
# DS-K1T502 Series Access Control Terminal

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

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, 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. |

## ⚠ Dangers

- All the electronic operation should be strictly compliance with the electrical safety regulations, fire prevention regulations and other related regulations in your local region.
- Please use the power adapter, which is provided by normal company. The power consumption cannot be less than the required value.
- Do not connect several devices to one power adapter as adapter overload may cause over-heat or fire hazard.
- Please make sure that the power has been disconnected before you wire, install or dismantle the device.
- When the product is installed on wall or ceiling, the device shall be firmly fixed.
- If smoke, odors or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service center.
- Do not ingest battery, Chemical Burn Hazard.
  This product contains a coin/button cell battery. If the coin/button cell battery is swallowed, it can cause severe internal burns in just 2 hours and can lead to death.
  Keep new and used batteries away from children. If the battery compartment does not close securely, stop using the product and keep it away from children. If you think batteries might have been swallowed or placed inside any part of the body, seek immediate medical attention.
- If the product does not work properly, please contact your dealer or the nearest service center. Never attempt to disassemble the device yourself. (We shall not assume any responsibility for problems caused by unauthorized repair or maintenance.)

## ⚠ Cautions

- This equipment is not suitable for use in locations where children are likely to be present.
- Do not drop the device or subject it to physical shock, and do not expose it to high electromagnetism radiation. Avoid the equipment installation on vibrations surface or places subject to shock (ignorance can cause equipment damage).

- Do not place the device in extremely hot (refer to the specification of the device for the detailed operating temperature), cold, dusty or damp locations, and do not expose it to high electromagnetic radiation.
- The device cover for indoor use shall be kept from rain and moisture.
- Exposing the equipment to direct sun light, low ventilation or heat source such as heater or radiator is forbidden (ignorance can cause fire danger).
- Do not aim the device at the sun or extra bright places. A blooming or smear may occur otherwise (which is not a malfunction however), and affecting the endurance of sensor at the same time.
- Please use the provided glove when open up the device cover, avoid direct contact with the device cover, because the acidic sweat of the fingers may erode the surface coating of the device cover.
- Please use a soft and dry cloth when clean inside and outside surfaces of the device cover, do not use alkaline detergents.
- Please keep all wrappers after unpack them for future use. In case of any failure occurred, you need to return the device to the factory with the original wrapper. Transportation without the original wrapper may result in damage on the device and lead to additional costs.
- Improper use or replacement of the battery may result in hazard of explosion. Replace with the same or equivalent type only. Dispose of used batteries according to the instructions provided by the battery manufacturer.
- You can view the device License via the website: *http://opensource.hikvision.com/Home/List?id=46*.

# Available Models

The access control terminal contains the following models:

| Product Name | Model |
|---|---|
| Access Control Terminal | DS-K1T502DBWX-C, DS-K1T502DBWX-QRE1, DS-K1T502DBWX-CQRE1, DS-K1T502DBWX-CE1, DS-K1T502DBFWX-CE1, DS-K1T502DBWX-E1, DS-K1T502DBFWX-E1 |

**Table 1-1 Available Mobile Web Browsers**

| Operation System | Browser | Version | Available |
|---|---|---|---|
| Android | Xiaomi 12, default browser | 16.6.6 | Yes |
| | Huawei P30, default browser | 12.1.1.321 | Yes |
| | Xiaomi 5s plus, default browser | 14.2.22 | Yes |
| | Huawei P30 Pro, default browser | 12.1.2.301 | Yes |
| | Redmi k40, default browser | 16.5.12 | Yes |
| IOS | Safari | 15.4 | Yes |

# Contents

# Chapter 1 Quick Operation

You can scan the following QR code to get detail information of device appearance, installation, wiring and quick operation.

**Figure 1-1 Quick Start Guide QR Code**

# Chapter 2 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.: 80
- The default user name: admin

## 2.1 Activate via Mobile Web

You can activate the device via mobile web.

**Steps**

**Note**

After powering on the device for the first time, the hotspot function is enabled by default.

1. Enable the mobile phone's Wi-Fi function. Search and add the device hotspot (hotspot name: AP_Serial No.).

   **Note**

   - Hotspot name/password: AP_Serial No.
   - Hold key 5 on the device keypad for 5 s to enable/disable the hotspot function.
   - After 30 min after device powering on, the hotspot function will be disabled automatically.
   - After device activation, the hotspot password will be changed to the device activation password.

2. The mobile phone will jump to the web browser page. Create a new password (admin password) and confirm the password.

   **Note**

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

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

## 2.2 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**

   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.

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.

## 2.3 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**

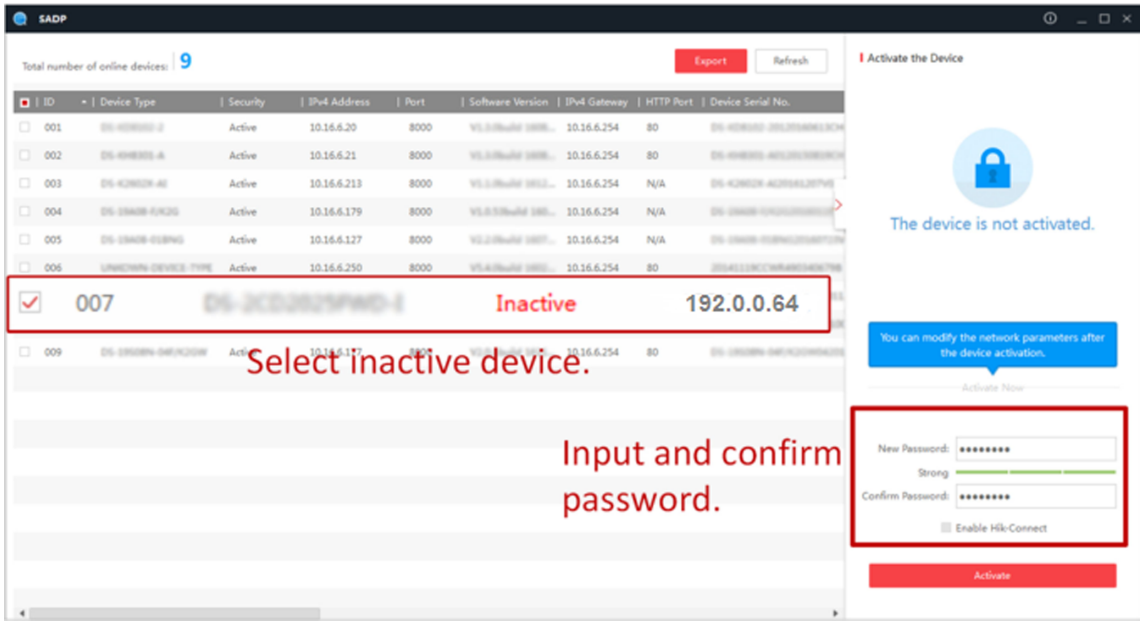
1. Run the SADP software and search the online devices.

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.

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.

## 2.4 Activate Device via iVMS-4200 Client Software

For some devices, you are required to create the password to activate them before they can be added to the iVMS-4200 software and work properly.

**Steps**

**Note**

This function should be supported by the device.

1. Enter the Device Management page.
2. Click on the right of **Device Management** and select **Device**.
3. Click **Online Device** to show the online device area.

   The searched online devices are displayed in the list.
4. Check the device status (shown on **Security Level** column) and select an inactive device.
5. Click **Activate** to open the Activation dialog.
6. Create a password in the password field, 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 installer and/or end-user.

   **Note**

   Characters containing admin and nimda are not supported to be set as activation password.
7. Click **OK** to activate the device.

# Chapter 3 Typical Scenarios

## 3.1 Identity Authentication

After network configuration, system parameters configuration and user configuration, you can go back to the initial page for identity authentication. The system will authenticate person according to the configured authentication mode.

### 3.1.1 Authenticate via Single Credential

Set the user authentication type before authentication. For details, see .

Authenticate fingerprint, card, PIN, or QR code.

**Fingerprint**

Place the enrolled fingerprint on the fingerprint module and start authentication via fingerprint.

**Card**

Present the card on the card presenting area and start authentication via card.

**Note**

The card can be normal IC card, or encrypted card.

**QR Code**

Put the QR code in front of the device camera or QR code recognition area to authenticate via QR code.

**Note**

- Dynamic QR codes need to be authenticated within the validity period. Once the QR code is refreshed, the old QR code will not be authenticated.
- Authentication via QR code should be supported by the device.

**PIN**

Enter the PIN to authenticate via PIN.

If authentication completed, a prompt "Authenticated" will pop up.

### 3.1.2 Authenticate via Multiple Credential

**Before You Start**

Set the user authentication type before authentication. For details, see .

**Steps**

1. Authenticate any credential according to the instructions on the live view page.

**Note**

- The card can be normal IC card, or encrypted card.
- If the QR Code Scanning function is enabled, you can put the QR code in front of the device camera or QR code recognition area to authenticate via QR code.

**2.** After the previous credential is authenticated, continue authenticate other credentials.

**Note**

For detailed information about scanning fingerprint, see *Tips for Scanning Fingerprint*.

If authentication succeeded, the prompt "Authenticated" will pop up.

## 3.2 Call and Video Intercom

Set the SIP server IP, calling and video intercom between devices are available.

Set Device A as SIP server, and set Device A's IP as SIP server IP. For details, see . All other devices that need to call each other should be registered to the server.

Set device room number. For details, see ***Set Device No. via Web*** .

On the device main page, enter the device room No. to call. When the other device is answered, video intercom can be performed.

# Chapter 4 Quick Operation via Web Browser

## 4.1 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.

## 4.2 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.

## 4.3 Time Settings

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

**Device Time**

Display the device time in real time.

**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.

**DST**

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

Click **Next** to save the settings and go to the next parameter. Or click **Skip** to skip time settings.

## 4.4 Privacy Settings

Set the picture uploading and storage parameters.

Click in the top right of the web page to enter the wizard page. After setting device language, time and environment, you can click **Next** to enter the **Privacy Settings** page.

### Picture Uploading and Storage

**Upload Picture After Linked Capture**

Upload the pictures captured by linked camera to the platform automatically.

**Save Pictures After Linked Capture**

If you enable this function, you can save the picture captured by linked camera to the device.

Click **Next** to save the settings and go to the next paramater. Or click **Skip** to skip privacy settings.

## 4.5 No. and System Network

**Steps**

1. Click in the top right of the web page to enter the wizard page. After previous settings, you can click **Next** to enter the **No. and Network System Network** settings page.
2. Set the device type.

**Note**

- If set the device type as **Door Station**, you can set the **Floor No.**, **Door Station No.**, **Community No.**, **Building No.**, **Unit No.**, **Floor No.**, and **Door Station No.**.
- If set the device type as **Outer Door Station**, you can set **Outer Door Station No.**, and **Community No.**

**Device Type**

The device can be used as a door station or outer door station. Select a device type from the drop-down list.

**Community No.**

Set the device community No.

**Building No.**

Set the device building No.

**Unit No.**

Set the device unit No.

**Floor No.**

Set the device installed floor No.

**Door Station No.**

Set the device installed door station No.

**Note**

The main door station No. is 0, and the sub door station No. ranges from 1 to 16.

**Outer Door Station No.**

Set the device installed outer door station No.

**Note**

The No. ranges from 1 to 99.

3. Set the video intercom network parameters.

**Registration Password**

Set the registration password of the main station for communication. Set the registration password of the main station for communication.

**Main Station IP**

Enter the main station's IP address that used for communication.

**Private Server IP**

Refers to the SIP server IP. Enter the main station's IP address that used for communication. At this time the main station is used as a SIP server. Other intercom devices should registered to this server address to realize communication.

**Enable Protocol 1.0**

If enabled, the door station can be registered to the main station by old protocol version. If disabled, the door station can be registered to the main station by new protocol version.

4. Click **Complete** to save the settings after the configuration.

# Chapter 5 Operation via Web Browser

## 5.1 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*** .

### 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.

## 5.2 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.

## 5.3 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.

## 5.4 Help

### 5.4.1 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.

### 5.4.2 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.

## 5.5 Logout

Log out the account.

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

## 5.6 Quick Operation via Web Browser

### 5.6.1 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.

### 5.6.2 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.

### 5.6.3 Time Settings

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

**Device Time**

Display the device time in real time.

**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.

**DST**

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

Click **Next** to save the settings and go to the next parameter. Or click **Skip** to skip time settings.

### 5.6.4 Privacy Settings

Set the picture uploading and storage parameters.

Click in the top right of the web page to enter the wizard page. After setting device language, time and environment, you can click **Next** to enter the **Privacy Settings** page.

#### Picture Uploading and Storage

**Upload Picture After Linked Capture**

Upload the pictures captured by linked camera to the platform automatically.

**Save Pictures After Linked Capture**

If you enable this function, you can save the picture captured by linked camera to the device.

Click **Next** to save the settings and go to the next paramater. Or click **Skip** to skip privacy settings.

### 5.6.5 No. and System Network

**Steps**

1. Click in the top right of the web page to enter the wizard page. After previous settings, you can click **Next** to enter the **No. and Network System Network** settings page.
2. Set the device type.

**Note**

- If set the device type as **Door Station**, you can set the **Floor No.**, **Door Station No.**, **Community No.**, **Building No.**, **Unit No.**, **Floor No.**, and **Door Station No.**.
- If set the device type as **Outer Door Station**, you can set **Outer Door Station No.**, and **Community No.**

**Device Type**

The device can be used as a door station or outer door station. Select a device type from the drop-down list.

**Community No.**

Set the device community No.

**Building No.**

Set the device building No.

**Unit No.**

Set the device unit No.

**Floor No.**

Set the device installed floor No.

**Door Station No.**

Set the device installed door station No.

**Note**

The main door station No. is 0, and the sub door station No. ranges from 1 to 16.

**Outer Door Station No.**

Set the device installed outer door station No.

**Note**

The No. ranges from 1 to 99.

3. Set the video intercom network parameters.

**Registration Password**

Set the registration password of the main station for communication. Set the registration password of the main station for communication.

**Main Station IP**

Enter the main station's IP address that used for communication.

**Private Server IP**

Refers to the SIP server IP. Enter the main station's IP address that used for communication. At this time the main station is used as a SIP server. Other intercom devices should registered to this server address to realize communication.

**Enable Protocol 1.0**

If enabled, the door station can be registered to the main station by old protocol version. If disabled, the door station can be registered to the main station by new protocol version.

4. Click **Complete** to save the settings after the configuration.

## 5.7 Person Management

Click **Add** to 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, gender, and person type.
If you select **Visitor** as the person type, you can set the visit times.
Click **Save** to save the settings.

### Set Permission Time

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

### Add Card

Click **Person Management → Add** to enter the Add Person page.
Click **Add Card**, enter the **Card No.** and select the **Property**, and click **OK** to add the card.
Click **Save** to save the settings.

### Add Fingerprint

**Note**

Only devices supporting the fingerprint function can add the fingerprint.

Click **Person Management → Add** to enter the Add Person page.

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

### Add PIN

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.
Click **Configuration → Security → Password Mode** , select **PIN Mode** as **Device-Set Personal PIN**.
Click **Person Management → Add** to enter the Add Person page.
Set the PIN.
Click **Save** to save the settings.

### Authentication Settings

Click **Person Management → Add** to enter the Add Person page.
Set the authentication type.
Click **Save** to save the settings.

### Delete Person

On the person management page, check the person need to delete and click **Delete**.
Click **Clear All** to clear all person.

### Edit Person

On the person management page, check the person need to edit. Click to edit the person information.

### Filter

On the person management page, enter **Employee ID / Name / Card No.**. Select **Credential Status**, and click **Filter** to filter the person. Click **Reset** to clear all conditions.

## 5.8 Access Control Management

### 5.8.1 Overview

You can view the live video of the device, real-time event, person information, network status, basic information, and device capacity.

Function Descriptions:

**Door Status**

Click to view the device live view.

Set the volume when starting live view.

**Note**

If you adjust the volume when starting two-way audio, you may hear a repeated sounds.

You can capture image when starting live view.

Select the streaming type when starting live view. You can select from the main stream and the sub stream.

Full screen view.

 /  /  / 

The door status is open/closed/remaining open/remaining closed.

**Controlled Status**

You can select open/closed/remaining open/remaining closed status according to your actual needs.

**Real-Time Event**

You can view the event Employee ID, Name, Card No., Event Type, Time, and Operation. You can also click **View More** to enter the search conditions, including the event 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.

**Person Information**

You can view the added and not added information of person, card, and fingerprint.

**Network Status**

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

**Basic Information**

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

**Device Capacity**

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

**Note**

Only devices supporting fingerprint function can display the fingerprint capacity.

**View More**

You can click **View More** to view the event details.

### 5.8.2 Search Event

Click **Event Search** to enter the Search page.

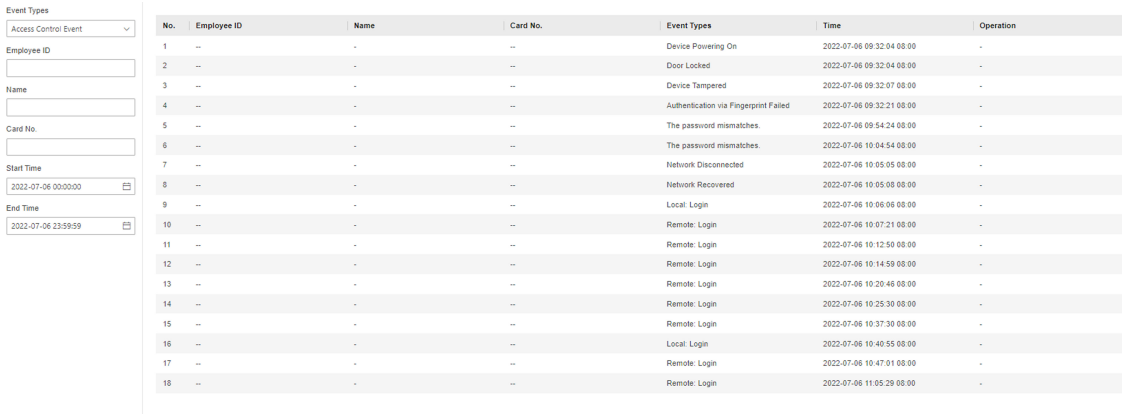



**Figure 5-1 Search Event**

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**.

The results will be displayed on the right panel.

### 5.8.3 Door Parameter Configuration

Configure parameters for unlocking doors.

### Enable Door 2

You can enable door 2 to set corresponding parameters.

**Steps**

1. Click **Access Control → Access Control Parameters → Door Parameters** .
2. Enable Door 2.

**Note**

- Door 2 needs to be enabled first before configuration.
- Only PoE series devices support this function.

3. Click **Save**.

**What to do next**

You can set corresponding parameters of door 2.

## 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 Magnetic Sensor Type via PC Web

You can select door contact type according to the wiring method.

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

Select magnetic sensor type as remain closed or remain open. By default, it is **Remain Closed** (excluding special needs).

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**.

## 5.8.4 Authentication Settings

### Select Main or Sub Card Reader via PC Web

Set the terminal for person authentication.

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

Select the terminal as main or sub card reader.

Set other parameters and click **Save**.

### Double Door Control

You can enable Double Door Control, then the device can control 2 doors.

**Steps**

1. Click **Access Control → Access Control Parameters → Authentication Settings** .
2. Enable **Double Door Control**.

**Note**

After enabling, the device can control 2 doors. Anti-passback functions will be invalid.

3. Click **Save**.

### View Terminal Type and Model via PC Web

You can view terminal type and model.

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

View **Terminal Type** and **Terminal Model**.

### Enable Authentication Device via PC Web

After enabling, the authentication terminal can be used for card swiping.

**Steps**

1. Click **Access Control → Parameter Settings → Authentication Settings** to enter the settings page.
2. Enable **Authentication Device**. After enabling, the terminal can be used for card swiping normally.
3. Click **Save**.

## External Devices Authentication

You can set external devices authentication requirement.

**Steps**

1. Click **Access Control → Access Control Parameters → Authentication Settings** .
2. Enable **External Devices Authentication**.

   **Note**

   After enabling, external devices require authentication.
3. Click **Save**.

## Set Authentication via PC Web

Configure Certification.

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

When selecting main card reader as the Terminal, you can select Authentication from the drop-down list. When there is more than one authentication, you should set **Single Credential Authenticating Timeout** and **Control Initial Authentication Type**.

**Single Credential Authenticating Timeout**

You can configure the duration for each certification.

**Note**

The password authenticating timeout is 20 s by default, which is not limited by above settings.

**Control Initial Authentication Type**

If enabled, all selected types can be used for first-time authentication.

When selecting sub card reader as the Terminal, you can select Authentication from the drop-down list.

Click **Save**.

## Set Authentication Interval via PC Web

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. If other person authenticate in the configured interval, the person can authenticate again.

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

When you select the terminal as main card reader, set **Authentication Interval**, and click **Save**.

## Enable Alarm of Max. Failed Attempts via PC Web

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

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

When you select the terminal as main or sub card reader, slide to enable **Alarm of Max. Failed Attempts**, and set **Max. Authentication Failed Attempts**.

Click **Save**.

## Enable/Disable Tampering Detection via PC Web

You can enable tampering detection, the device will automatically generate tampering events when the card reader is removed or taken away.

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

Enable or disable **Tampering Detection** according to your actual needs. After enabling the function, the device will automatically generate tampering events when the card reader is removed or taken away. If the function is disabled, no alarm events will be generated.

Click **Save**.

## Enable/Disable Card No. Reversing via PC Web

You can enable or disable the card No. reversing function.

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

Enable **Card No. Reversing**, the read card No. will be in reverse sequence.

Click **Save**.

## Enable/Disable QR Code Recognition via Web Client

You can enable/disable the QR Code recognition function.

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

If the device support QR code recognition, you can enable **QR Code** and the device can read the QR code converted from the card No.

Click **Save**.

## Set Communication with Controller Every via PC Web

You can set communication with controller every of sub card reader. If the card reader can't connect with the access controller in the set time, the card reader is offline.

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

When you select the terminal as sub card reader, set **Communication with Controller Every**, and click **Save**.

## Set Timeout Duration of Entering Password via Web Client

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.

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

When selecting the sub card reader as the Terminal, you can set **Max. Interval When Entering Password** and click**Save**.

## Set OK LED Polarity and Error LED Polarity via PC Web

Select the polarity of the diodes for OK and ERR interfaces according to actual wiring, with a default positive polarity.

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

When you select the terminal as sub card reader, set **OK LED Polarity** and **Error LED Polarity**, and click **Save**.

## Enable/Disable Bluetooth and Open Door via Gesture via PC Web

You can set to enable device bluetooth and open door via gesture via PC Web.

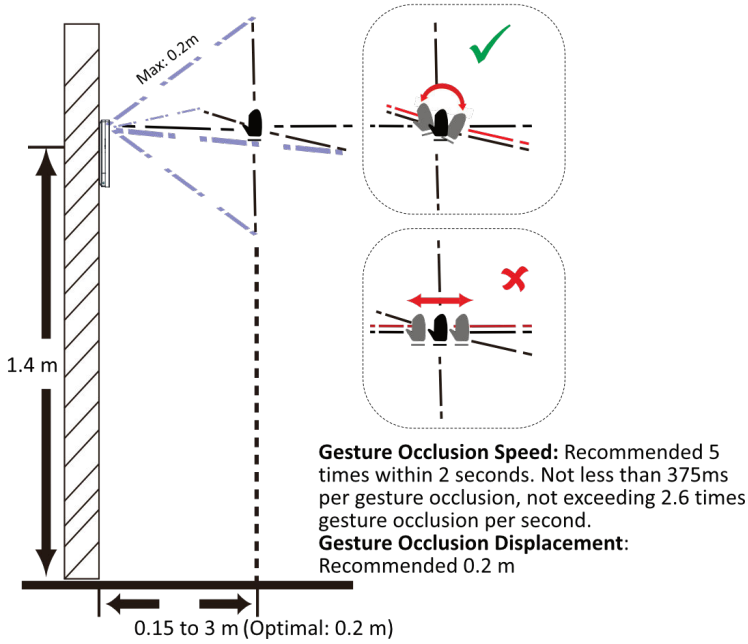
**Before You Start**
You should add the device to mobile App before operation.

**Steps**
1. Click **Access Control → Parameter Settings → Authentication Settings** to enter the settings page.
2. In the bluetooth parameter configuration section, enable **Enable Bluetooth**.

3. Enter **Device Name**. After the bluetooth is connected, click **Save**. Enable **Open Door via Bluetooth**, you can control the door remotely.
4. You can enable **Open Door via Gesture** and set **Occlusion Times**. After the number of occlusion reaches the set limit, the door will be controlled to open.

**Note**

- You need to enable **Bluetooth** and **Open Door via Bluetooth** first to make **Open Door via Gesture** function take effect.
- Continuously occluding detector is not allowed. The duration of each occlusion can not exceed 5 seconds.
- For gesture occlusion, the vertical distance of the hand movement from the center of the camera should be approximately 0.15 to 0.3 meters, with an optimal distance around 0.2 meters. The effective gesture area extends 0.2 meters up, down, left, and right from the center.
  The recommended hand movement speed is five times within 2 seconds. A single hand movement should take no less than 375 ms, and the fastest detectable speed is 2.6 hand movements per second. During the gesture, the wrist displacement should exceed 0.2 meters. Moving the hand vertically toward or away from the camera does not count as a gesture (avoid hand-waving motions without wrist movement). Detection effectiveness is lower when the wrist displacement is less than 0.2 meters.
  When a gesture is detected, the green light flashes briefly. When the Occlusion Time is set to 2, the red light flashes rapidly between two gesture occlusions, and after the required number of gestures is reached, the red light returns to a steady on state.



### Set Authentication Plan

You can set authentication plan.

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

Select the authentication type and authentication schedule type, if you select **Custom**, you need drag the time period in the time bar.

Click **Save**.

## 5.8.5 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.

Click **Enable NFC Security Encryption**. When enabled, the card reader can only recognize the NFC credential generated from Hik-Connect.

### 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**.

After enabling, the device can read DESFire card.

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

Enable **Enable DESFire Card**.

Enable **DESFire Card Read Content** and click **Save**. After enabling, the device can read DESFire 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.

## 5.8.6 Linkage Settings

When the configured event is triggered, upload the event information to the central platform according to the configured method.

**Steps**

1. Click **System and Maintenance → System Configuration → Event → Linkage Settings** to enter the settings page.

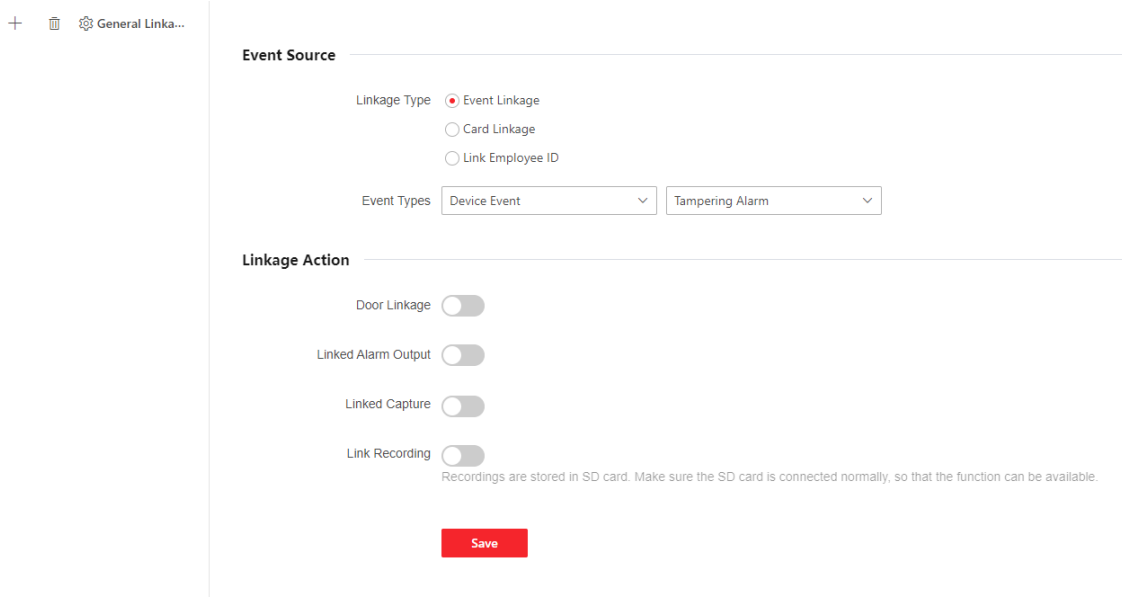



**Figure 5-2 Linkage Settings**

2. Click **+** .
3. Set event source. Select the linkage type as **Event Linkage**, **Card Linkage** or **Link Employee ID**.
   - Select **Linkage Type** as **Event Linkage**, you can select event types according to your actual needs.
   - Select **Linkage Type** as **Card Linkage**, enter **Card No.** and select **Card reader**.
   - Select **Linkage Type** as **Link Employee ID**, enter **Employee ID** and select **Card reader**.
4. Set linkage action.
   1) Enable **Door Linkage**, check and select door action.
   2) Enable **Linked Alarm Output**, check and select alarm output action.
   3) Enable **Linked Capture**.
   4) Enable **Link Recording**, click **General Linkage Settings** to set pre-record time and recording delay, and enable record audio when recording video. Click **Save**.

   **Note**

   To use the recording function, you need to prepare the SD card. After recording, you can click **Event Search** to view recordings. For details, see ***Search Event***
5. Click**Save** to enable the settings.

### 5.8.7 Set Working Mode via PC Web

You can set the terminal parameters of the device.

**Note**

Only some models support this function, please refer to the specific device.

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

**Working Mode**

You can set the working mode as access control mode or permission free mode.

**Access Control Mode**

The access control mode is the device normal mode. You should authenticate your credential for accessing.

### 5.8.8 Set Remote Verification

The device will upload the person's authentication information to the platform. The platform will judge to open the door or not.

Go to **Access Control → Parameter Settings → Terminal Parameters**.

Click**Save** after parameters are configured.

**Remote Verification**

After enabling the remote verification, when authenticating, the device will upload authentication information to the platform, and the platform will confirm whether to open the door.

### 5.8.9 Privacy Settings

#### 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 Picture Uploading and Storage Parameters

Set picture uploading and storage parameters.

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

Enable the function.

**Save Pictures After Linked Capture**

If you enable this function, the captured pictures will be saved to the device automatically.

Click **Save**.

#### Clear All Pictures in Device via PC Web

You can clear all captured pictures in the device.

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

Click **Clear**. All captured pictures will be deleted.

### 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**.

## 5.9 Video Intercom Settings

### 5.9.1 Set Device No. via Web

The device can be used as a door station or outer door station. You should set the device No. before usage.

Click **Access Control → Call Settings → Device No.** .


**Figure 5-3 Device No. Settings**

If set the device type as **Door Station**, you can set the **Floor No.**, **Door Station No.**, **Community No.**, **Building No.**, and **Unit No.**

**Device Type**

The device can be used as a door station or outer door station. Select a device type from the drop-down list.

**Note**

If you change the device type, you should reboot the device.

**Floor No.**

Set the device installed floor No.

**Door Station No.**

Set the device installed floor No.

**Note**

- If you change the No., you should reboot the device.
- The main door station No. is 0, and the sub door station No. ranges from 1 to 16.

**Community No.**

Set the device community No.

**Building No.**

Set the device building No.

**Unit No.**

Set the device unit No.

**Note**

If you change the No., you should reboot the device.

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

If set the device type as **Outer Door Station**, you can set outer door station No., and community No.

**Outer Door Station No.**

If you select outer door station as the device type, you should enter a number between **1** and **99**.

**Note**

If you change the No., you should reboot the device.

**Community No.**

Set the device community No.

### 5.9.2 Configure Video Intercom Network Parameters via Web Browser

You can set the registration password, main station IP and private server IP, and you can enable protocol 1.0 according to your actual needs.

Click **Call Settings → Video Intercom Network** to enter the settings page.

**Registration Password**

Set the registration password of the main station for communication. Set the registration password of the main station for communication.

**Main Station IP**

Enter the main station's IP address that used for communication.

**Private Server IP**

Refers to the SIP server IP. Enter the main station's IP address that used for communication. At this time the main station is used as a SIP server. Other intercom devices should registered to this server address to realize communication.

**Enable Protocol 1.0**

If enabled, the door station can be registered to the main station by old protocol version. If disabled, the door station can be registered to the main station by new protocol version.

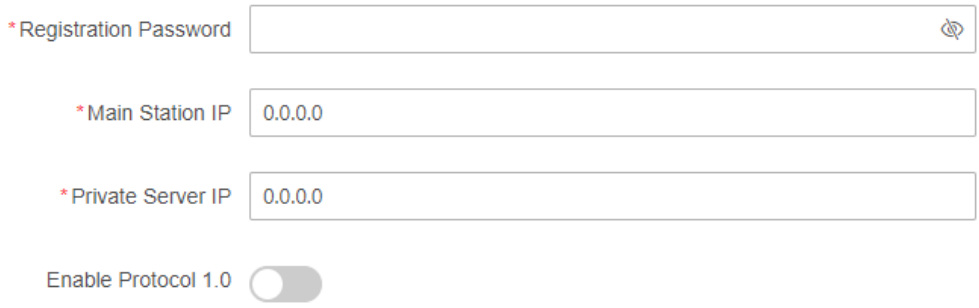



**Figure 5-4 Video Intercom Network**

After configuration, you can achieve communication between access control devices and video intercom door station, indoor station, main station, platforms, etc.

Click **Save**.

## 5.9.3 Call Settings

Set the Max. communication time.

Go to **Access Control → Call Settings → Call Settings**.

**Max. Communication Time**

The Maximum communication time when the main station and the other devices are in the call. When the communication time exceeds the configured time, the communication will stop. The Max. communication time range is 90 s to 120 s.

**Calling Channel Settings**

You can set Calling Channel via **Hik-Connect Personal** or **Hik-Connect Team**.

### 5.9.4 Set Press Button to Call via PC Web

Set the button linked device for calling.

**Steps**

1. Click **Access Control → Call Settings → Press Button to Call**.

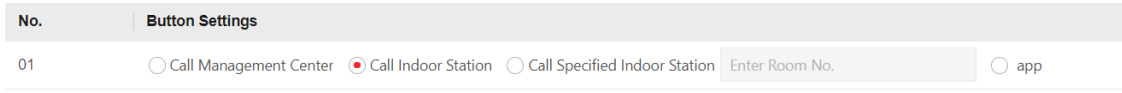



**Figure 5-5 Press Button to Call**

2. Set the button as **Call Management Center**, **Call Indoor Station**, **Call Specified Indoor Station**,or app.

**Note**

- When you check Call Specified Indoor Station, you should set the linked room's No.
- If you check app, you can call HC or HCC.

3. Click **Save**.

### 5.9.5 Number Settings via PC Web

Set SIP number for the room. The rooms can communicate with each other via SIP number.

**Steps**

1. Go to **Access Control → Call Settings → Number Settings**.
2. Click **Add**, and enter **Room No.** and **SIP1** phone number.
3. **Optional:** Click **Add** to add the SIP number or click to delete the number.
4. **Optional:** You can click **Import No.** to import SIP No. through Excel in batch. You can click **Download SIP No. Data Template**, and enter the data to import.

**Note**

Please refer to the downloaded EXCEL for detailed filling instructions.

5. **Optional:** You can click **Export No.** and click **Confirm** to export SIP No.
6. Click**Save**.
7. **Optional:** You can click **Delete** to delete room number and its SIP number.

## 5.10 Device Management

You can view the device No., type, IP, serial No., model, version, floor No., room No., No., arming status, user name, network status and operation. You can also add indoor station and sub door station on the device management page, and manage, upgrade or delete devices.

**Steps**

1. Click**Device Management**.
2. Click **Add**.
3. Select **Device Type**, enter **Device Password**, **Registration Password**, **Serial No.**, **IP Address**, **IPv4 Subnet Mask**, **IPv4 Default Gateway**, **Port**, **Floor No.**, and **No.** (not needed to enter **Floor No.**, and **No.** for indoor station, but **Room No.** is needed) .
4. Click **Save**.
5. **Optional:** You can also perform the following operations.

| | |
|---|---|
| **Delete Device** | Check devices need to delete, and click **Delete**. |
| **Import Device** | Click **Import**, download the template. After filling the information, click to import the devices. |
| **Export Device** | Click **Export** to export the device information files to local PC. |

## 5.11 System Configuration

### 5.11.1 Set Local Parameters

Set the live view parameters, record file saving path, and captured pictures saving path.

#### Set Live View Parameters

Click **System and Maintenance → Local** to enter the Local page. Configure the stream type, the play performance, auto start live view, and the image format and click **Save**.

#### Set Record File Saving Path

Click **Configuration → Local** to enter the Local page. Select a record file size and select a saving path from your local computer and click **Save**.
You can also click **Open** to open the file folder to view details.

#### Set Captured Pictures Saving Path

Click **Configuration → Local** to enter the Local page. Select a saving path from your local computer and click **Save**.
You can also click **Open** to open the file folder to view details.

### 5.11.2 View Device Information via PC Web

View the device name, device No., language, model, serial No., version, number of channels, IO input, IO output, lock, alarm input, alarm output, and device capacity, etc.

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

You can view the device name, device No., language, model, serial No., version, number of channels, IO input, IO output, lock, alarm input, alarm output, and device capacity, etc.

Click **Upgrade** in the Firmware Version, you can go to the upgrade page to upgrade the device.

### 5.11.3 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** .

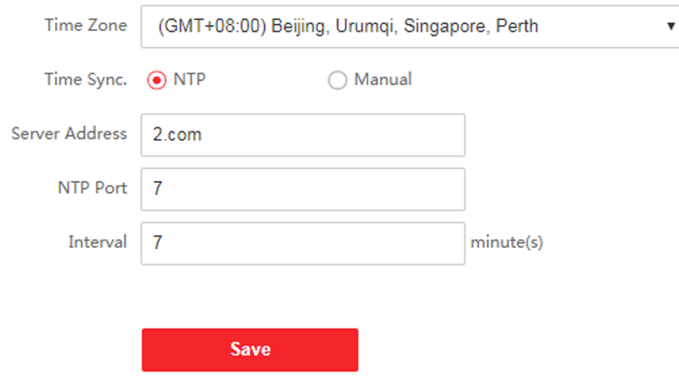



**Figure 5-6 Time Settings**

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

**Time Zone**

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

**Time 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 Type/Server Address/NTP Port/Interval**

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

### 5.11.4 Set DST

**Steps**

1. Click **System and Maintenance → System Configuration → System → System Settings → Time Settings** .
2. Enable **DST**.
3. Set the DST start time, end time and bias time.
4. Click **Save** to save the settings.

### 5.11.5 Change Administrator's Password

**Steps**

1. Click **System and Maintenance → System Configuration → System → User Management → 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 installer and/or end-user.

### 5.11.6 Account Security Settings via PC Web

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 → 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.

### 5.11.7 Online Users

The information of users logging into the device is shown.

Go to **System and Maintenance → System Configuration → System → User Management → Online Users** to view the list of online users.

### 5.11.8 View Device Arming/Disarming Information via PC Web

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.

### 5.11.9 Network Settings

#### Set Basic Network Parameters

Click **System and Maintenance → System Configuration → Network → Network Settings → TCP/IP** .

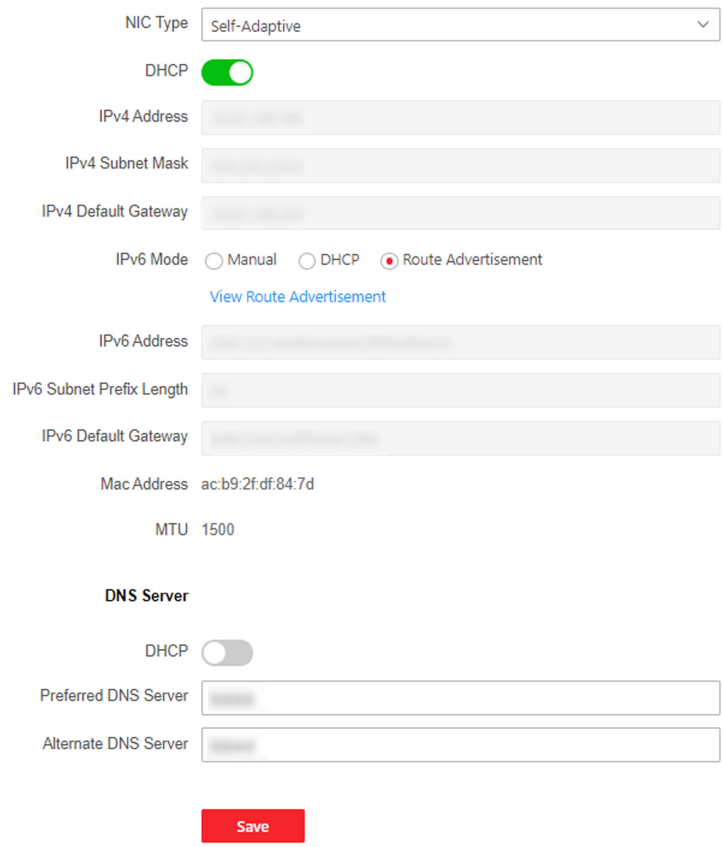



**Figure 5-7 TCP/IP Settings Page**

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

**NIC Type**

Select a NIC type from the drop-down list. By default, it is **Auto**.

**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** .

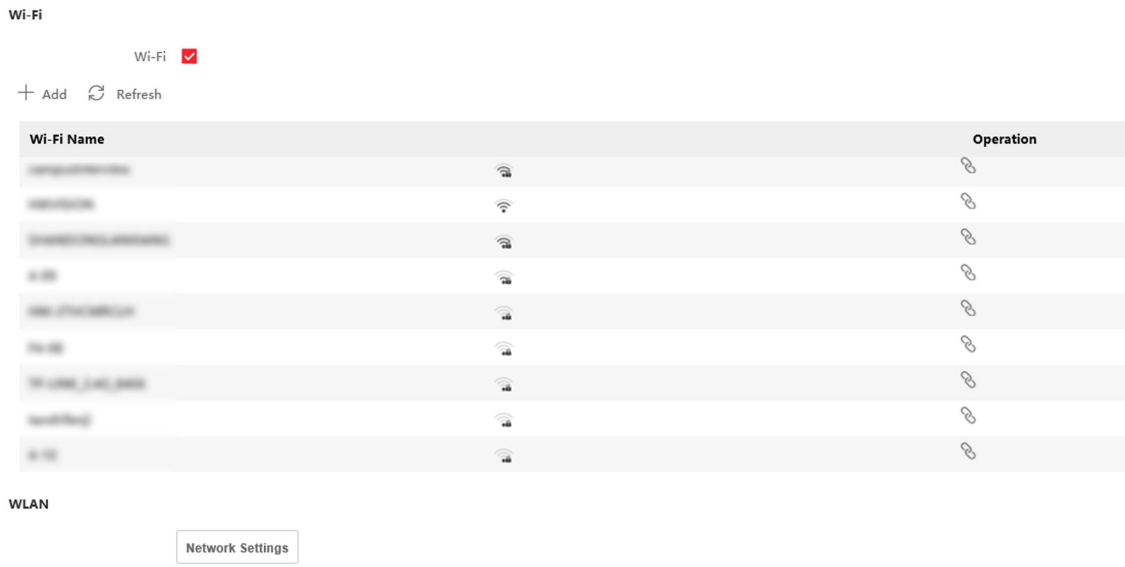



**Figure 5-8 Wi-Fi Settings Page**

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**.

## Device Hotspot

Set the device hotspot.

Click **System and Maintenance → System Configuration → Network → Network Settings → Device Hotspot** .

Click **Enable Device Hotspot** to enable the function and view the device hotspot name.

**Note**

By default, the hotspot name is the AP_Device Serial No.

Click **Save**.

## Set Port via PC Web

Click **System and Maintenance → System Configuration → Network → Network Service** .

**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 → RTSP** .

**RTSP**

It refers to the port of real-time streaming protocol.

## Set ISUP Parameters via PC Web

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** .
2. Check **Enable**.
3. Set the ISUP version, server address, device ID, and the ISUP status.

**Note**

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

4. Set the ISUP listening parameters, including ISUP alarm center IP address/domain name, ISUP alarm center URL, and ISUP alarm center port.
5. Click **Save**.

## Platform Access via PC Web

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 the checkbox of **Custom**, and you can set the server address by yourself.
4. Enter the verification code.
5. 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.

6. Click **Save** to enable the settings.

## Bluetooth Settings

You can enable bluetooth function.

Click **Configuration → Network → Network Settings → Bluetooth** .

**Open**

Enable **Open** to enable the bluetooth function.

**Device Name**

You can edit the device name connected to the bluetooth.

**Connection Status**

You can view the connection status.

**Open Door via Bluetooth**

After enabling this function, you can open doors via HikCentral Connect or HikCentral Access Control.

**Note**

You should add devices to the HCC or HCAC before opening door via bluetooth. Via HCAC, you can also realize the auto door open function. for details, see the HCAC's user manual.

## VoIP Account Settings

You can realize voice call by network.

**Steps**

1. Go to **System and Maintenance → System Configuration → Network → Device Access → VoIP**.
2. Enable **VoIP Gateway**.
3. Set **Register User Name**、**Registration Password**、**Server IP Address**、**Server Port**、**Expiry Time**、**Register Status**、**Number**、**Display User Name.**

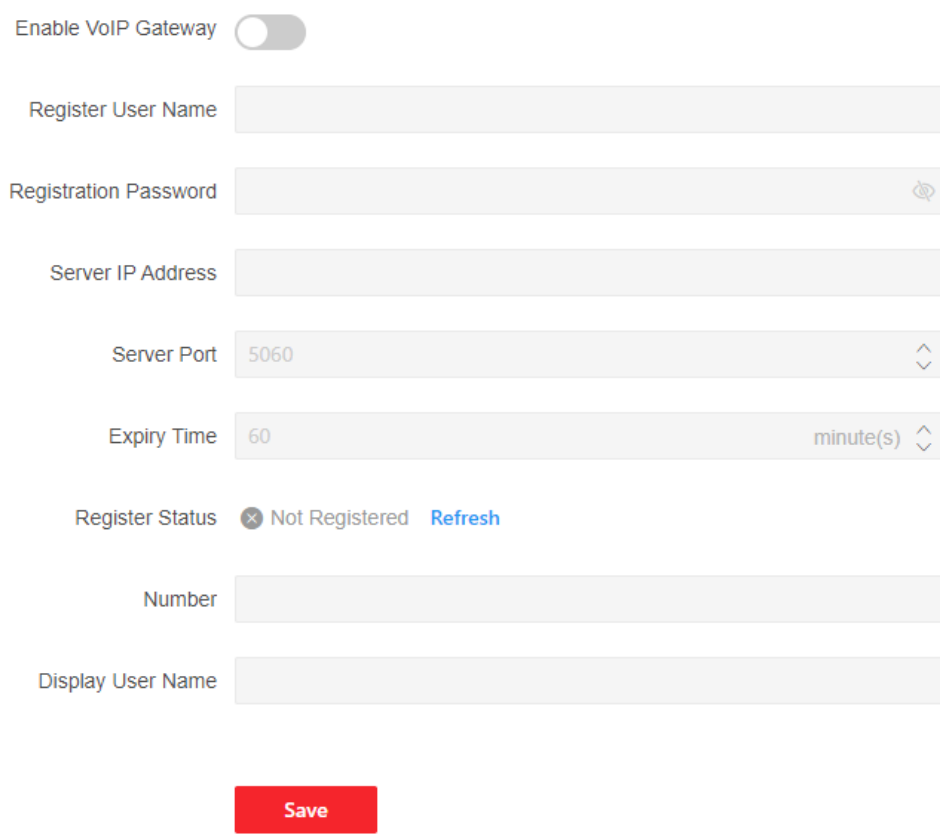



**Figure 5-9 VoIP Account Settings**

**Registration Password**

Enter the registration password for communication via SIP server. The registration password for the SIP server is configured usually in the main station's SIP settings.

**Server IP Address**

Enter the main station's IP address that used for VoIP communication. At this time the main station is used as a SIP server. Other intercom devices should registered to this server address to realize communication.

**Number / Display User Name**

The device displayed call number and user name.

4. Click **Save**.

## 5.11.10 Set Video and Audio Parameters via PC Web

### Configure Video Parameters via Web Browser

You can set quality, resolution and other parameters of device camera.

Click **System and Maintenance → System Configuration → Video/Audio → Video** to enter the settings page.

Set camera name, stream type, video type, resolution, bit rate type, video quality, frame rate, Max. bitrate, video encoding and I frame interval.

Click **Save**.

### Configure Audio Parameters via PC Web

You can set device volume.

Go to **System and Maintenance → System Configuration → Video/Audio → Audio**.

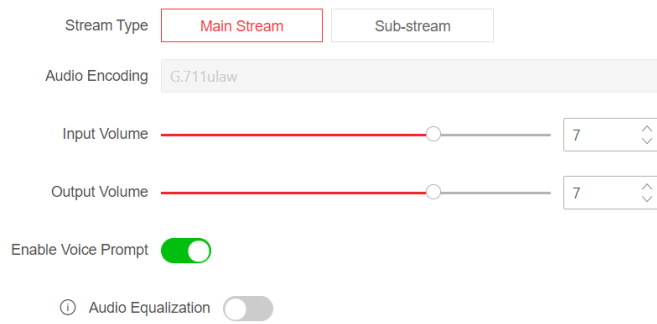



**Figure 5-10 Audio**

Set stream type and audio encoding according to your actual needs. Slide to set input and output volume.

Slide to enable **Voice Prompt**.

You can enable **Audio Equalization**, the device wil auto adjust frequency by audio algorithm to improve audio quality and equalize audio effect.

Click **Save**.

### 5.11.11 Image Parameters Settings

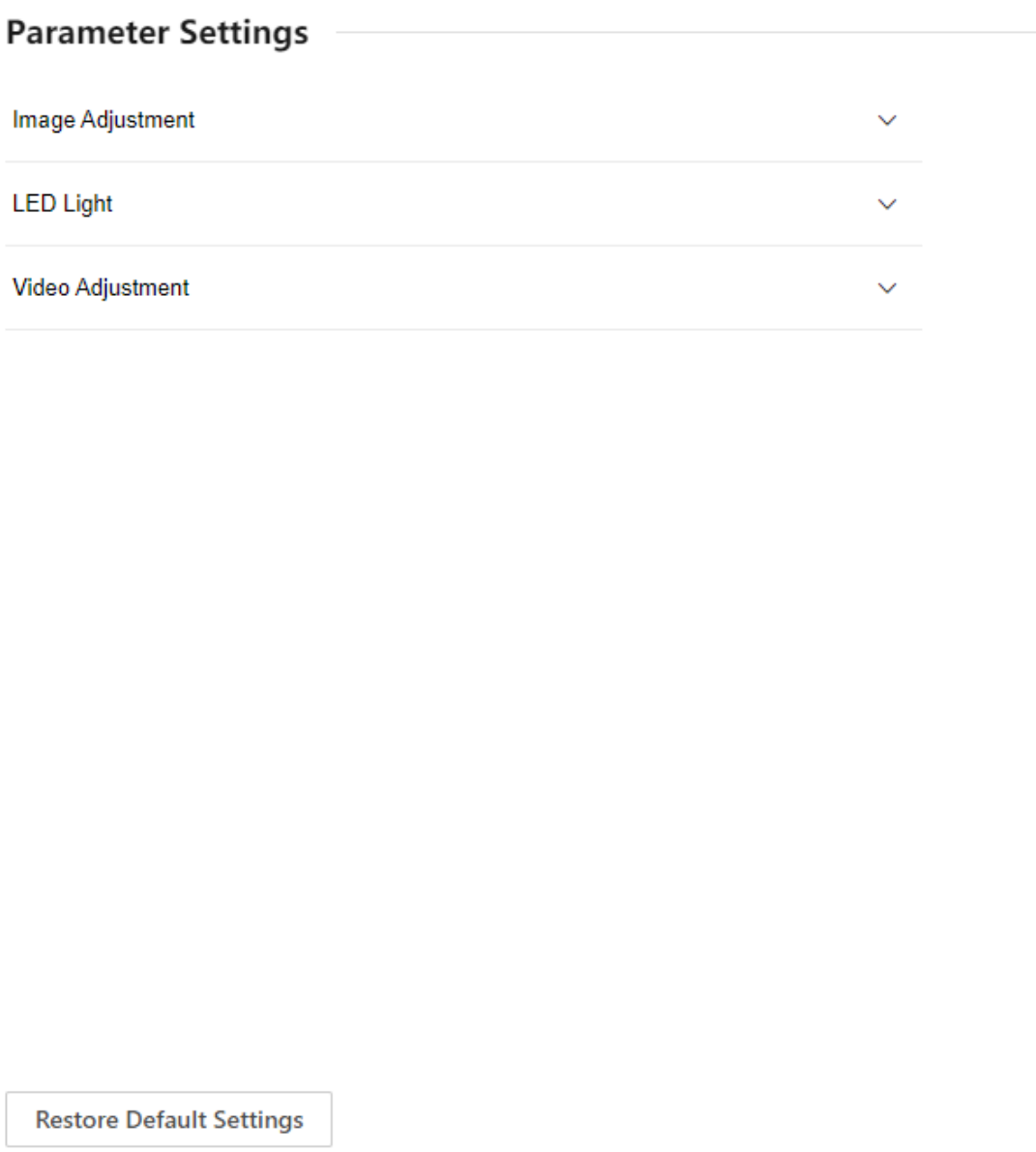



**Figure 5-11 Display Settings**

## Set Brightness/Contrast/Saturation/Sharpness via PC Web

You can set picture information such as brightness, contrast, saturation and sharpness of live view page.

Click **System and Maintenance → System Configuration → Image → Display Settings** to enter the settings page.

**Image Adjustment**

Drag the block or enter numbers to set brightness, contrast, saturation and sharpness.

Click **Restore Default Settings** to restore the to the default.

## Set LED Light via PC Web

You can adjust the brightness of the supplement light.

**Steps**

1. Click **System and Maintenance → System Configuration → Image → Display Settings** to enter the settings page.
2. Set the type, mode and brightness of the supplement light.
3. **Optional:** Click **Restore Default Settings** to restore the to the default.

## Set Video Standard via PC Web

You can set the video standard of live view page.

Click **System and Maintenance → System Configuration → Image → Display Settings** to enter the settings page.

**Video Adjustment**

Set the video frame rate during remote preview. You need to reboot the device to make the new settings effective.

**PAL**

25 frames per second. Suitable for mainland China, Hong Kong (China), the Middle East countries, Europe countries, etc.

**NTSC**

30 frames per second. Suitable for the USA, Canada, Japan, Taiwan (China), Korea, the Philippines, etc.

Click **Restore Default Settings** to restore the to the default.

### 5.11.12 Set Event Detection via PC Web

After setting the motion detection event, if there is moving objects trigger the rule, the device will report to the platform.

Click **System and Maintenance → System Configuration → Event → Event Detection**.

Enable **Motion**.

Set the motion detection area on the live view part of the page.

Click  , and draw an area in the live view page. When there is moving objects into the area, an alarm will be triggered.

Click  to delete the area.

Click  to capture pictures.

Click  to start recording. Click again to stop. The recording will be saved to local PC.

Click  to view the live view in full screen mode.

**Sensitivity**

Set the sensitivity that will trigger the rule. The higher the sensitivity, the easier to trigger the rule.

**Arming Schedule**

Exit the time schedule.

Click **Edit**, and click **Arm**. On the time schedule, you can draw the arming duration. Click **Save**. In the arming duration, if there is rule triggered, it will linked to report to platform.

**Notify Surveillance Center**

After enabling the function, if there is rules triggered, the device will report to platform.

**HTTP**

After enabling the function, if there is rules triggered, the device will report to platform by HTTP.

Click **Save**.

### 5.11.13 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**.

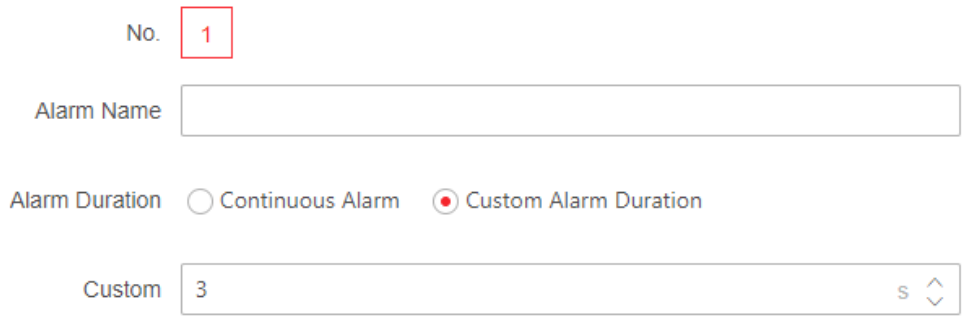



**Figure 5-12 Alarm Settings**

**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.

### 5.11.14 Access Configuration

### Set RS-485 Parameters via PC Web

You can set the RS-485 parameters including the peripheral, address, baud rate, etc.

Click **System and Maintenance → System Configuration → Access Configuration → RS-485** .

Select the RS-485's protocol from the drop-down list.

Check **Enable RS-485**, and set the parameters.

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

**No.**

Set the RS-485 No.

**Peripheral Type**

Select a peripheral from the drop-down list according the actual situation. You can select from **Card Reader**, **Extension Module**, **Access Controller**, or **Disable**.

**Note**

After the peripheral is changed and saved, the device will reboot automatically.

**RS-485 Address**

Set the RS-485 Address according to your actual needs.

**Note**

If you select **Access Controller**: If connect the device to a terminal via the RS-485 interface, set the RS-485 address as 2. If you connect the device to a controller, set the RS-485 address according to the door No.

**Baud Rate**

The baud rate when the devices are communicating via the RS-485 protocol.

## Set Wiegand Parameters via PC Web

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** .

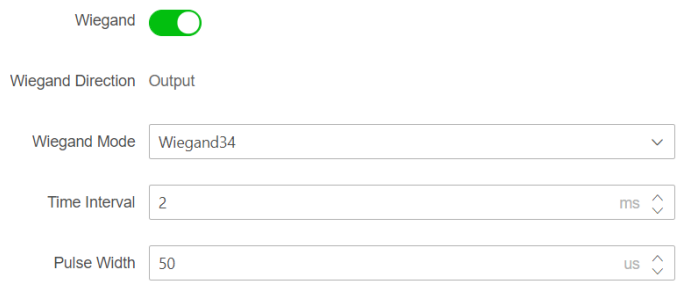



**Figure 5-13 Wiegand Page**

2. Check **Wiegand** to enable the Wiegand function.
3. Set a transmission direction.

**Output**

The can connect an external access controller. And the two devices will transmit the card No. via Wiegand 26 or 34.

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.

## Elevator Control via PC Web

**Steps**

1. Click **System and Maintenance → System Configuration → Access Configurations → Elevator Control Parameters** .

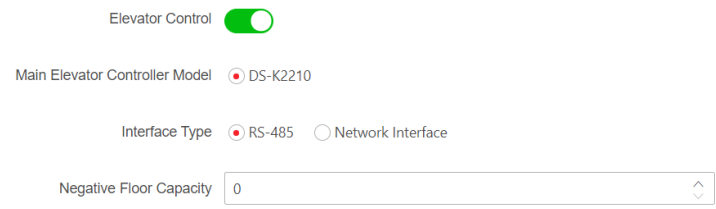



**Figure 5-14 Elevator Control**

2. Enable **Elevator Control**.
3. Set the elevator parameters.

**Main Elevator Controller Model**

View the elevator model.

**Interface Type**

Select a communication type from the drop-down list for elevator communication.

If you select **RS-485**, make sure you have connected the device to the elevator controller with RS-485 wire.

If you select **Network Interface**, enter the elevator controller's IP address, port No., user name, and password for communication.

**Negative Floor Capacity**

Set the negative floor number.

**Note**

- Up to 4 elevator controllers can be connected to 1 device.
- Up to 10 negative floors can be added.
- Make sure the interface types of elevator controllers, which are connected to the same device, are consistent.

## 5.12 System and Maintenance

### 5.12.1 Reboot

You can reboot the device.

Click **System and Maintenance → Maintenance → Restart** to enter the settings page.

Click **Restart** to reboot the device.

### 5.12.2 Upgrade

#### Upgrade Locally via PC Web

You can upgrade the device locally.

Click **System and Maintenance → Maintenance → Upgrade** to enter the settings page.

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

#### Online Upgrading via PC Web

You can upgrade the device online.

Click **System and Maintenance → Maintenance → Upgarde** to enter the settings page.

Click**Check for Updates**to check whether there is updated versions.

If the device is connected to the network and added to Hik-Connect App, you can tap **Device Upgrade → Online Upgrade** on device for upgrading when there is an updated version in Hik-Connect App.

### 5.12.3 Restoration

#### Restore to Factory Settings via Web Browser

You can restore device to factory settings.

Click **System and Maintenance → Maintenance → Backup and Reset** to enter the settings page.

Click **Restore All**, all parameters will be restored to the factory settings. You should activate the device before usage.

### Restore to Default Settings via PC Web

You can restore device to default settings.

Click **System and Maintenance → Maintenance → Backup and Reset** to enter the settings page.

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

## 5.12.4 Export Device Parameters via PC Web

Export device parameters.

Go to **System and Maintenance → Maintenance → Backup and Reset** .

**Backup**

Click **Export** to export device parameters.

**Note**

Export device parameters and import those parameters to other devices.

## 5.12.5 Import Device Parameters via PC Web

Import the configuration parameters.

Go to **System and Maintenance → Maintenance → Backup and Reset** .

**Import Config File**

Click and select a file from local PC. Click **Import**.

## 5.12.6 Device Debugging

You can set device debugging parameters.

### 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.

### 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**.

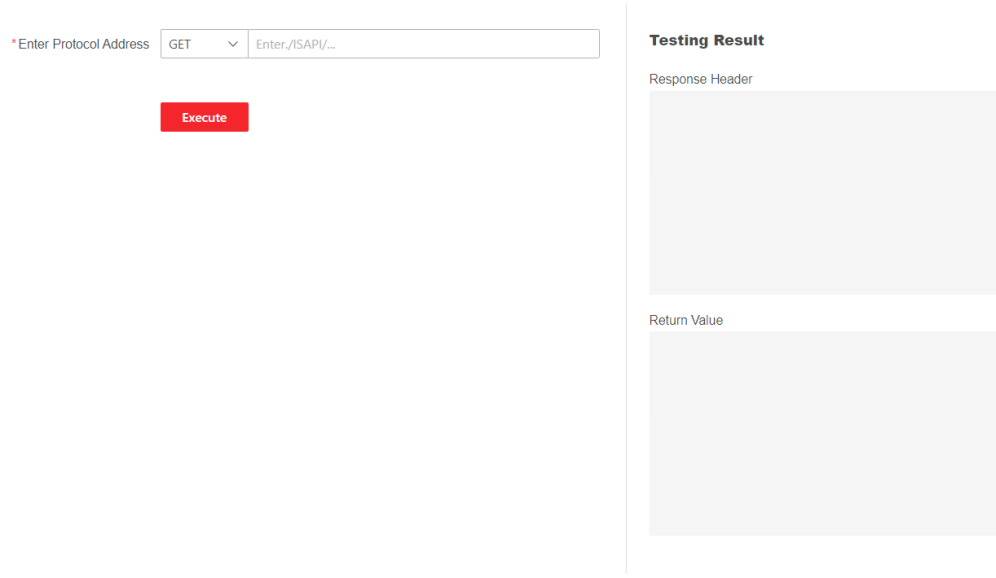



**Figure 5-15 Protocol Testing**

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

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

## 5.12.7 View Log via PC Web

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.

## 5.12.8 Security Mode Settings

Set the security mode for logging in the client software.

On the Device for Management page, click **Maintenance and Security → Security → Security Service** .

Select a security mode, and click **Save**.

**Security Mode**

High security level for user information verification when logging in the client software.

**Compatible Mode**

The user information verification is compatible with the old client software version when logging in.

### 5.12.9 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 Self-signed Certificate

**Steps**

1. Go to **System and Maintenance → Safe → Certificate Management** .
2. In the **Certificate Files** area, select a **Certificate Type** from the drop-down list.
3. Click **Create**.
4. Input certificate information.
5. Click **OK** to save and install the certificate.

   The created certificate is displayed in the **Certificate Details** area.

   The certificate will be saved automatically.
6. Download the certificate and save it to an asking file in the local computer.
7. Send the asking file to a certification authority for signature.
8. Import the signed certificate.
   1) Select a certificate type in the **Import Key** area, and select a certificate from the local, and click **Import**.
   2) Select a certificate type in the **Import Communication Certificate** area, and select a certificate from the local, and click **Import**.

#### Import Other Authorized Certificate

If you already has an authorized certificate (not created by the device), you can import it to the device directly.

**Steps**

1. Go to **System and Maintenance → Safe → Certificate Management** .
2. In the **Import Key** and **Import Communication Certificate** areas, select certificate type and upload certificate.

3. Click **Import**.

## Import CA Certificate

**Before You Start**

Prepare a CA certificate in advance.

**Steps**

1. Go to **System and Maintenance → Safe → Certificate Management** .
2. Create an ID in the **Import CA Certificate** 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 6 Configure the Device via the Mobile Browser

### Set Network by TCP/IP

If device has connected to wired network, set the device IP address and enable the device hotspot via the Web browser. For details, see the PC web browser's settings.
Enable the phone's Wi-Fi function and search the device hotspot.
Open the phone's browser and enter the device IP address to enter the mobile browser's settings page.

### Set Network by Wi-Fi

If device has connected to Wi-Fi, set the device IP address and enable the device hotspot via the Web browser. For details, see the PC web browser's settings.
Enable the phone's Wi-Fi function and search the device hotspot.

**Note**

The device and the phone should be in the same Wi-Fi environment, or you cannot visit the device by the phone's browser.

Open the phone's browser and enter the device IP address to enter the mobile browser's settings page.

## 6.1 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**.

## 6.2 Forget Password

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

**Steps**

1. On the login page, tap **Forget Password**.
2. Select Verification Mode.

   **Security Question Verification**

   If you have set security questions on the device or mobile web, you can enter the answers to reset the password. Tap **Security Question Verification**, and tap **Next**.
3. Enter the answer of the security question, and tap **Next**.
4. Enter the new password and confirm it.
5. Tap **Next**.

## 6.3 Account Security Settings

Change the reserved phone No. and when you forgot the password, you can use the phone No. to change the login password.

**Steps**

**Note**

Only the device and the phone are in the same LAN, can you see the settings.

1. Tap → **User Management** → ··· → **Account Security Settings**.
2. Change the reserved phone No. When you forget your login password, you can enter the phone No. to change the password.
3. Tap **Save**.

## 6.4 Home

You can view the door status, enter the configuration page via shortcut entry, view the network status, and view basic information.

### Door Status

You can view the door status. And control the door status.

### Shortcut Entry

Tap the configuration function name and enter the page.

### Network Status

You can view the network connection status.

### Basic Information

You can view the device model, serial No., and version, or enter the basic information page.

## 6.5 Configuration

### 6.5.1 View Device Information

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

Tap → **System Settings** → **Basic Information** to enter the configuration page.

You can view the device name, language, model, serial No., version, IO input number, local RS-485 number, number of alarm output, register number, Mac address, and device capacity, etc.

### 6.5.2 Time Settings

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

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

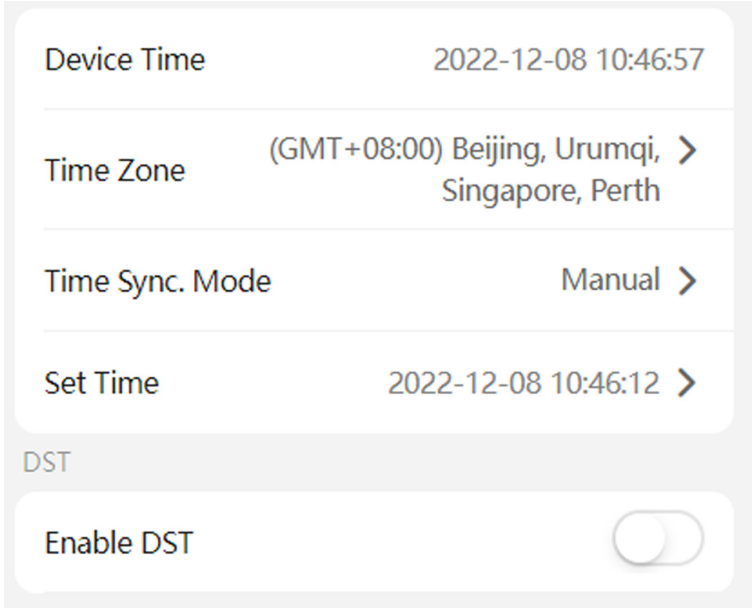



**Figure 6-1 Time Settings**

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.

### 6.5.3 Set DST

**Steps**

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

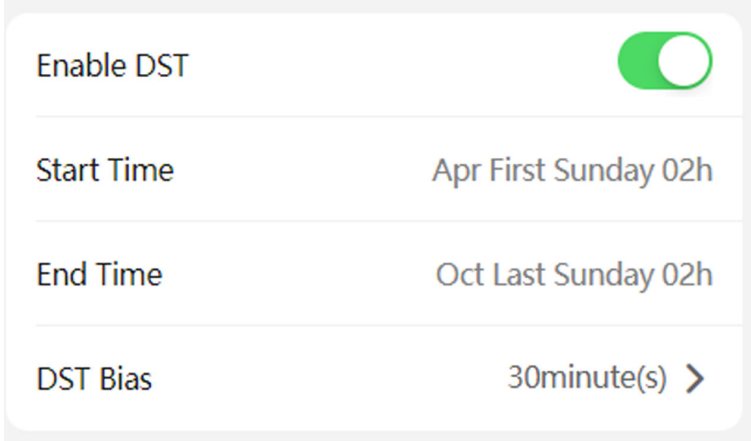



**Figure 6-2 DST**

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

### 6.5.4 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.

### 6.5.5 Network

You can configure the wired network, Wi-Fi and hotspot parameters of the device.

### Wired Network

Set wired network.

Tap → **Communication Settings** → **Wired Network** 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 Settings

Set the Wi-Fi parameters of the device.

**Before You Start**

After the device is added to the App, you can enabled the device Wi-Fi function. And then you can set eh Wi-Fi parameters in the mobile web.

**Steps**

1. On the home page, tap → **Communication Settings** → **Wi-Fi**.
2. Enable **Wi-Fi**.
3. Select a Wi-Fi in the list and enter the password to connect.
4. **Optional:** Add a Wi-Fi.
   1) Slide the page to the end and tap **Add Network**.
   2) Enter **Wi-Fi Name**, and select the Wi-Fi's **Encryption Type**.
   3) Tap **OK**.
5. **Optional:** Set WLAN.
   1) Set the connected Wi-Fi's name, and view the network details.
   2) Tap **WLAN Settings**.
   3) Set the WLAN parameters.

**Enable DHCP**

Enable **DHCP** to **Auto DNS**, the device will allocate the IP and DNS automatically.

**Disable DHCP**

Manually set the IP and DNS server.

4) Tap **Save**.

**Result**

After Wi-Fi and WLAN settings, you can enter the WLAN IP address in the mobile browser to login the device.

## Set Device Hotspot

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

**Steps**

1. Tap → **Communication 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 and HTTPS according to actual needs when accessing the device via network.

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

## 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 **Register Status** and **Binding Status**.
5. You can tap **Bind An Account → View QR Code** , scan the QR code to bind an acount.
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. Tap **Save** to save the settings.

### VoIP Settings

Tap → **Device Access → VoIP** to enter the settings page.

Tap to **Enable VoIP Gateway**.

Set VoIP parameters and tap **Save** to save the parameters.

## 6.5.6 User Management

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

**Steps**

**1.** Tap → **Person Management** to enter the settings page.

**2.** Add user.

1) Tap**+**.

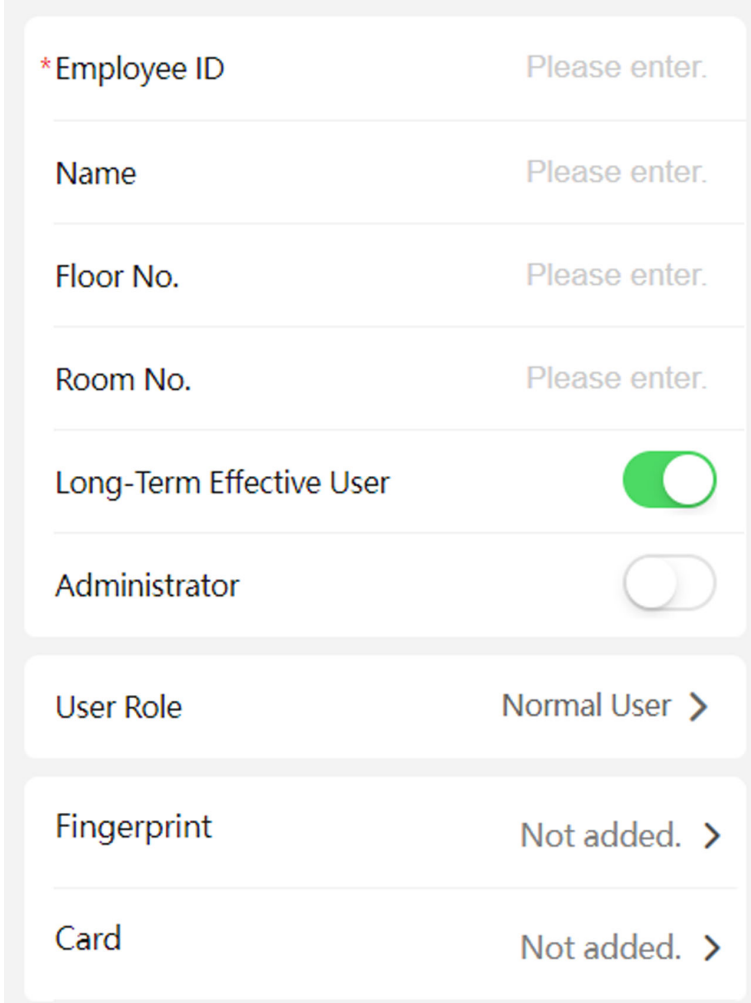



**Figure 6-3 Add User**

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.

**Floor No./Room No.**

Enter the floor No./room No.

**Long-Term Effective**

Set the user permission as long-term effective.

**Start Date/End Date**

Set **Start Date** and **End Date** of user permission.

**Administrator**

If the user needs to be set as administrator, you can enable **Administrator**.

**User Role**

Select your user role.

**Fingerprint**

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

**Card**

Add card. Tap **Add Card**. Enter the **Card No.**, or present the card on the device and tap **Read**, and select the **Property**. Tap **Save** to add the card.

**Password**

**Note**

- Before configuring passwords, it is necessary to clarify whether the password is device-set personal PIN or a platform-applied personal PIN. If it is a device-set personal PIN, it can be created and edited on Web and cannot be created and edited on the platform; If it is a platform-applied personal PIN, it needs to be configured on the platform and cannot be edited on the Web.
- Make sure **Password Mode** is selected as **Device Password**.

Tap **Person Management → Add** to enter the Add Person page.

Enter the password.

3) Tap **Save**.

3. Tap the user that needs to be edited in the user list to edit the information.
4. Tap the user that needs to be deleted in the user list, and tap to delete the user.
5. You can search the user by entering the employee ID or name in the search bar.

### 6.5.7 Event Search

Tap → **Event Search**.

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

**Note**

Support searching for names within 32 digits.

The result will display in the list.

### 6.5.8 Audio Settings

You can enable or adjust the audio.

Tap → **Audio**.

Enable **Enable Voice Prompt** according to actual needs. The device will prompt voice instructions. You can also adjust the audio volume.

You can enable **Audio Equalization**, the device will auto adjust frequency by audio algorithm to improve audio quality and equalize audio effect.

Tap **Save**.

### 6.5.9 Access Control Settings

### Set Authentication Parameters

Set Authentication Parameters.

**Steps**

1. Tap → **Access Control** → **Authentication Settings** .
2. Tap **Save**.

**Terminal**

You can configure the device parameters. If you select main card reader, you need to configure the following parameters: Terminal Type, Terminal Model, Enable Card Reader, Authentication, Recognition Interval (s), Minimum Card Swiping Interval (s), Max. Authentication Failed Attempts Alarm/Alarm of Max. Failed Attempts, Enable Tampering Detection and Enable Card No. Reversing.

**Terminal Type**

Select terminal type as **Main** or **Sub**.

**Double Door Control**

After enabling, the device can control 2 doors. Anti-passback functions will be invalid.

**Terminal Model**

Get Terminal Model information.

**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.

**External Devices Authentication**

After enabling, external devices require authentication.

**Max. Authentication Failed Attempts Alarm/Alarm of Max. Failed Attempts**

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

**Enable Tampering Detection**

Enable the anti-tamper detection for the card reader.

**Enable Card No. Reversing**

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

**QR Code**

Enable the function and the user can use QR code to open the door.

**Note**

- Disable the IR light if enabling the QR code function. For details, see . The picture in low illumination environment may be affected due to disabling the IR light.
- Set QR code function via HCC or HCEC, you should select compatible to 1.0 or 2.0. 2.0 is recommended.

**Enable Bluetooth**

Enter **Device Name** and select **Bluetooth Encryption Version**. You can control the device remotely.

## Set Door Parameter

Set door parameters, including door name, open duration, exit button type, door remain open duration with first person, door open timeout alarm, door contact, extended open duration, duress code, super password, and dismiss code.

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

After settings, tap **Save**.

**Enable Door 2**

- Door 2 needs to be enabled first before configuration.
- Only PoE series devices support this function.

**Door No.**

You can select door No. to set parameters.

**Online Status**

You can view the door online status.

**Door Name**

Create a name for the door.

**Open Duration**

Set the door unlocking duration after swiping the card.

**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**

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.

**Door Opening Timeout Alarm Threshold**

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.

**Door Contact**

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

**Extended Open Duration**

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

**Duress Code**

The door can open by inputting the duress code when there is duress. At the same time, the client can report the duress event.

**Super Password**

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

**Dismiss Code**

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

**Note**

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

## Access Control and Elevator Control

**Steps**

1. Tap → **Access Control** → **Elevator Control Parameters**.
2. Enable **Elevator Control**, and set **Negative Floor Capacity**, **Main Elevator Controller Model**, and **Interface Type**.

**Note**

- Only main door station supports elevator control.
- If you select **Network Interface** as interface type, you should set server address, port, user, and password.

3. Tap **Save**.

## Terminal Parameters

You can set terminal parameters for accessing.

Tap → **Access Control** → **Terminal Parameters** .

You can set **Working Mode** as **Access Control Mode**. The access control mode is the device normal mode. You should authenticate your credential for accessing.

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

## Set Card Security

Configure cards for the device.

Tap → **Access Control** → **Card Security** .

Configure card parameters, and click **Save**.

**Enable NFC Card**

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

**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.

**Note**

It is recommended to encrypt sector 13.

**Enable EM Card**

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

**Note**

If the peripheral card reader supports presenting EM card, the function is also supported to enable/disable the EM card function

**Enable DESFire Card**

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

**DESFire Card Read Content**

After enable the DESFire card content reading function, the device can read the DESFire card content.

### 6.5.10 Access Configuration

### Set RS-485 Parameters

You can set the RS-485 parameters including the peripheral, address, baud rate, etc.

Tap → **Access Configuration** → **RS-485** .

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

**Peripheral Type**

Select a peripheral from the drop-down list according the actual situation. You can select from **Card Reader**, **Extension Module**, or **Access Controller**.

**Note**

After the peripheral is changed and saved, the device will reboot automatically.

**RS-485 Protocol**

**Private**

The device can connect with the third party device via RS-485.

**OSDP**

Standard RS-485 protocol.

**RS-485 Address**

Set the RS-485 Address according to your actual needs.

**Note**

If you select **Access Controller**: If connect the device to a terminal via the RS-485 interface, set the RS-485 address as 2. If you connect the device to a controller, set the RS-485 address according to the door No.

**Baud Rate**

The baud rate when the devices are communicating via the RS-485 protocol.

**Data Bit**

The data bit when the devices are communicating via the RS-485 protocol.

**Stop Bit**

The stop bit when the devices are communicating via the RS-485 protocol.

**Parity/Flow Ctrl/Communication Mode**

Enabled by default.

**Output Type**

Set the output type according to your actual needs.

## Secure Door Control Unit

Select the door to be controlled by Secure Door Control Unit to ensure safer door opening.

**Steps**

1. Tap → **Access Configuration** → **Secure Door Control Unit** to enter the settings page.
2. Select the door.

**Note**

Selecting Door 1 means that Door 1 will be controlled by secure door control unit to ensure safer door opening.

3. You can view the Secure Door Control Unit status.

## 6.5.11 Call Settings

## Set Device No. via Mobile Web

The device can be used as access control device, door station, or outer door station. You can set the device number for video intercom.

Tap → **Intercom** → **Device ID Settings**.

Tap **Save**.

If select the device type as **Door Station** or **Access Control Device**, you can set the device period No., building No., unit No., floor No., and door station No.

**Device Type**

The device can used as door station. You can select other device type from the drop-down list.

**Community No.**

Enter the device community No. (period No.)

**Building No.**

Enter the device building No.

**No.**

Customize device No.

**Note**

- If the device type is **Door Station** or **Access Control Device**, the No. should be between 0 and 99.
- After changing the device type or No., you should reboot the device to take effect.

**Unit No.**

Enter the device unit No.

**Floor No.**

Enter the device floor No.

If select the device type as **Outer Door Station** , you can set the device period No., and outer door station No.

**Device Type**

The device can used as out door station. You can select other device type from the drop-down list.

**Community No.**

Enter the device community No. (period No.)

**No.**

Customize device No.

**Note**

- If the device type is **Outer Door Station**, the No. should be between 1 and 99.
- After changing the device type or No., you should reboot the device to take effect.

**Note**

After changing the device type or No., you should reboot the device to take effect.

## Session Settings

You can set the registration password, main station IP and private server IP, and you can enable protocol 1.0 according to your actual needs.

Tap → **Intercom** → **Session Settings**.

**Registration Password**

Set the registration password of the main station for communication. Set the registration password of the main station for communication.

**Main Station IP**

Enter the main station's IP address that used for communication.

**Private Server IP**

Refers to the SIP server IP. Enter the main station's IP address that used for communication. At this time the main station is used as a SIP server. Other intercom devices should registered to this server address to realize communication.

**Enable Protocol 1.0**

If enabled, the door station can be registered to the main station by old protocol version. If disabled, the door station can be registered to the main station by new protocol version.

After configuration, you can achieve communication between access control devices and video intercom door station, indoor station, main station, platforms, etc.

Click **Save**.

## Call Settings

you can set Max. communication duration between the main station and other devices.

Tap → **Intercom** → **Call Settings**.

**Max. Communication Time**

The Maximum communication time when the main station and the other devices are in the call. When the communication time exceeds the configured time, the communication will stop. The Max. communication time range is 90 s to 120 s.

## Number Settings

Set SIP number for the room. The rooms can communicate with each other via SIP number.

**Steps**

1. Tap → **Intercom** → **Number Settings**.
2. Enter **Room No.** and **SIP Number1**.
3. Tap **Save**.
4. **Optional:** Tap the configured room No., edit or tap **+Add** to add another SIP number.
5. **Optional:** Tap **Delete** to delete room number.

## Press Button to Call via Mobile Web

You can press the button to call.

**Steps**

1. Tap → **Intercom** → **Press Button to Call**.
2. Tap **1** to enter the page.

**Note**

- When you check Call Specified Indoor Station, you should set the linked room's No.
- By default, you can press the button to call indoor station, and hold the button to call center.

3. Select the item that the button linked to. When select **Call Specified Indoor Station**, you should set the room's No.
4. Tap **Save**.

## 6.5.12 Set Privacy Parameters via Mobile Web

Set picture uploading and storage parameters.

Tap → **Privacy Settings**.

**Picture Uploading and Storage**

You can enable **Save Pictures After Linked Capture** or **Upload Picture After Linked Capture**. The captured pictures will upload or save to the platform.

Tap **Save**.

## 6.5.13 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 → **Configuration** → **Security** → **Password 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**.

### 6.5.14 Upgrade and Maintenance

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

#### Restart Device

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

#### Upgrade

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

**Note**

Do not power off during the upgrading.

#### Restore Parameters

Tap → **Default** .

**Restore to Default Settings**

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

**Restore to Factory Settings**

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

### 6.5.15 View User Document

View the user document.

**Note**

Only when you enter the mobile web by IP address, can you view the user document. Login by hot spot does not support the function.

Tap to enter the page.

Tap **View Online Document** to view the user manual.

### 6.5.16 Open Source Software Licenses

You can view the open source software licenses.

Tap to enter the page.

Tap **Open Source Software Licenses**.

### 6.5.17 Log Out of Mobile Web

Log out of the configuration page on the mobile web.

On the home page, tap → **Log Out** , and tap **OK** to log out of the web.

If you need to go to the configuration page, please enter user name and password again.

# Chapter 7 Other Platforms to Configure

You can also configure the device via iVMS-4200 Client Software or HikCentral Access Control. For details, see the platforms' user manual.

**iVMS-4200 Client Software**

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

***http://enpinfodata.hikvision.com/analysisQR/showQR/ca930247***

**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. |

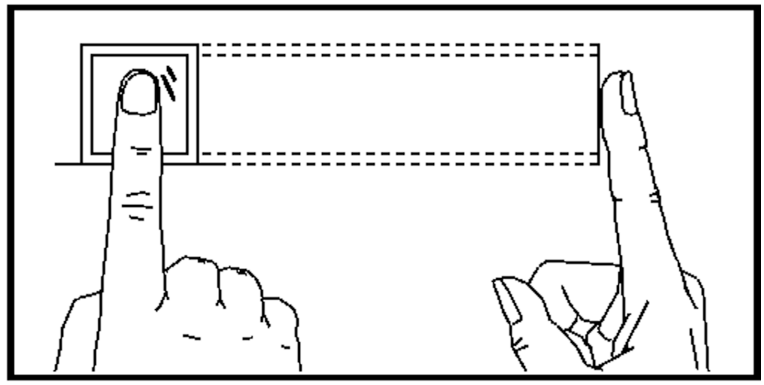
# Appendix C. Tips for Scanning Fingerprint

## Recommended Finger

Forefinger, middle finger or the third finger.

## Correct Scanning

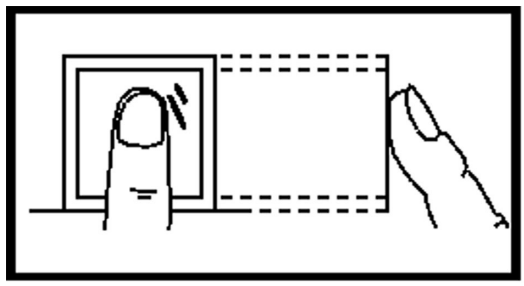
The figure displayed below is the correct way to scan your finger:



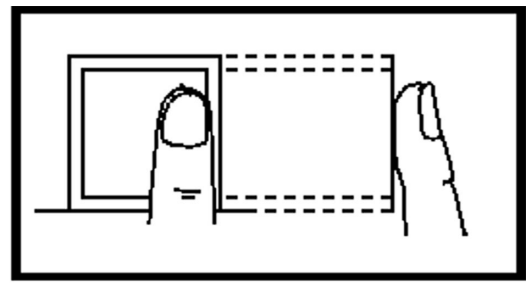
You should press your finger on the scanner horizontally. The center of your scanned finger should align with the scanner center.

## Incorrect Scanning

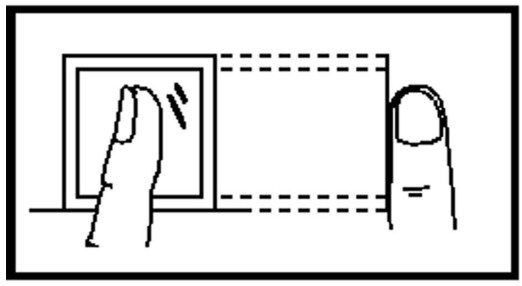
The figures of scanning fingerprint displayed below are incorrect:



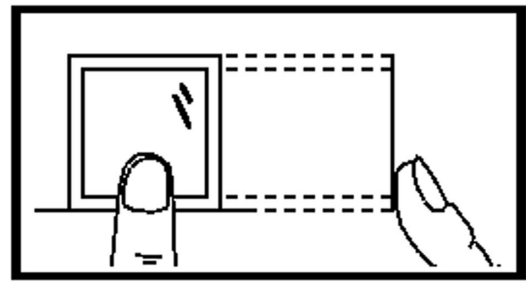
Vertical



Edge I



Side



Edge II

### Environment

The scanner should avoid direct sun light, high temperature, humid conditions and rain.
When it is dry, the scanner may not recognize your fingerprint successfully. You can blow your finger and scan again.

### Others

If your fingerprint is shallow, or it is hard to scan your fingerprint, we recommend you to use other authentication methods.
If you have injuries on the scanned finger, the scanner may not recognize. You can change another finger and try again.


See Far, Go Further