensitive0).

4. You can view **Network Connection Status** and **Binding Status**.
5. You can set **Network Connection Priority**.
6. Tap **Save** to enable the settings.

Set ISUP Parameters

Set the ISUP parameters for accessing device via ISUP protocol.

Steps

Note

The function should be supported by the device.

1. Tap → **Device Access** → **ISUP** to enter the settings page.
2. Enable **ISUP**.
3. Set the ISUP version, server Address, port, device ID and encryption key.

Note

If you select 5.0 as the version, you should set the encryption key as well.

4. You can view **Registration Status**.
5. You can set **Network Connection Priority**.
6. Set the ISUP listening parameters, including ISUP alarm center IP address/domain name, ISUP alarm center URL, and ISUP alarm center port.
7. Tap **Save** to save the settings.

Set Network Penetration Service

When the device is deployed in the LAN, you can enable the penetration service to realize device remote management.

Steps

1. Tap → **Device Access** → **Network Penetration Service** to enter the settings page.

2. Tap **Enable Penetration Service**.
3. Set **Server IP Address** and **Server Port**. Create **User Name** and **Password**.
4. **Optional:** You can set **Heartbeat Timeout**. The value range is 1 to 6000.
5. **Optional:** You can view the status of the penetration service. Click **Refresh** to refresh the status.
6. Tap **Save**.

Note

The penetration service will auto disabled after 48 h.

9.4.6 Alarm Settings

Alarm Input Settings

Set the device's alarm input parameters.

Tap → **Alarm Settings** → **Alarm Input** .

Select the device, set alarm name. Click **Save**.

Alarm Output Settings

Set the device's alarm output parameters.

Tap → **Alarm Settings** → **Alarm Output** .

Select the device. Select a alarm output device No. Create a name for the alarm output device and set the alarm duration. Tap **Save**.

Continuous Alarm

The alarm output device will continuously in the alarm status.

Custom Alarm Duration

You should set the custom duration. The alarm output device will be in the alarm status for the configured time duration.

Note

Range: from 1 to 5999s.

9.4.7 Access Configuration

Set Wiegand Parameters

You can set the Wiegand transmission direction.

Steps

Note

Some device models do not support this function. Refer to the actual products when configuration.

1. Tap → **Access Configuration** → **Wiegand Settings** .
2. Select a access point from the list.
3. Set Wiegand parameters.

   No.

   Select Wiegand No. for parameters settings.

   Wiegand

   Select to enable the card reader's Wiegand function.

   Wiegand Direction

   By default, the direction is **Input**.

   Wiegand Mode

   Select the Wiegand mode and the card reader can communicate with the controller by Wiegand 26/34 or other protocol.

   Click **Auto Recognize**, enter card No. to recognize the Wiegand mode. Enter the Card No., and click **Start to Recognize**. Present the card on the related card reader. The system will show the Wiegand mode. Click **OK**.

   If select **Custom**, you should set custom Wiegand parameters. Click **Custom Wiegand Settings**, and set the name, parity type, total length and Wiegand rule. Click **OK**.

   Wiegand Mapping Card Reader

   Select the Wiegand card reader related door and card reader direction.
4. Tap **Save** to save the settings.

Note

If you change the peripheral, and after you save the device parameters, the device will reboot automatically.

Door Magnetic Contact Settings

Set the opening and closing door status of the door magnetic contact to match the actual wiring method.

Before You Start

The access controller has connected to the door magnetic contact.

Steps

1. Tap → **Access Configuration** → **Host Parameter** . to enter the settings page.
2. Select the door magnetic contact status.

Barrier Open Status (Default)

The door magnetic contact is in open status in default. Access controller is connected to the door magnet contact through NO.

Door Closed Status

The door magnetic contact is in closed status in default. Access controller is connected to the door magnet contact through NC.

9.4.8 Organization And Person Management

You can add, edit, delete, and search organization and person via mobile Web browser.

Steps

1. Tap → **Person Management** to enter the settings page.
2. Add organization.
   1) Tap**Add**, and then tap **Add Organization**.
   2) Enter **Organization Name**.
   3) Select **Upper-Level Organization**.
   4) Tap **Save**.
3. Add user.
   1) Tap**Add**, and then tap **Add Person**.
   2) Set the following parameters.

Employee ID

Enter the employee ID. The Employee ID cannot be 0 or exceed 32 characters. It can be a combination of uppercase, lowercase letters and numbers.

Name

Enter your name. The name supports numbers, uppercase and lowercase English, and characters. The name is recommended to be within 32 characters.

User Type

Select user type.

Organization

Select organization.

Permission Type/Permission Group

Permission Type

By Permission Group

Click **Allocate** and select an added access permission. The person will contain the checked access permission. If you have not added the access permission in advance, you can click **Add Access Permission** to add. For details, see ***Permission Management*** . Click **OK**.

By Access Point

Click **Allocate** and select the access schedule. Click**Add** to add the access points. The person will contain the permissions of the access point within the access schedule. Click **OK**.

Fingerprint

Add fingerprint. Tap **Fingerprint**, then tap **+**, and add fingerprint via the fingerprint module.

Card

Add card. Tap **Card**, then tap **+**, enter the card No. and select card type.

PIN

Edit or view PIN.

Note

Before configuring PIN, it is necessary to clarify whether the PIN is a device-set personal PIN or a platform-applied personal PIN. If it is a device-set personal PIN, it can be created or edited on the device or on the web, and cannot be set on other platforms; If it is a platform-applied personal PIN, it can be created or edited on the platform, and issued to the device before it can be used. It cannot be set on the device or on the web.

3) Tap **Save**.

4. Tap **More**.

1) Select **Gender**.

2) Set the following parameters.

Long-Term Effective User

Set the user permission as long-term effective.

Date of Issue/Date of Expiry

Set **Date of Issue** and **Date of Expiry** of person permission.

Extended Open

After Extended Door Opening is enabled, the close time needs to be configured in Door Parameters.

Authentication Type

Select authentication type.

5. Tap **Save**.

9.4.9 Device Management

Auto Search Device

The system can automatically search for not added modules that have been connected to the access controller.

Tap → **Device Management** → **Add** → **Auto Search Device** . The searched not added modules will be displayed in the list of the page.

Add Access Module

Add access module manually.

Steps

1. Tap → **Device Management** → **Add** → **Add Access Module** to enter the settings page.
2. Select the dial address of the access module, and set the DIP switch of the access module to be consistent with the one shown in the picture. Set **Device Name**. Tap **Next**.

   Note

   After adding or modifying the dialing address of the access module, you need to reboot the access module to take it effect.
3. Select door and set the door parameters, and tap **Next**.

   Select Door of Access Module

   According to the door actually controlled by the access module, select door.

   Door Name

   Create the door name associated with the access module.

   Area

   Choose the area from the drop-down list. If you have not created an associated area in advance, click **Add Area** to create.

   Open Duration

   Set the action time after the associated door is unlocked. If the door is not opened within the set time, the door will lock automatically. The range can be set from 1 to 255 s.

   Door Magnetic Sensor Type

   You can set Door Magnetic Sensor Type as **Remain Open** or **Remain Closed** according to your actual needs. By default, it is **Remain Closed**.

   Exit Button Type

   Under normal circumstances, it is Remain Open (except for special needs).

   Extended Open Duration

   For the elderly or children with reduced mobility, by set Extended Open Duration, the door magnetic sensor opening time after swiping card can be appropriately delayed.
4. Select the access point, set the card reader parameters associated with the module, and tap **Next**.

   Select Access Point

   According to the door actually controlled by the access module, select access point.

   Select Card Reader

Select Enter or Exit according to the actual card reader location.

Card Reader Name

Create the card reader name.

Card Reader Description

View the card reader description. Read Only

QR Code

If the card reader supports the QR code authentication function, this function can be enabled, then on the card reader, it can be carried out through the QR code authentication.

Enable Bluetooth

If the card reader supports the Open Door via Bluetooth function, this function can be enabled, then on the card reader, the door can be opened via bluetooth.

5. Set alarm input and output parameters.

Alarm Input

Select the alarm input No. and set the name.

Alarm Output

Select the alarm output No. and set the name. You can set **Alarm Duration**.

Continuous Alarm

The alarm output device will continuously in the alarm status.

Custom Alarm Duration

You should set the custom duration. The alarm output device will be in the alarm status for the configured time duration.

Note

Range: from 1 to 5999s.

6. Tap **Save**.

Add I/O Module

Add I/O module manually.

Steps

1. Tap → **Device Management** → **Add** → **Add I/O Module** to enter the settings page.
2. Select the dial address of the module, and set the DIP switch of the module to be consistent with the one shown in the picture. Set **Device Name**. Tap **Next**.

Note

After adding or modifying the dialing address of the module, you need to reboot the module to take it effect.

3. Set alarm input and output parameters.

Alarm Input

Select the alarm input No. and set the name.

Alarm Output

Select the alarm output No. and set the name. You can set **Alarm Duration**.

Continuous Alarm

The alarm output device will continuously in the alarm status.

Custom Alarm Duration

You should set the custom duration. The alarm output device will be in the alarm status for the configured time duration.

Note

Range: from 1 to 5999 s.

4. Tap **Save**.

9.4.10 Access Control Settings

Set Door Parameters

Tap → **Access Control** → **Door Parameters** .

Select the corresponding door and edit the door parameters. Tap **Save** to save the settings after the configuration. You can tap **Save and Sync. to All**.

Door Name

You can create a name for the door.

Area

Select the area.

Open Duration

Set the door unlocking duration. If the door is not opened for the set time, the door will be locked.

Door Opening Timeout Alarm Threshold

Set the Door Opening Timeout Alarm Threshold, an alarm will be triggered if the door has not been closed within the configured time duration.

Exit Button Type

You can set the exit button as **Remain Open** or **Remain Closed** according to your actual needs. By default, it is **Remain Open**.

Door Remain Open Duration with First Person (min)

Set the door open duration when first person is in. After the first person is authorized, it allows multiple persons access the door or other authentication actions.

Super Password

The specific person can open the door by inputting the super password.

Note

The duress code and the super code should be different. And the digit ranges from 4 to 8.

Set Authentication Parameters

Set Authentication Parameters.

Steps

1. Tap → **Access Control** → **Authentication Settings** .
2. Select the corresponding card reader and edit the authentication parameters.

Card Reader

Select card reader for settings.

Card Reader Type/Card Reader Description

Get card reader description. They are read-only.

Authentication

Select an authentication mode according to your actual needs from the drop-down list.

Authentication Interval

You can set the authentication interval of the same person when authenticating. The same person can only authenticate once in the configured interval. A second authentication will be failed.

Alarm of Max. Failed Attempts

Enable to report alarm when the card reading attempts reach the set value.

Lock When Card Swiping Attempts Exceed Limit/Max. Failed Attempts

Enable to report alarm when the card reading attempts reach the set max. failed attempts.

QR Code

Enable the function and the card reader can recognize the QR code for authentication.

Note

The function should be supported by the card reader.

Enable Bluetooth

Enable the bluetooth function and the you can use the bluetooth function (e.g. opening door) on the card reader.

Device Name/Transmitting Power

Edit the card reader's name and its transmitting power.

Open Door via Bluetooth

Enable the function and you can open the door via bluetooth through App. You should add the device to the App before use the function.

Advanced Settings

Enable Authentication Device

Enable the authentication function.

Communication with Controller Every

When the access control device cannot connect with the card reader for longer than the set time, the card reader will turn offline automatically.

Max. Interval When Entering Password

When you entering the password on the card reader, if the interval between pressing two digits is longer than the set value, the digits you pressed before will be cleared automatically.

Enable Tampering Detection

Enable the anti-tamper detection for the card reader.

OK LED Polarity/Error LED Polarity/Buzzer Polarity

Set OK LED Polarity/Error LED Polarity/Buzzer Polarity of the access control device according to the card reader parameters. Generally, adopts the default settings.

3. Tap **Save**. You can tap **Save and Sync. to All**.

Smart Settings

Set smart parameters.

Fingerprint Parameters

Tap → **Smart** → **Fingerprint Parameters** .

Fingerprint Recognition

Enable **Fingerprint Recognition**.

Fingerprint Security Level

You can set the security level of fingerprint. The higher the security level you set, the lower the False Acceptance Rate (FAR) will be. The higher the security level you set, the lower the False Rejection Rate (FRR) will be.

Set Privacy Parameters

Set the storage parameters.

Tap → **Access Control** → **Privacy Settings** .

Event Storage Settings

Delete Old Events Periodically

Enter number to set the period for event deleting. All events will be deleted according to the configured time duration.

Delete Old Events by Specified Time

Set a time and all events will be deleted on the configured time.

Overwriting

The earliest 5% events will be deleted when the system detects the stored events has been over 95% of the full space.

Password Mode

Before configuring passwords, it is necessary to clarify whether the password is a device-set personal PIN or a platform-applied personal PIN. If it is a device-set personal PIN, it can be created or edited on the device or on the web, and cannot be set on other platforms; If it is a platform-applied personal PIN, it can be created or edited on the platform, and issued to the device before it can be used. It cannot be set on the device or on the web.

Steps

1. Tap → **Access Control** → **Privacy Settings** → **PIN Mode**

   Device-Set Personal PIN

   It can be created or edited on the device or on the web, and cannot be set on other platforms.

   Platform-Applied Personal PIN

   It can be created or edited on the platform, and issued to the device before it can be used. It cannot be set on the device or on the web.

2. Tap **Save**.

Set Card Security

Tap → **Access Control** → **Card Settings** to enter the configuration page.

Set the parameters and tap **Save**.

Enable NFC Card

In order to prevent the mobile phone from getting the data of the access control, you can enable NFC card to increase the security level of the data.

Enable NFC Security Encryption

After enabling, the card reader can only recognize the NFC credential generated from the Hik-Connect.

Enable M1 Card

Enable M1 card and authenticating by presenting M1 card is available.

M1 Card Encryption

M1 card encryption can improve the security level of authentication.

Sector

Enable the function and set the encryption sector. By default, Sector 13 is encrypted. It is recommended to encrypt sector 13.

Enable EM Card

Enable EM card and authenticating by presenting EM card is available.

Note

EM card is supported when the device connects a peripheral card reader that supports presenting EM card.

Enable DESFire Card

The device can read the data from DESFire card when enabling the DESFire card function.

Enable FeliCa Card

The device can read the data from FeliCa card when enabling the FeliCa card function.

Card Authentication Mode

Select card authentication mode.

Enable Reversed Card No.

The read card No. will be in reverse sequence after enabling the function.

9.4.11 Event Search

Tap → **Event Search** to enter the Search page.

Enter the search conditions, and tap **Search**.

Note

Support searching for names within 32 digits.

9.4.12 Upgrade and Maintenance

Restart device, restore device parameters, and upgrade device version.

View Handling Advice

Tap → **Maintenance** → **Restart** .

You can view item exception records, and view handling advice.

Restart Device

Tap → **Maintenance** → **Restart** .
Tap **Restart** to restart the device.

Upgrade

Tap → **Maintenance** → **Upgrade** .
Tap **Upgrade** to upgrade the device.

Note

Do not power off during the upgrading.

Restore Parameters

Tap → **Maintenance** → **Default** .

Restore

The device will restore to the default settings, except for the device IP address and the user information.

Restore All

All parameters will be restored to the factory settings. You should activate the device before usage.

Device Debugging

Tap → **Maintenance** → **Device Debugging** .
You can enable **SSH** for device debugging.

View Log

Tap → **Maintenance** → **Log** .
Set log type and time, and tap **Search** to search logs.

9.4.13 View User Manual

Tap → **View User Manual** . You can scan the QR code with your mobile phone for details.

9.4.14 View Open Source Software License

Tap → **Open Source Software Statement** , you can view the Open Source Software Statement.

Chapter 10 Other Platforms to Configure

You can also configure the device via HikCentral Access Control. For details, see the platforms' user manual.

HikCentral Access Control (HCAC)

Click/tap the link to view the HCAC's user manual.

http://enpinfodata.hikvision.com/analysisQR/showQR/f2f6cf42

Appendix A. Legal Information

About this Document

- This Document includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only.
- The information contained in the Document is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of the Document at the Hikvision website (***https://www.hikvision.com***). Unless otherwise agreed, Hangzhou Hikvision Digital Technology Co., Ltd. or its affiliates (hereinafter referred to as "Hikvision") makes no warranties, express or implied.
- Please use the Document with the guidance and assistance of professionals trained in supporting the Product.

About this Product

- This product can only enjoy the after-sales service support in the country or region where the purchase is made.
- If the product you choose is a video product, please scan the following QR code to obtain the "Initiatives on the Use of Video Products", and read it carefully.

Acknowledgment of Intellectual Property Rights

- Hikvision owns the copyrights and/or patents related to the technology embodied in the Products described in this Document, which may include licenses obtained from third parties.
- Any part of the Document, including text, pictures, graphics, etc., belongs to Hikvision. No part of this Document may be excerpted, copied, translated, or modified in whole or in part by any means without written permission.
- HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.
- Other trademarks and logos mentioned are the properties of their respective owners.

LEGAL DISCLAIMER

- TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR

IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.

- YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.
- YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.
- IN THE EVENT OF ANY CONFLICTS BETWEEN THIS DOCUMENT AND THE APPLICABLE LAW, THE LATTER PREVAILS.

Data Protection

- To protect data, the development of Hikvision Products incorporates privacy by design principles. For example, for Products with facial recognition features, biometrics data is stored in your Products with encryption method; for fingerprint Products, only fingerprint template will be saved, which is impossible to reconstruct a fingerprint image.
- As a data controller/processor, you may process personal data, including collection, storage, use, processing, disclosure, deletion, etc. You are advised to pay attention to and comply with applicable laws and regulations related to the protection of personal data, including without limitation, conducting security controls to safeguard personal data, such as, implementing reasonable administrative and physical security controls, conduct periodic reviews and the assessments of the effectiveness of your security controls.

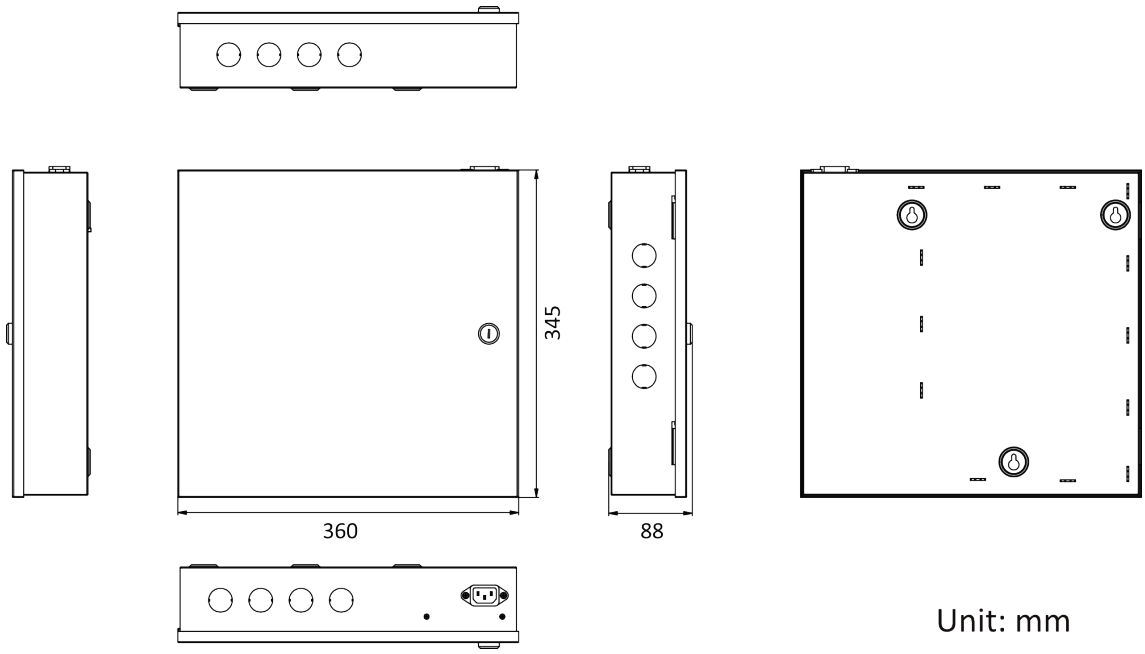
Appendix B. Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
 **Danger**	Indicates a hazardous situation which, if not avoided, will or could result in death or serious injury.
 **Caution**	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
 **Note**	Provides additional information to emphasize or supplement important points of the main text.

Appendix C. Dimension

Dimension of 1-Door/2-Door/4-Door Access Controller



Unit: mm


See Far, Go Further