DS-K1T323 Series Face Recognition 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

CE

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

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



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



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

Safety Instruction

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

The precaution measure is divided into Dangers and Cautions:

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

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

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

⚠ Danger:

- All the electronic operation should be strictly compliance with the electrical safety regulations, fire prevention regulations and other related regulations in your local region.
- 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:

- 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.
- Biometric recognition products are not completely applicable to anti-spoofing environments. If you require a higher security level, use multiple authentication modes.

Available Models

Product Name	Model
Face Recognition Terminal	DS-K1T323MBFWX-E1
	DS-K1T323MBWX-E1
	DS-K1T323MBWX-QRE1
	DS-K1T323EBFWX-E1
	DS-K1T323EBWX-E1
	DS-K1T323EBWX-QRE1

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.

© Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

Contents

Chapter 1 Appearance 1

Chapter 2 Installation 2

2.1 Installation Environment 2

2.2 Surface Mounting 2

Chapter 3 Wiring 8

3.1 Terminal Description 8

Chapter 4 Activation 9

4.1 Activate via Mobile Web 9

4.2 Activate via Web Browser 9

4.3 Activate via SADP 10

4.4 Activate Device via iVMS-4200 Client Software 11

Chapter 5 Configure the Device via the Mobile Browser 13

5.1 Login 13

5.2 Overview 14

5.3 Forget Password 14

5.4 Configuration 15

5.4.1 View Device Information 15

5.4.2 Time Settings 15

5.4.3 Set DST 16

5.4.4 User Management 16

5.4.5 Network Settings 17

5.4.6 User Management 20

5.4.7 Search Event 21

5.4.8 Access Control Settings 22

5.4.9 Video Intercom Settings 25

5.4.10 Audio Settings 27

5.4.11 Face Parameters Settings 27
5.4.12 Upgrade and Maintenance 29
5.4.13 View Online Document 29
5.4.14 View Open Source Software License 29
Chapter 6 Operation via Web Browser 30
6.1 Login 30
6.2 Forget Password 30
6.3 Download Web Plug-In 30
6.4 Help 31
6.4.1 Open Source Software Licenses 31
6.4.2 View Online Help Document 31
6.5 Logout 31
6.6 Quick Operation via Web Browser 31
6.6.1 Change Password 31
6.6.2 Select Language 32
6.6.3 Time Settings 32
6.6.4 Privacy Settings 33
6.6.5 Administrator Settings 33
6.6.6 No. and System Network 34
6.7 Person Management 35
6.8 Device Management 37
6.9 Access Control Management 37
6.9.1 Overview 37
6.9.2 Search Event 39
6.9.3 Door Parameter Configuration 39
6.9.4 Authentication Settings 41
6.9.5 Set Face Parameters 45
6.9.6 Card Settings 48

6.9.7 Linkage Settings 50
6.9.8 Set Working Mode via PC Web 50
6.9.9 Set Remote Verification 50
6.9.10 Privacy Settings 51
6.9.11 Call Settings 52
6.10 System Configuration 56
6.10.1 View Device Information via PC Web 56
6.10.2 Set Time 56
6.10.3 Change Administrator's Password 57
6.10.4 Account Security Settings via PC Web 58
6.10.5 View Device Arming/Disarming Information via PC Web 58
6.10.6 Network Settings 58
6.10.7 Set Video and Audio Parameters via PC Web 63
6.10.8 Image Parameter Settings 63
6.10.9 Access Configuration 65
6.10.10 Time and Attendance Settings 65
6.11 Preference Settings 68
6.11.1 Set Sleep Time via PC Web 68
6.11.2 Customize Authentication Desk via PC Web 68
6.11.3 Set Notice Publication via PC Web 68
6.11.4 Customize Prompt Voice via PC Web 69
6.11.5 Set Authentication Result Text via PC Web 69
6.12 System and Maintenance 70
6.12.1 Reboot 70
6.12.2 Upgrade 70
6.12.3 Restoration 71
6.12.4 Export Device Parameters via PC Web 71
6.12.5 Import Device Parameters via PC Web 71

6.12.6 Device Debugging 72
6.12.7 View Log via PC Web 75
6.12.8 Advanced Settings via PC Web 75
6.12.9 Security Management 75
6.12.10 Certificate Management 75
Chapter 7 Other Platforms to Configure 78
Appendix A. Symbol Conventions 79
Appendix B. Tips for Scanning Fingerprint 80
Appendix C. Tips When Collecting/Comparing Face Picture 82
Appendix D. Tips for Installation Environment 84

Chapter 1 Appearance

Refer to the following contents for detailed information of the face recognition terminal:

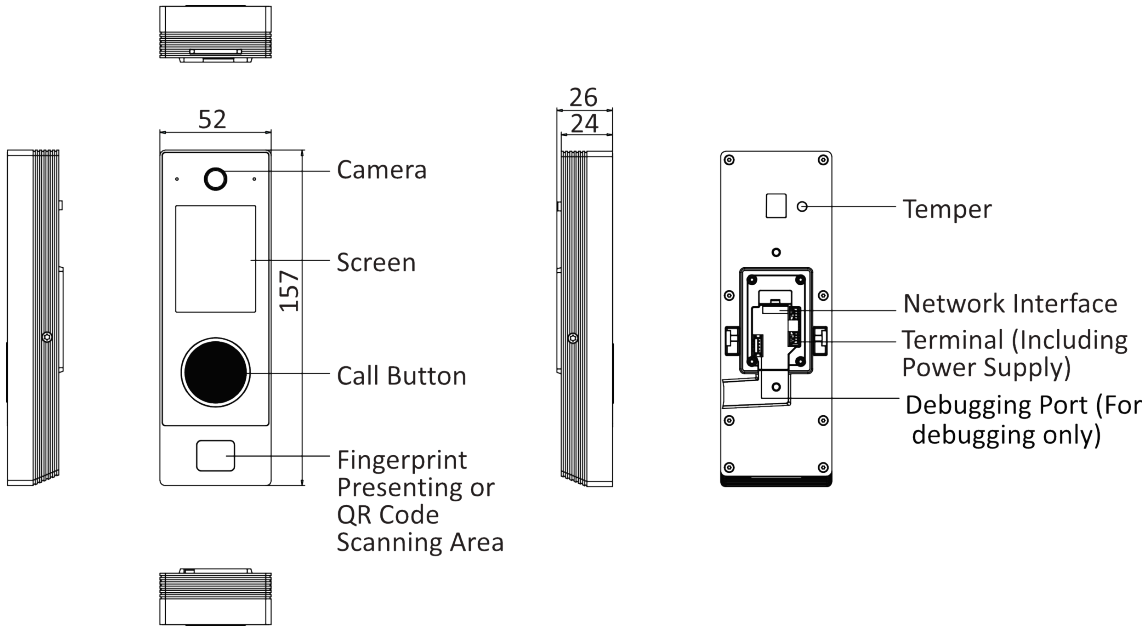


Figure 1-1 Appearance 1

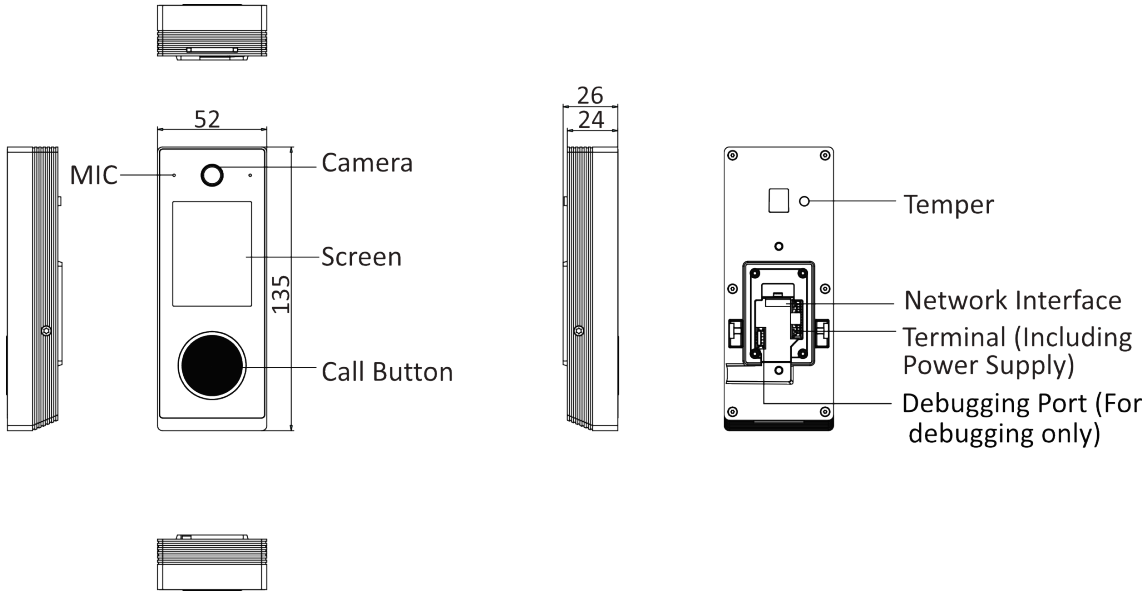


Figure 1-2 Appearance 2

Chapter 2 Installation

2.1 Installation Environment

- The minimum bearing weight of the wall or other places should be 3 times heavier than the device weight.
- • Please prepare the following tools and accessories: screwdriver (self purchased), screws, cables, and adapters (self purchased).

2.2 Surface Mounting

Steps

1. Make sure the cables are threaded through the hole.

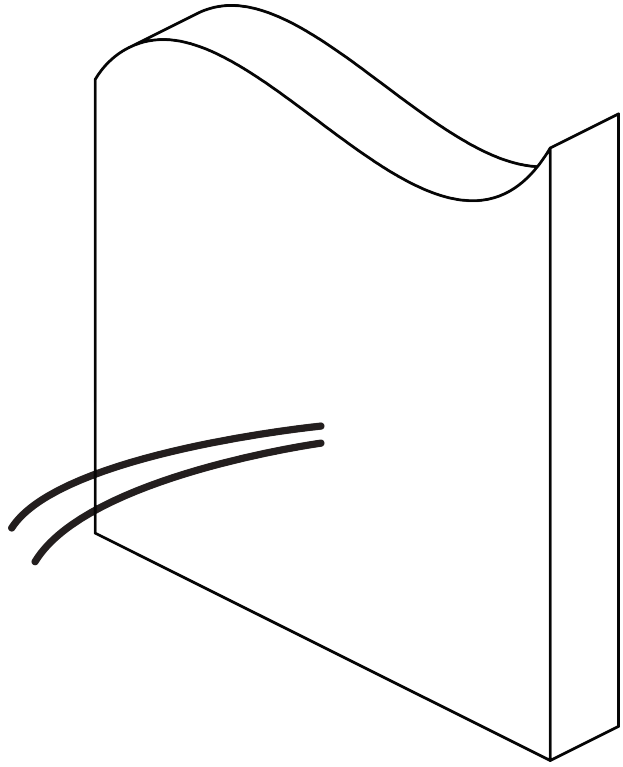


Figure 2-1 Thread Cables

2. Secure the mounting plate on the gang box with two supplied screws (SC-KA4×25).

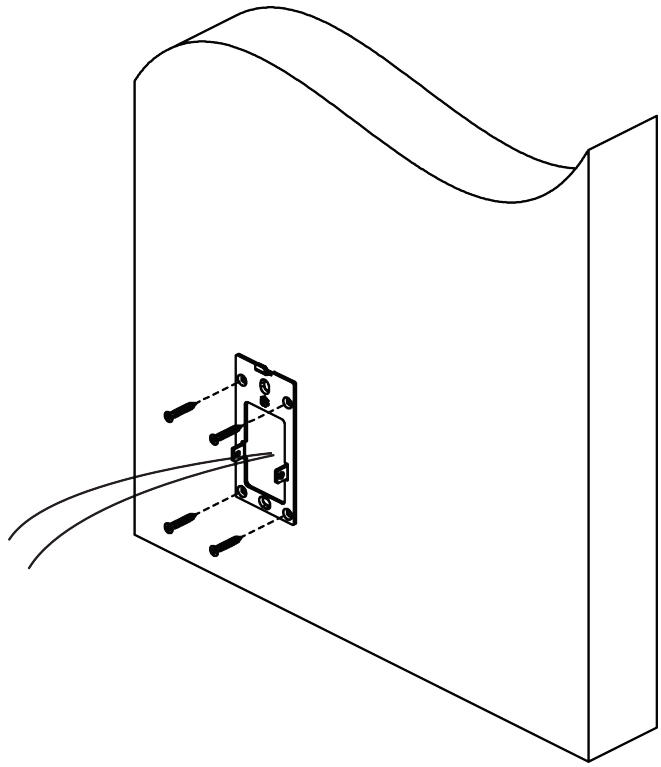


Figure 2-2 Secure Mounting Plate

3. Use a screwdriver to loosen the screws on the back cover of the device and remove the back cover.

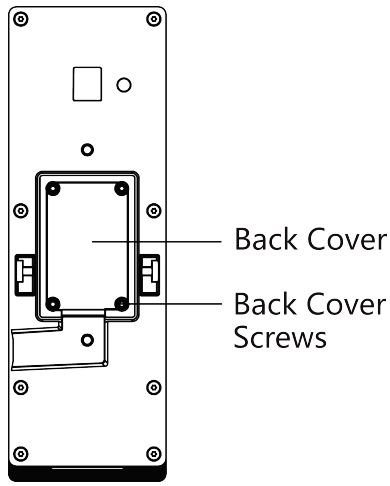


Figure 2-3 Remove Device Back

4. Complete the wiring. See the wiring diagram below (1.4) for details. And Fix the back cover.

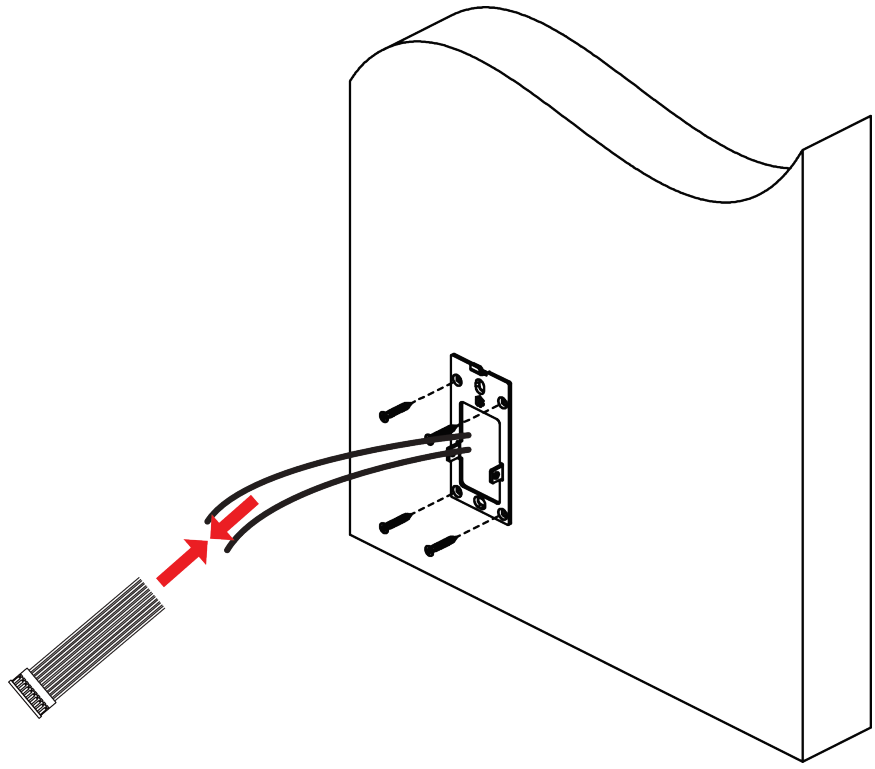


Figure 2-4 Wiring

5. Apply silicone sealant among the cable wiring area to keep the raindrop from entering.

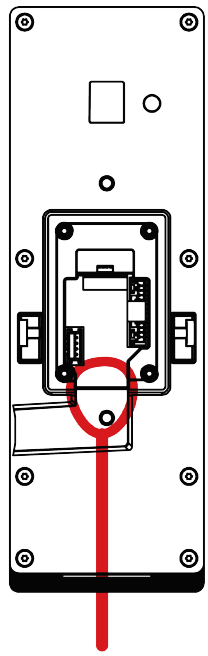


Figure 2-5 Apply silicone sealant

6. Hang the device into the plate from top to bottom. Secure the device on the mounting plate with 2 supplied screw (SC-KM3X8-T10-SUS-NL).

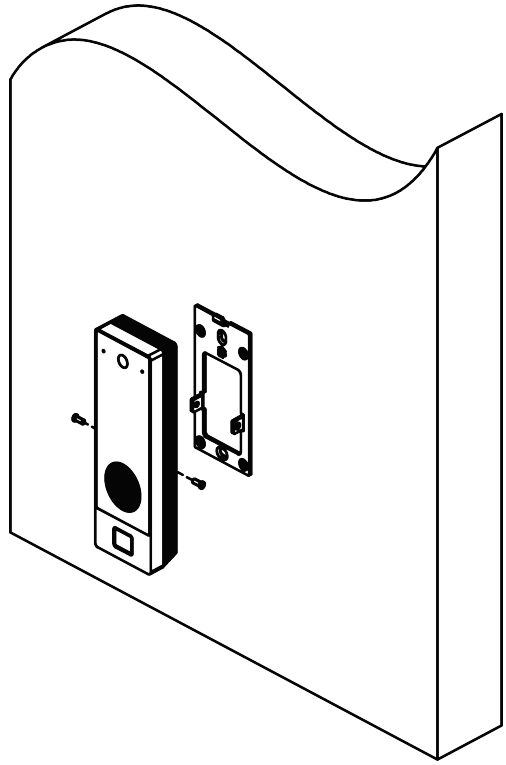


Figure 2-6 Secure Device

7. Complete the installation.

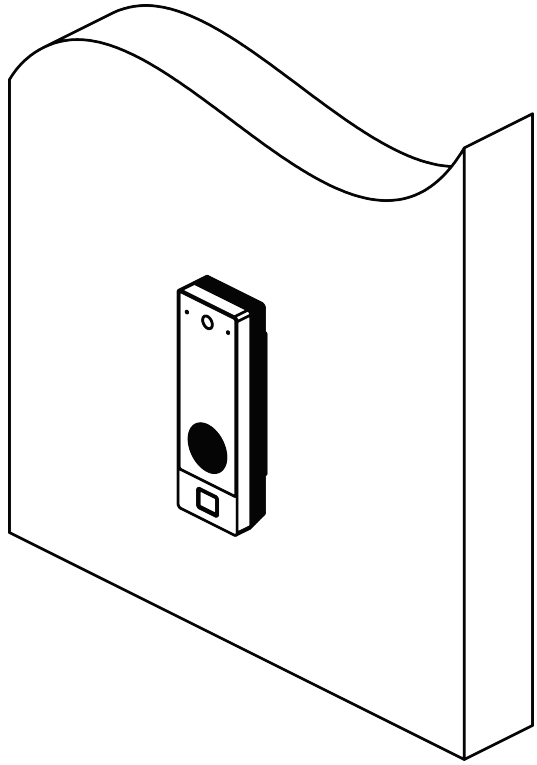


Figure 2-7 Complete Installation

Chapter 3 Wiring

The device supports connecting to the door lock, the exit button, the alarm output/input devices, the Wiegand card reader, the access controller, and the power supply. You can wire the peripherals according to the descriptions below.

If connect the Wiegand card reader with the access controller, the face recognition terminal can transmit the authentication information to the access controller and the access controller can judge whether to open the door or not.

Note

- If the cable size is 18 AWG, you should use a 12 V switched-mode power supply. And the distance between the power supply and the device should be no more than 20 m.
- If the cable size is 15 AWG, you should use a 12 V switched-mode power supply. And the distance between the power supply and the device should be no more than 30 m.
- If the cable size is 12 AWG, you should use a 12 V switched-mode power supply. And the distance between the power supply and the device should be no more than 40 m.

3.1 Terminal Description

The terminal's diagram is as follows:

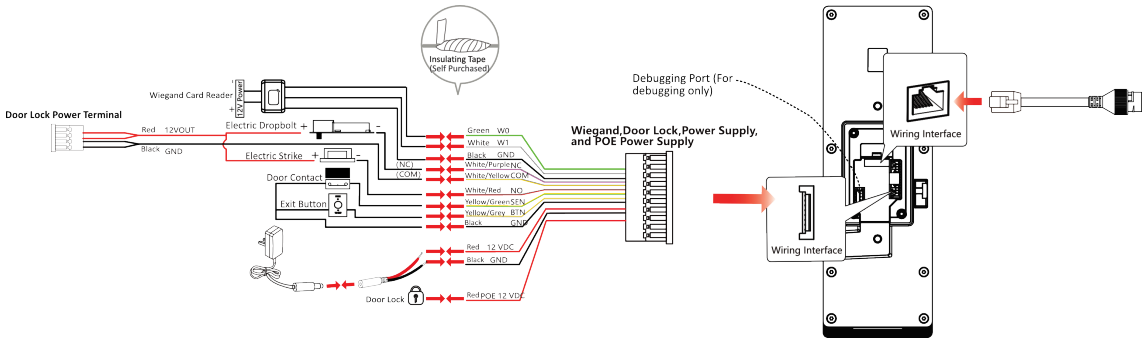


Figure 3-1 Terminal Diagram

Chapter 4 Activation

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

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

The default values of the device are as follows:

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

4.1 Activate via Mobile Web

You can activate the device via mobile web.

Steps

1. After the device is powered on, the hotspot is enabled by default. Search for and connect to the device hotspot on your phone.

   Note

   - Device hotspot name is AP_ Serial No., and initial password of device hotspot is Serial No. After restarting or switching from non-AP mode to AP mode after activation, the hotspot password will be changed to the activation password.
   - You can log in to the mobile web client only when the device is in AP mode.

2. Open the browser address bar of the mobile phone and enter 192.168.8.1 to enter the activation interface.
3. Set the activation password and confirm it.

   Note

   - The password must be 8 to 16 characters long.
   - The password must be composed of two or more combinations of numbers, lowercase letters, uppercase letters, and special characters.
   - The password cannot contain the user name, 123, admin, 4 or more consecutive digits in increments or decrement, or the same symbol.

4. Tap **Activate Device**.

4.2 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

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

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

4.3 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.

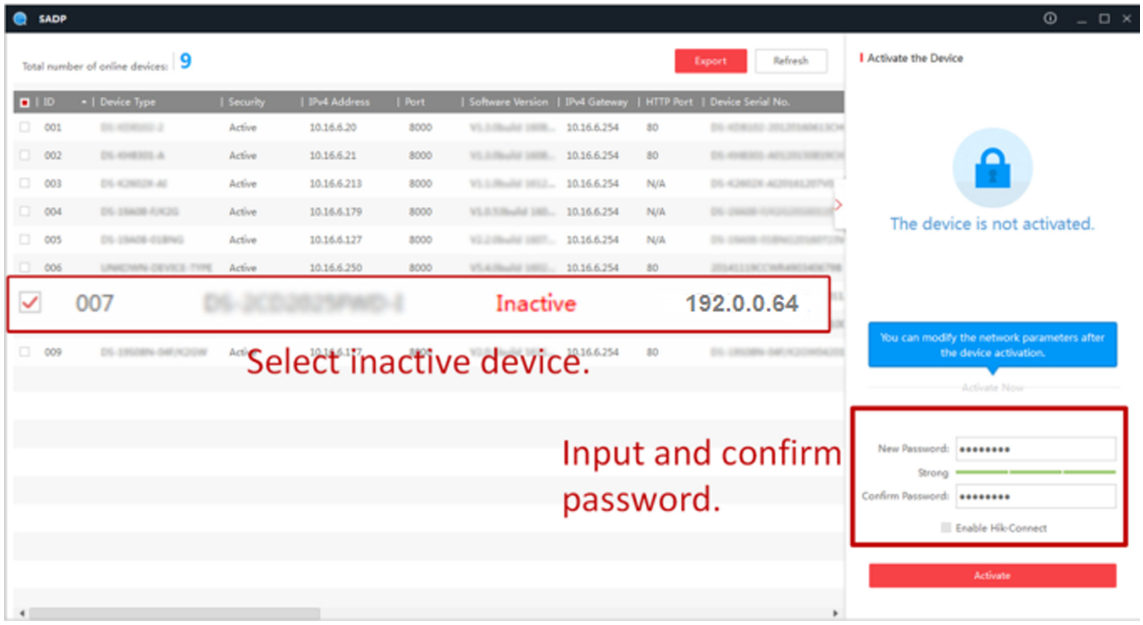
Caution

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.

Note

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

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



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

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

4.4 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 5 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.

Set Network by AP

When the device is powered on for the first time, the device hotspot is enabled by default and will automatically turn off after 30 minutes; it must then be manually enabled. Use a mobile phone to open WLAN, search for the device hotspot, and connect to it (hotspot name: AP_device serial number; password: device serial number). After a successful connection, the phone will automatically redirect to the mobile web page, where you can perform activation and configuration. If the browser page does not open automatically after connecting to the hotspot, go to the browser and enter ***www.acsvis.com*** to access it.

5.1 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**.

5.2 Overview

You can view the door status, network status and basic information, and set person management, smart settings, authentication settings, and door parameters via shortcut entry.

Function Descriptions:

Door Status

/ / /

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

Shortcut Entry

You can set person management, smart settings, authentication settings, and door parameters via shortcut entry.

Network Status

You can view the connected and registered status of wired network, wireless network, bluetooth, ISUP and Hik-Connect.

Basic Information

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

5.3 Forget Password

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

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

Select **Verification Mode**.

Security Question Verification

Answer the security questions.

E-mail Verification

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

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

5.4 Configuration

5.4.1 View Device Information

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

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

You can device name, language, model, serial No., version, number of channels, IO input number, IO output number, number of alarm input and output, Mac address, factory information and device capacity, etc.

5.4.2 Time Settings

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

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

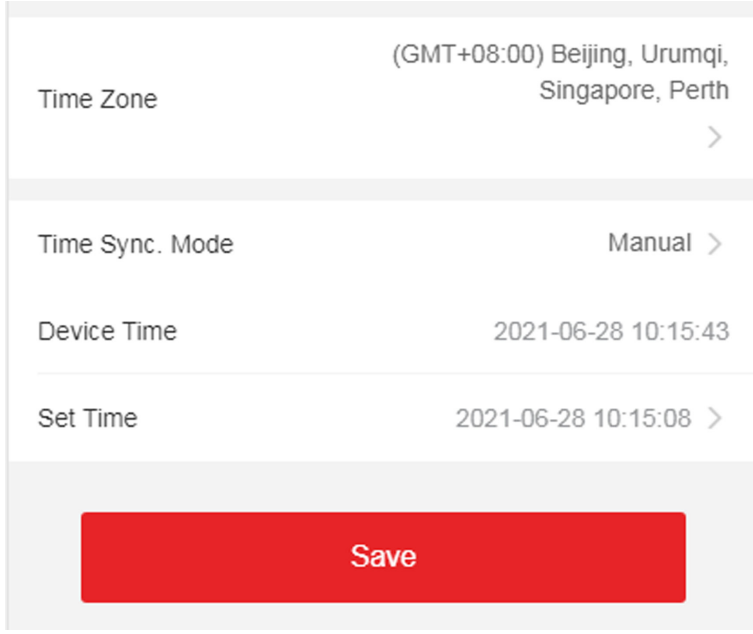


Figure 5-1 Time Settings

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.

5.4.3 Set DST

Steps

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

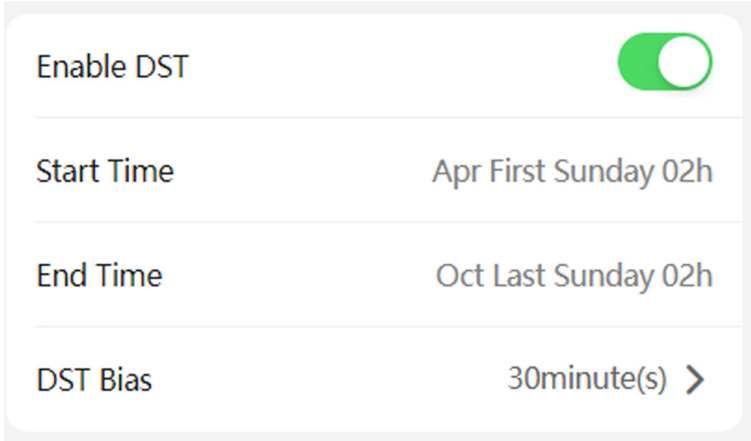


Figure 5-2 DST

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

5.4.4 User Management

Steps

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

Note

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using 8-16 characters, including at least two kinds

of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.

5.4.5 Network Settings

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, 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 automatically.

DNS Server

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

Set Wi-Fi Parameters

Set the Wi-Fi parameters for device wireless connection.

Steps

Note

The function should be supported by the device.

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

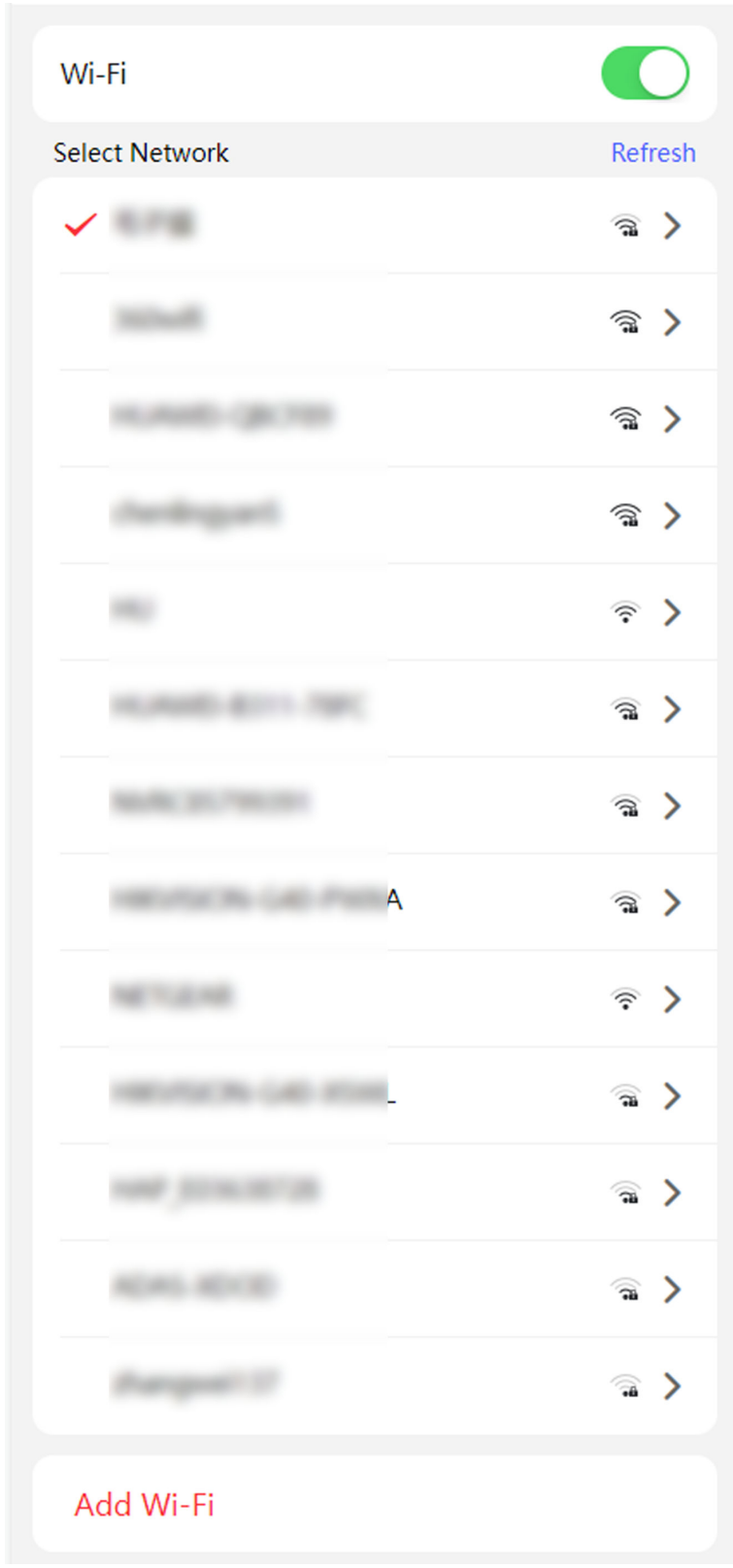


Figure 5-3 Wi-Fi

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

Set 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.

Device Hotspot

After enabling the device hotspot, you can use the mobile phone to connect the hotspot and set.

Note

You can set the parameters only when you connect the device by hotspot. If you login the device by IP address, the function is not supported.

On the home page, tap → **Network Settings** → **Device Hotspot** .

Enable **Device Hotspot** and tap **Save**.

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. Enable **Video Encryption**, and create the password and confirm it.

Note

After adding the device to APP, you need to enter the video encryption password to live view the device.

6. You can tap **Bind An Account → View QR Code** , scan the QR code to bind an acount.
7. 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.

5.4.6 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**+**.
   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.

Long-Term Effective User

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**.

Attendance Check Only

After enabling, the person will not be granted with access control permission.

User Role

Select your user role.

Face

Add Face picture. Tap **Face**, then tap **Camera** to add face or tap **Choose from Album** to import the face.

Fingerprint

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

Card

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

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.

5.4.7 Search Event

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

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.

5.4.8 Access Control Settings

Set Authentication Parameters

Set Authentication Parameters.

Steps

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

Terminal

Select terminal for settings.

Terminal Type/Terminal Model

Get terminal description. They are read-only.

Enable Authentication Device

Enable the authentication function.

Authentication

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

Continuous Face Recognition Interval (s)

You can set the interval between 2 continuous recognition of a same person during the authentication. In the configured interval, Person A can only recognized once. If another person (Person B) has recognized during the interval, Person A can recognized again.

Authentication Interval

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

Alarm of Max. Failed Attempts

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

Main Interface Mode

You can set the **Main Interface Mode** as **Authentication Mode** or **Simple**.

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.

Set Door Parameters

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

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

Name

You can create a name for the door.

Open Duration

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

Exit Button Type

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

Door Remain Open Duration with First Person (min)

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

Door Open Timeout Alarm

An alarm will be triggered if the door has not been closed within the configured time duration.

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

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

Unlock Password

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

Note

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

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.

Remote Authentication

After enabling the **Remote Authentication**, when authenticating, the device will upload authentication information to the platform, and the platform will confirm whether to open the door.

Verify Credential Locally

After enabling the function, the device will check permission but not estimate the plan template.

Timeout Period

You can set remote authentication timeout period.

Offline Remote Verifying Unlocking

After enabling the function, you can unlock remotely offline.

Result Return Mode

Set the result return mode.

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

Set Card Security

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

Set the parameters and tap **Save**.

Enable NFC Card

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

Enable M1 Card

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

M1 Card Encryption

M1 card encryption can improve the security level of authentication.

Sector

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

Enable EM Card

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

Note

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

Enable DESFire Card

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

Enable FeliCa Card

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

5.4.9 Video Intercom Settings

Device ID Settings

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

Steps

1. Tap → **Intercom** → **Device ID Settings** .
2. Set the following parameters.

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.

Period No.

Set the device period 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.

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.

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.

Period No.

Set the device period No.

Session Settings

Enable the communication between door station, main station, and video intercom server.

Steps

1. Tap → **Intercom** → **Session Settings** .
2. Set registration password, main station IP, private server IP and enable Protocol 1.0.

   Registration Password

   Activation password of the main station.

   Main Station IP

   IP address of the main station.

   Private Server IP

   IP address of the private server.

   Enable Protocol 1.0

   After enabling, the device is registered to the main station through the previous protocol. If disabled, the device is registered to the main station through the new protocol.
3. Tap **Save**.

Time Duration Settings

Set the Max. call duration.

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

Set the Max. communication time. Tap **Save**.

Note

The Max. call duration range is 90 s to 120 s.

Press Button to Call

Steps

1. Tap → **Intercom** → **Press Button to Call** .
2. Select the No. Select **Call Indoor Station**, **Call Specified Indoor Station**, **Call Management Center** or **APP** at your needs.

Note

If you check **Call Specified Indoor Station**, you need to enter the number of the indoor station.

Number Settings

You can call the room SIP to call the room.

Steps

1. Tap → **Intercom** → **Number Settings** .
2. Tap **+**, enter the **Room No.** and **SIP Number**.
3. Tap **Save**.

5.4.10 Audio Settings

Steps

1. Tap → **Audio** .
2. **Optional:** Set input and output volume.
3. Enable Voice Prompt according to your actual needs.

5.4.11 Face Parameters Settings

Set Face Parameters.

Face Parameters Settings

Tap → **Smart** → **Face Recognition Parameters** .

Face Anti-spoofing

Enable or disable the live face detection function. If enabling the function, the device can recognize whether the person is a live one or not.

Live Face Detection Security Level

After enabling the face anti-spoofing function, you can set the matching security level when performing live face authentication.

1:1 Matching Threshold

Set the matching threshold when authenticating via 1:1 matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate.

1:N Matching Threshold

Set the matching threshold when authenticating via 1:N matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate. The maximum value is 100.

Face Recognition Timeout Value (s)

Configure the timeout period for face recognition. If the face recognition time exceeds the configured value, the device will prompt the face recognition timeout.

Fingerprint Parameters

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

Fingerprint Security Level

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

Face Mask Detection Parameters

Face with Mask Detection

After enabling the face with mask detection, the system will recognize the captured face with mask picture. You can set face with mask1:N matching threshold, its ECO mode, and the strategy.

None

If the person do not wear a face mask when authenticating, the device will not prompt a notification.

Reminder of Wearing

If the person do not wear a face mask when authenticating, the device prompts a notification and the door will open.

Must Wear

If the person do not wear a face mask when authenticating, the device prompts a notification and the door keeps closed.

Face with Mask & Face (1:1)

Set the matching value when authenticating with face mask via 1:1 matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate.

Face with Mask 1:N Matching Threshold

Set the matching threshold when authenticating with face mask via 1:N matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate.

Note

The functions vary according to different models. Refers to the actual device for details.

Tap **Save** to save the settings.

5.4.12 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.

5.4.13 View Online Document

Tap → **View Online Document** . Tap **View Online Document**, you can scan the QR code with your mobile phone for details.

5.4.14 View Open Source Software License

Tap → **Open Source Software License** , and tap **Open Source Software License** to view the device license.

Chapter 6 Operation via Web Browser

6.1 Login

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

Note

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

Login via Web Browser

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

Login via Remote Configuration of Client Software

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

6.2 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.

6.3 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.

6.4 Help

6.4.1 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.

6.4.2 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.

6.5 Logout

Log out the account.

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

6.6 Quick Operation via Web Browser

6.6.1 Change Password

You can change the device password.

Click on the top right of the web page to enter the **Change Password** page. You can set security questions from the drop-down list and fill in the answers.

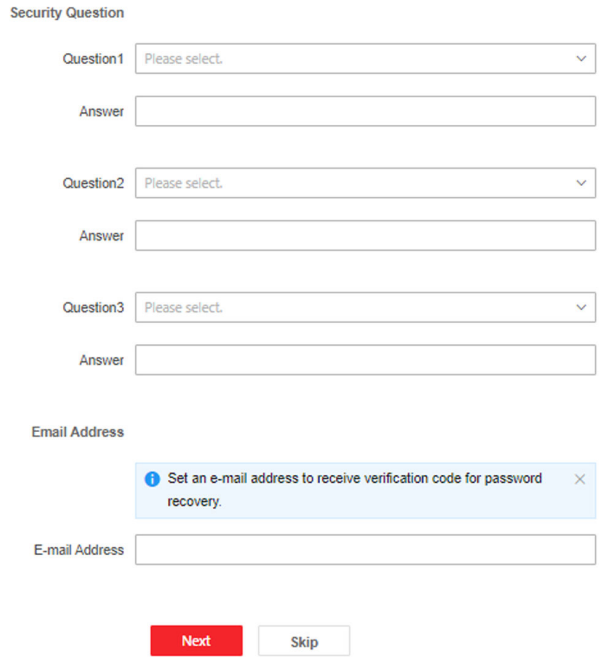


Figure 6-1 Change Password

Click **Next** to complete the settings. Or click **Skip** to skip the step.

6.6.2 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.

6.6.3 Time Settings

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

Time Zone

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

Time Sync.

NTP

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

Manual

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

Server Address/NTP Port/Interval

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

DST

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

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

6.6.4 Privacy Settings

Set the picture uploading and storage parameters.

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

Picture Uploading and Storage

Save Picture When Authenticating

Save picture when authenticating automatically.

Upload Picture When Authenticating

Upload the pictures when authenticating to the platform automatically.

Save Registered Picture

The registered face picture will be saved to the system if you enable the function.

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 parameter. Or click **Skip** to skip privacy settings.

6.6.5 Administrator Settings

Steps

1. Click in the top right of the web page to enter the wizard page.
2. Enter the employee ID and name of the administrator.
3. Select a credential to add.

Note

You should select at least one credential.

1) Click **Add Face** to upload a face picture from local storage.

Note

The uploaded picture should be within 200 K, in JPG、JPEG、PNG format.

2) Click **Add Card** to enter the Card No. and select the property of the card.

Note

Up to 5 cards can be supported.

3) Click **Add Fingerprint** to add fingerprints.

Note

Up to 10 fingerprints are allowed.

6.6.6 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.

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.

6.7 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.
If you select **Custom Type**, you can edit the name. The changed name will be applied to the device.
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.

Authentication Settings

Click **Person Management → Add** to enter the Add Person page.
Set the authentication type.
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 Face Picture

Click **Person Management → Add** to enter the Add Person page.
Click **+ Upload** to upload a face picture from the local PC.

Note

The picture format should be JPG or JPEG or PNG, and the size should be less than 200 kb.

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.

Device No. Settings

Click **Person Management → Add** to enter the Add Person page.
Add the person's basic information. Go to the Device No. module. Click **Add** and enter the person belonged room No. and floor No. Click **Add** or **Save and Continue**.

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.

6.8 Device Management

You can manage the linked device on the page.

Steps

1. Click **Device Management** to enter the settings page.
2. Click **Add** to add the indoor station or sub door station. Enter the parameters and click **Save** to add.
3. Click **Import** to download the template. Enter the information of the device in the template and click to import the template.
4. Click **Export** to export the information to the PC.
5. Select the device and click **Delete** to remove the selected device from the list.
6. Click **Refresh** to get the device information.
7. **Optional:** Set Device Information.

Edit Device Information	Click to edit device information.
Delete Device Information	Click to delete device information from the list.
Search Devices	Select **Status** and **Device Type** to search devices.

6.9 Access Control Management

6.9.1 Overview

You can view the live video of the device, linked device, person information, network status, basic information, and device capacity.

Function Descriptions:

Door Status

Click on the video to view the device live video.

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.

/ / /

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



You can record when starting live view.

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



Full screen view.

Controlled Status

You can control the door to be opened, closed, remaining open or remaining closed 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 page of Event Search. You can select event types, enter 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.

Link Device

You can view the quantity and status of linked devices.

Note

You can click **View More** to go to ***Device Management*** .

Person Information

You can view the added and not added information of person credentials.

Network Status

You can view the connected and registered status of wired network, wireless network, Hik-Connect, ISUP, and VoIP.

Basic Information

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

Device Capacity

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

6.9.2 Search Event

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

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

The results will be displayed on the right panel.

6.9.3 Door Parameter Configuration

Configure parameters for unlocking doors.

View Device Online Status

View and refresh the device status.

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

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

Set Door Name

Create door name.

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

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

Set Open Duration via PC Web

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

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

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

Click **Save**.

Set Door Open Timeout Alarm via PC Web

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

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

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

Click **Save**.

Set Lock Door when Door Closed

You can set lock door when door closed.

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

You can enable **Lock Door when Door Closed**.

Click **Save**.

Set Door Lock Status via Web Page

Select door lock's status according to wiring method.

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

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

Click **Save**.

Set 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 Door Lock Powering Off Status via PC Web

You can set the door lock status when the door lock is powering off.

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

Set **Door Lock Powering Off Status**. By default, it is remain closed.

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.

6.9.4 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**.

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**.

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 Recognition Interval via PC Web

Set the time interval between two continuous face recognitions when authenticating.

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

When you select the terminal as main or sub card reader, set recognition interval, and click **Save**.

Note

Please enter a number between 1 and 10.

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**.

Set Sub Card Reader Position

You can choose the position for the sub card reader.

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

When Sub Card Reader is selected as the Terminal, you can select the position of sub card reader as **Different Side from Main Card Reader**or**Same Side as Main Card Reader**. 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**.

6.9.5 Set Face Parameters

Enable/Disable Face Anti-spoofing via Web Browser

When enabled, the device can recognize whether the person is a live one or not.

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

Enable **Face Anti-spoofing** and click **Save**.

Enable or disable the live face detection function. When enabled, the device can recognize whether the person is a live one or not. If the face is not a live one, authentication will fail.

Set Anti-Spoofing Detection Level via PC Web

After enabling the face anti-spoofing function, you can set the matching security level when performing live face authentication.

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

Select the anti-spoofing detection level and click **Save**.

You can choose from general, advanced and professional. The higher the level, the lower the fake recognition rate and the higher the rejection rate.

Set Recognition Distance via PC Web

You can set the distance between the authenticating user and the device camera.

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

Select the recognition distance, and click **Save**.

Set Pitch Angle via PC Web

You can set the pitch angle of the lens during face recognition and authentication.

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

Note

Different models may support different parameters, please refer to the actual page.

Set **Pitch Angle** and click **Save**.

Set Yaw Angle via PC Web

You can set the yaw angle of the lens during face recognition and authentication.

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

Note

Different models may support different parameters, please refer to the actual page.

Set yaw angle, and click **Save**.

Set Face Picture Quality Grade for Applying via PC Web

The grade for face authentication needs to be higher than the threshold to be successful.

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

Note

Different models may support different parameters, please refer to the actual page.

Set **Face Picture Quality Grade for Applying** , the grade for face authentication needs to be higher than the threshold to be successful.

Click **Save**.

Set 1:1 Face Grade Threshold via PC Web

Set 1:1 face grade threshold.

Go to **Access Control → Parameters Settings → Smart** .

Set **1:1 Face Picture Grade Threshold**, and click **Save**.

The higher the threshold, the higher the requirements for the quality of the captured images of the front camera, and the easier to prompt authentication failure.

Set Face 1:1 Matching Threshold via PC Web

Set face 1:1 matching threshold.

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

Set face 1:1 matching threshold and click **Save**.

The larger the value of the threshold, the fault acceptance rate will be lower and the false rejection rate will be higher when authenticating via face. The maxium value is 100.

Set 1:N Matching Threshold via PC Web

You can set the matching threshold for face 1:N matching.

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

Set the 1:N matching threshold and click **Save**.

The larger the value, the smaller the false accept rate and the larger the false rejection rate. The maximum value is 100.

Set Face Recognition Area via Web Browser

You can set the recognition area of the lens during face recognition and authentication.

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

Drag the yellow box in the preview screen to adjust the effective area for face recognition on the left, right, up, and down sides.

Or drag the block or enter the number to set the effective area.

Click **Save**.

Click , , or to capture, record, or go to full screen view.

Enable/Disable Face with Mask Detection via PC Web

After enabling the face with mask detection, the system will recognize the captured face with mask picture or not.

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

After enabling the face with mask detection, you can set **Face without Mask Strategy**, **Face with Mask&Face (1:1)**, **Face with Mask 1:1 Match Threshold**.

Face without Mask Strategy

You can select **None**, **Reminder of Wearing Face Mask** and **Must Wear Face Mask**.

Reminder of Wearing Face Mask

If the person do not wear the face mask when authenticating, the device will pop up a prompt and the door will open.

Must Wear Face Mask

If the person do not wear the face mask when authenticating, the device will pop up a prompt and the door will keep closed.

Face with Mask&Face (1:1)

Set the matching value when authenticating with face mask via 1:1 matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate. The maximum value is 100.

Face with Mask&Face (1:N)

Set the matching threshold when authenticating with face mask via 1:N matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate. The maximum value is 100.

Click **Save**.

6.9.6 Card Settings

Enable/Disable NFC Protection via PC Web

After enabling, the device can read NFC card.

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

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

Enable/Disable M1 Card via Web Client

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

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

Click to **Enable M1 Card**.

M1 Card Encryption

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

Sector

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

Note

You are advised to encrypt sector 13.

Click **Save**.

Enable/Disable EM Card via Web Client

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

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

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

Note

- If the peripheral card reader which can read EM card is connected, after enabling this function, you can also swipe EM card via this card reader.
- When a Dual-frequency Card Module is connected, you can swipe both the EM card and the DESfire card at the same time. However, swiping the card on the device is invalid.

Set DESFire Card

You can enable DESFire card and DESFire card read content.

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

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

Note

When a Dual-frequency Card Module is connected, you can swipe both the EM card and the DESfire card at the same time. However, swiping the card on the device is invalid.

Set FeliCa Card

You can enable FeliCa card.

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

Select **Enable FeliCa Card**.

Set Card No. Authentication Parameters via Web

Set the card reading content when authenticate via card on the device.

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

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

Full Card No.

All card No. will be read.

3 bytes

The device will read card via read 3 bytes.

4 bytes

The device will read card via 4 bytes.

6.9.7 Linkage Settings

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

Steps

1. Click **Access Control → Parameter Settings → Linkage Settings** to enter the settings page.
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 Capture**.
5. Click**Save** to enable the settings.

6.9.8 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.

6.9.9 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.

Verify Credential Locally

After enabling the function, the device will check permission but not estimate the plan template.

6.9.10 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 Authentication Result via PC Web

Set authentication result contents, such as picture, name, employee ID, and temperature.

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

Check the displayed contents in the authentication result, such as picture, name, employee ID.

Check **Name De-identification** and **ID De-identification** according to actual needs. After de-identification, the name and the ID will display parts of contents.

Set **Authentication Result Display Duration** and the authentication result will display the configured time duration.

Click **Save**.

Configure Picture Uploading and Storage via PC Web

You can set picture uploading and storage parameters.

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

Save Picture When Auth.

Save picture when authenticating automatically.

Upload Picture When Auth.

Upload the pictures when authenticating to the platform automatically.

Picture Mode

When selecting as default, the device will capture the panoramic view. You can set the Max. picture size and picture resolution.

When selecting as matting picture mode, the devicel will only capture face. You can set the Max. picture size.

Save Registered Picture

The registered face picture will be saved to the system if you enable the function.

Save Pictures After Linked Capture

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

Upload Picture After Linked Capture

Upload the pictures captured by linked camera to the platform automatically

Click **Save**.

Clear Device Pictures via PC Web

You can clear all registered, or captured face pictures.

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

Click **Clear** to clear all registered, captured face pictures.

6.9.11 Call Settings

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.** .

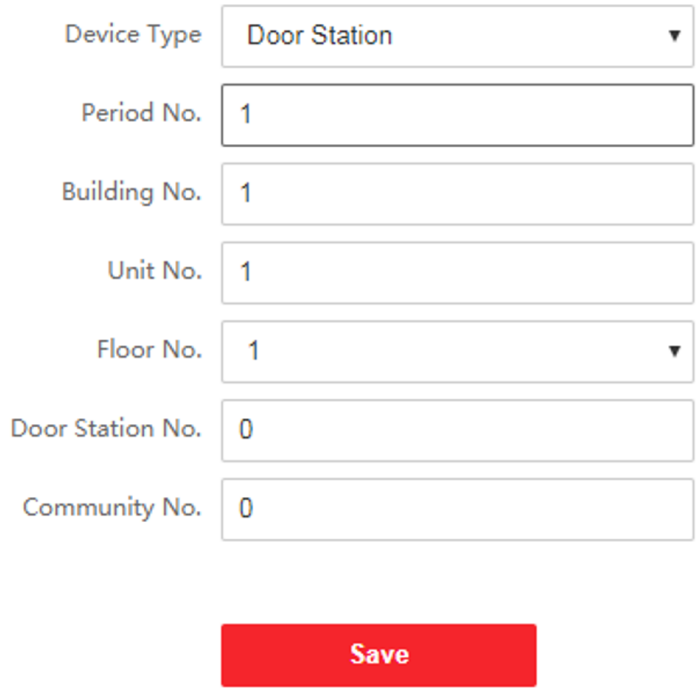


Figure 6-2 Device No. Settings

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.

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.

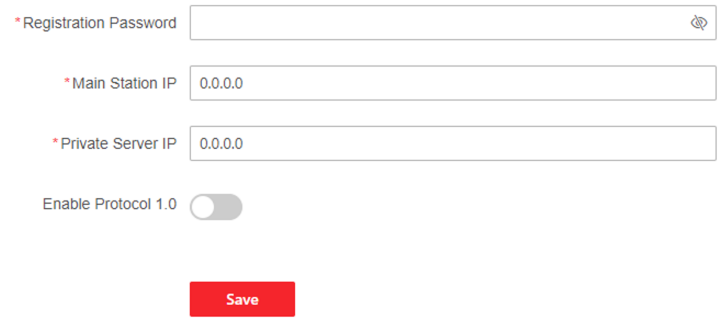


Figure 6-3 Video Intercom Network

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

Click **Save**.

Set Communication Time via PC Web

Set the max. communication time.

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

Enter the **Max. Communication Time**. Click **Save**.

Note

The Max. Communication time range is 90 s to 120 s.

Press Button to Call

Steps

1. Click **Configuration → Intercom → Press Button to Call** to enter the settings page.
2. Check **Call Indoor Station**, **Call Specified Indoor Station**, **Call Management Center** or **APP** at your needs.

   Note

   If you check **Call Specified Indoor Station**, you need to enter the number of the indoor station.
3. Click **Save**.

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**.



Figure 6-4 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. Click**Save**.
5. **Optional:** You can click **Delete** to delete room number and its SIP number.

6.10 System Configuration

6.10.1 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, register number, 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 device name, device No., language, model, serial No., version, number of channels, IO input, IO output, lock, register number, 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.

6.10.2 Set Time

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

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

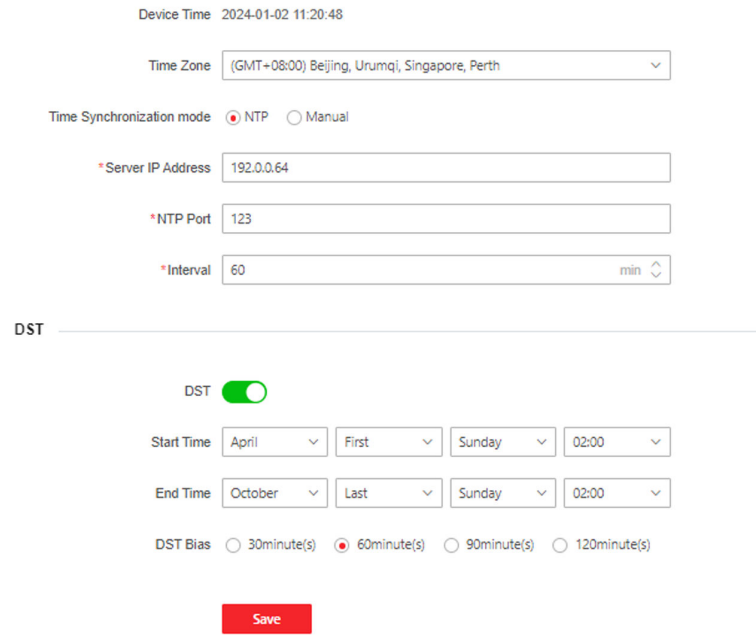


Figure 6-5 Time Settings

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.

6.10.3 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.

6.10.4 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.

6.10.5 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.

6.10.6 Network Settings

Set Basic Network Parameters via PC Web

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

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

NIC Type

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

DHCP

If uncheck the function, you should set the IPv4 address, IPv4 subnet mask, IPv4 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 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** .

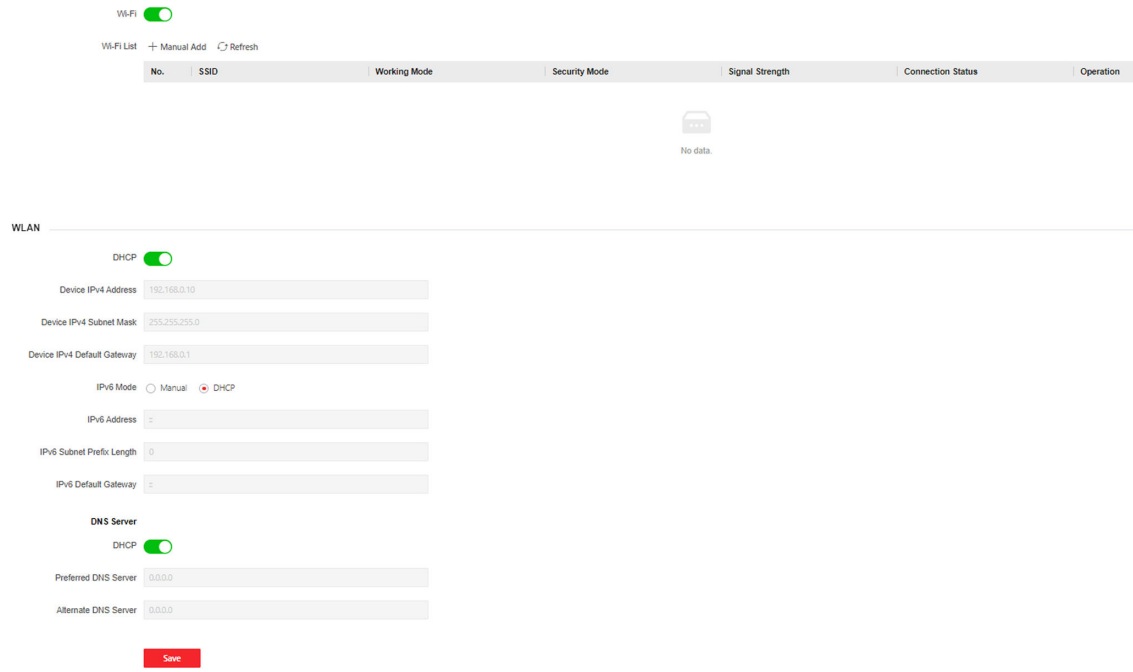


Figure 6-6 Wi-Fi Settings Page

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**.

Set Port via PC Web

Go to **System and Maintenance → System Configuration → Network → Network Service** .

Enable/Disable HTTP

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

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

Click**Save** after parameters are configured.

HTTP Port

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

HTTPS Port

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

HTTP Listening

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

View RTSP Port via PC Web

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

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

View the Port.

Set WebSocket(s) via PC Web

View WebSocket and WebSockets port.

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

View WebSocket and WebSockets port.

Enable SDK Service

After enabling SDK service, the device can be connected to the SDK server.

Click **System and Maintenance → System Configuration → Network → Device Access → SDK Server** to enter the settings page.

Enter **Server Port**.

Click **Save** to enable the settings.

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.

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.**

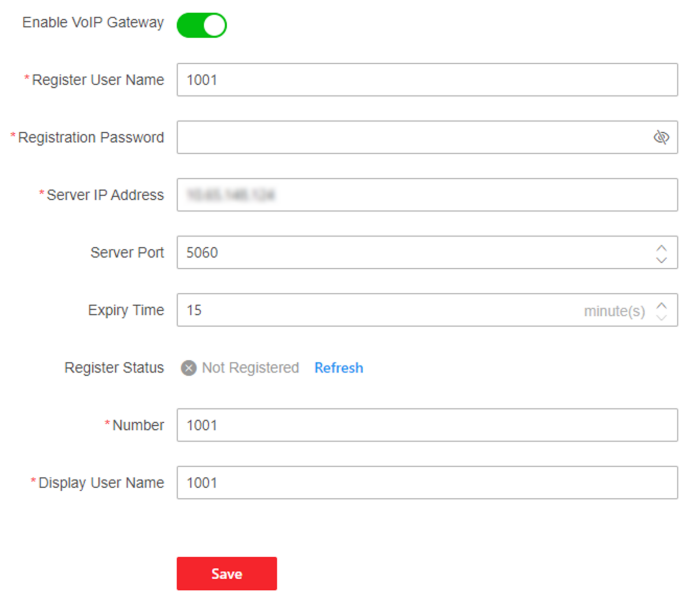


Figure 6-7 VoIP Account Settings

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**.

6.10.7 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**.

Slide to set input and output volume.

Slide to enable **Voice Prompt**.

Tap **Save**.

6.10.8 Image Parameter 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 WDR via PC Web

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

Enable or disable wide dynamic range. After enabling, both bright and dark parts of the scene can be seen more clearly at the same time.

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.

6.10.9 Access Configuration

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.
- Only the device supporting interface board can set the Wiegand parameters.

1. Click **System and Maintenance → System Configuration → Access Configuration → Wiegand Settings** .
2. Check **Wiegand** to enable the Wiegand function.
3. Set a transmission direction.

   Input

   The device can connect a Wiegand card reader.
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.

6.10.10 Time and Attendance Settings

If you want to record the person's working hour, late arrivals, early departures, breaks, absenteeism, etc., you can add the person to the shift group and assign a shift schedule (a rule for the attendance defining how the schedule repeats, the shift type, break settings, and the card swiping rule.) to the shift group to define the attendance parameters for the persons in the shift group.

Disable Attendance Mode via Web

Disable the attendance mode and the system will not display the attendance status on the initial page.

Steps

1. Click **System and Maintenance → System Configuration → Platform Attendance** to enter the settings page.
2. Disable the **Time and Attendance**.

Result

You will not view or configure the attendance status on the initial page. And the system will follow the attendance rule that configured on the platform.

Set Manual Attendance via Web

Set the attendance mode as manual, and you should select a status manually when you take attendance.

Before You Start
Add at least one user, and set the user's authentication mode. For details, see *User Management*.

Steps
1. Click **System and Maintenance → System Configuration → Platform Attendance** to enter the settings page.
2. Set the **Attendance Mode** as **Manual**.
3. Enable the **Attendance Status Required** and set the attendance status lasts duration.
4. Enable a group of attendance status.

   Note

   The Attendance Property will not be changed.
5. **Optional:** Select an status and change its name if required.

Result

You should select an attendance status manually after authentication.

Note

If you do not select a status, the authentication will be failed and it will not be marked as a valid attendance.

Set Auto Attendance via Web

Set the attendance mode as auto, and you can set the attendance status and its available schedule. The system will automatically change the attendance status according to the configured schedule.

Before You Start
Add at least one user, and set the user's authentication mode. For details, see *User Management*.

Steps
1. Click **System and Maintenance → System Configuration → Platform Attendance** to enter the settings page.
2. Set the **Attendance Mode** as **Auto**.
3. Enable the **Attendance Status Required** function.

4. Enable a group of attendance status.

Note

The Attendance Property will not be changed.

5. **Optional:** Select an status and change its name if required.
6. Set the status' schedule. Refers to for details.

Set Manual and Auto Attendance via Web

Set the attendance mode as **Manual and Auto**, and the system will automatically change the attendance status according to the configured schedule. At the same time you can manually change the attendance status after the authentication.

Before You Start

Add at least one user, and set the user's authentication mode. For details, see *User Management*.

Steps

1. Click **System and Maintenance → System Configuration → Platform Attendance** to enter the settings page.
2. Set the **Attendance Mode** as **Manual and Auto**.
3. Enable the **Attendance Status Required** function.
4. Enable a group of attendance status.

Note

The Attendance Property will not be changed.

5. **Optional:** Select an status and change its name if required.
6. Set the status' schedule. Refers to for details.

Result

On the initial page and authenticate. The authentication will be marked as the configured attendance status according to the schedule. If you tap the edit icon on the result tab, you can select a status to take attendance manually, the authentication will be marked as the edited attendance status.

Example

If set the **Break Out** as Monday 11:00, and **Break In** as Monday 12:00, the valid user's authentication from Monday 11:00 to 12:00 will be marked as break.

6.11 Preference Settings

6.11.1 Set Sleep Time via PC Web

The device will in sleep mode after the configured time duration. The function can reduce power consumption.

Go to **System and Maintenance → Preference → Screen Display** .



Figure 6-8 Sleep Settings

Slide **Sleep** and set the sleep time.

Click **Save**.

6.11.2 Customize Authentication Desk via PC Web

Customize the modules on the authentication page/desk.

Steps

1. Go to **System and Maintenance → Preference → Screen Display** .
2. Select **Application Mode**.

   Authentication Mode

   The device authentication page will display the live view page. And the person's name, employee ID, face pictures will all be displayed after authentication.

   Simple Mode

   After selecting this mode, the live view of the authentication page will be disabled. The person's name, employee ID, face pictures will all be hidden after authentication.
3. Click **Apply**.

6.11.3 Set Notice Publication via PC Web

You can set the notice publication for the device.

Go to **System and Maintenance → Preference → Notice Publication** .

Theme Management

Click **Media Library Management → +** to upload the picture from the local PC.

Note

Only the format of JPG and JPEG is supported. Each picture should be smaller than 1 MB with resolution up to 1920*1280.

Add Program

You can set the program name and select program type.

Picture

If you select picture, you can click **+** to add picture.

6.11.4 Customize Prompt Voice via PC Web

You can customize prompt voices for the device.

Steps

1. Go to **System and Maintenance → Preference → Custom Prompt** .



Figure 6-9 Custom Prompt

2. Click → and import audio file from local PC according to your actual needs.

Note

The uploaded audio file should be less than 512 kb, in WAV format.

6.11.5 Set Authentication Result Text via PC Web

Steps

1. Go to **System and Maintenance → Preference → Authentication Result Text** .

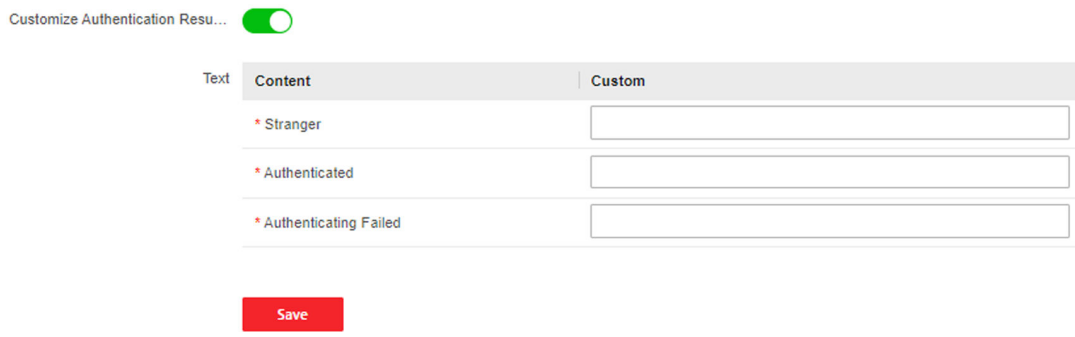


Figure 6-10 Authentication Result Text

2. Enable **Customize Authentication Result Text**.
3. Enter custom texts.
4. Click **Save**.

6.12 System and Maintenance

6.12.1 Reboot

You can reboot the device.

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

Click **Restart** to reboot the device.

6.12.2 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.

6.12.3 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.

6.12.4 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.

6.12.5 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**.

6.12.6 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.

Print Device Log via PC Web

You can print out the device log.

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

Click**Export** to print out the device log.

Capture Network Packet via PC Web

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

Go to **System and Maintenance → Maintenance → Device Debugging → Log for Debugging** .

Set **Capture Packet Duration**,**Capture Packet Size**, and click **Start Capture**.

Test Protocol via PC Web

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

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

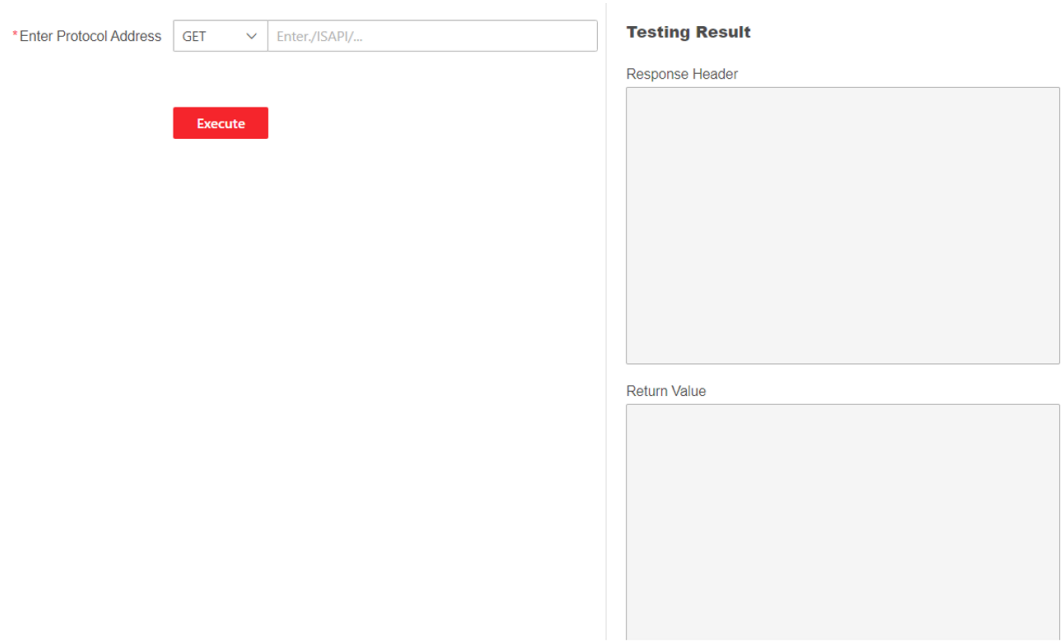


Figure 6-11 Protocol Testing

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

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

Network Diagnosis via PC Web

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

Go to **System and Maintenance → Maintenance → Device Debugging → Network Diagnosis** .

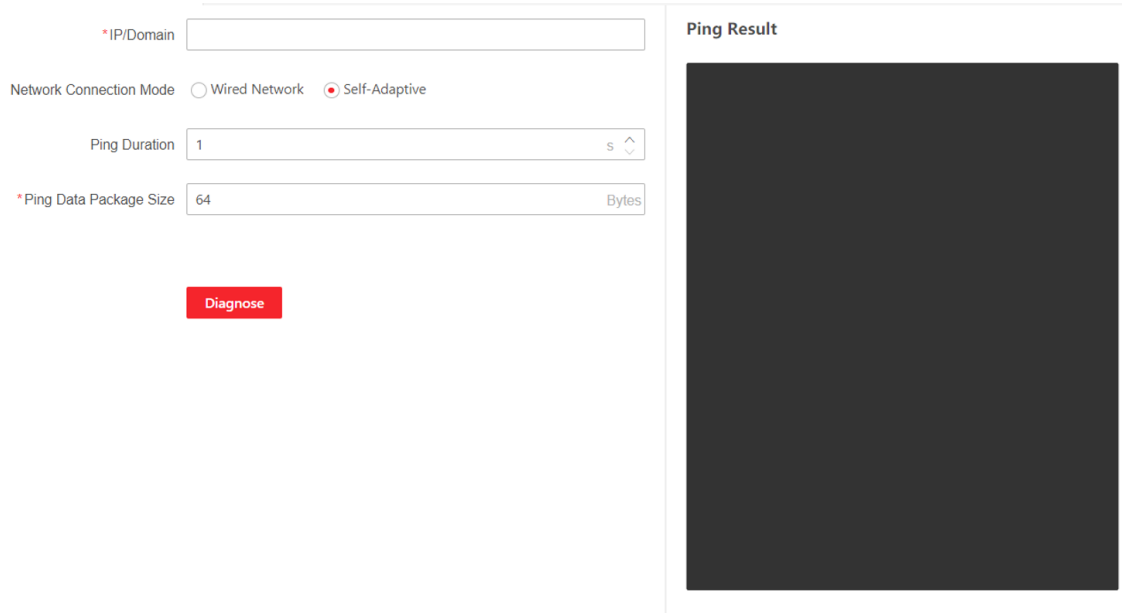


Figure 6-12 Network Diagnosis

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

Set Network Penetration Service via PC Web

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

Steps

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

Note

The penetration service will auto disabled after 48 h.

6.12.7 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.

6.12.8 Advanced Settings via PC Web

You can configure face parameters, palm parameters, and view version information.

Go to **System and Maintenance → Maintenance → Advanced Settings** .

Enter the device activation password and click **Enter**.

Face Parameter

Enable **Custom Anti-Spoofing Detection** and you can set the **Anti-Spoofing Detection Threshold 1:1**, **Anti-Spoofing Detection Threshold 1:N**.

Enable **Lock Face for Authentication**, and set **Lock Duration**. The face will be locked for the set lock duration after the failed attempt limit of anti-spoofing detection has been reached.

Click **Save**.

Version Information

You can view the different version information here.

6.12.9 Security Management

Set security level when login the PC web.

Go to **System and Maintenance → Safe → Security Service** .

Security Mode

High security level when logging in and verify user information.

Compatible Mode

Compatible with old user verification method.

Click **Save**.

6.12.10 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 a CSR (Certificate Signing Request) file in the local computer.
7. Send the CSR (Certificate Signing Request) 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 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. 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.

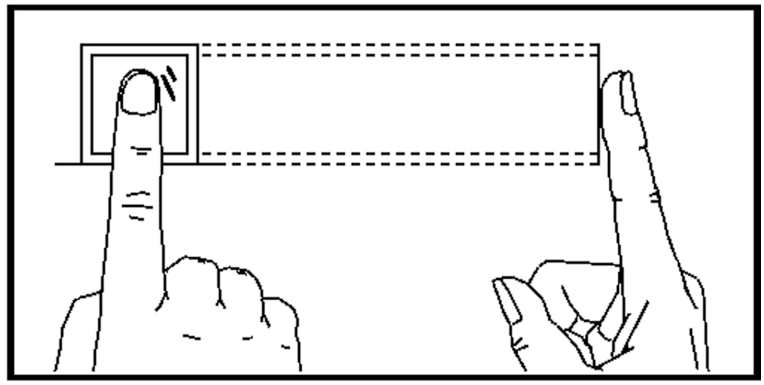
Appendix B. Tips for Scanning Fingerprint

Recommended Finger

Forefinger, middle finger or the third finger.

Correct Scanning

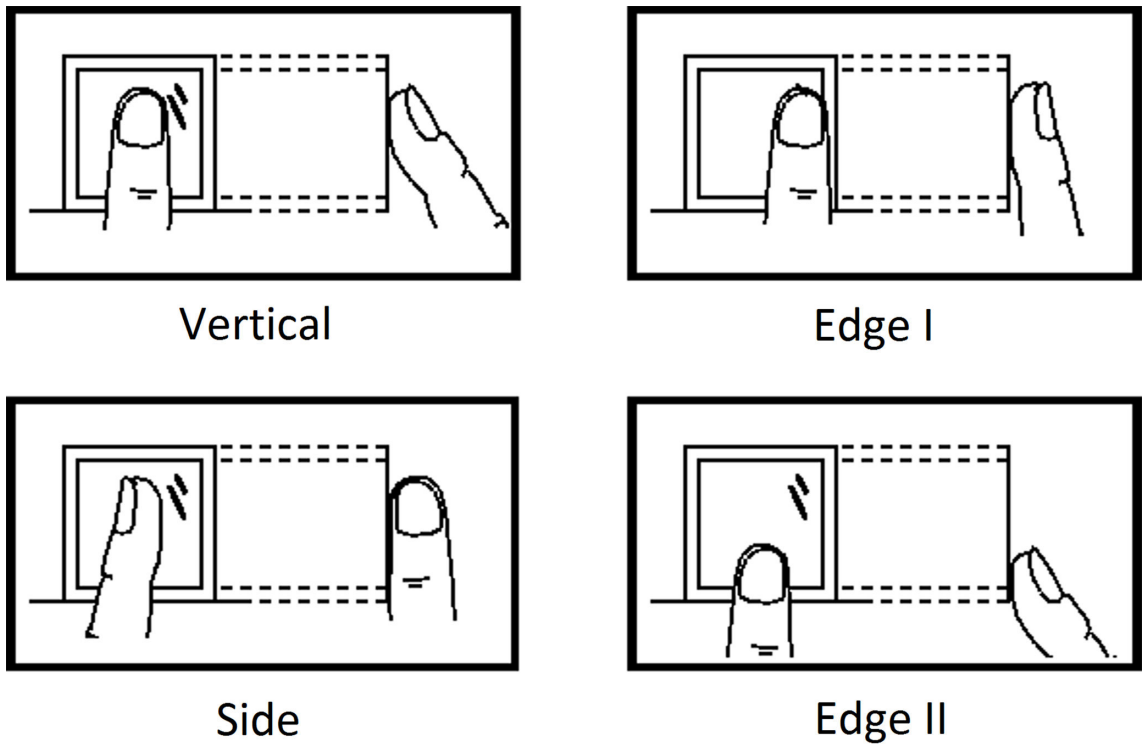
The figure displayed below is the correct way to scan your finger:



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:



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.

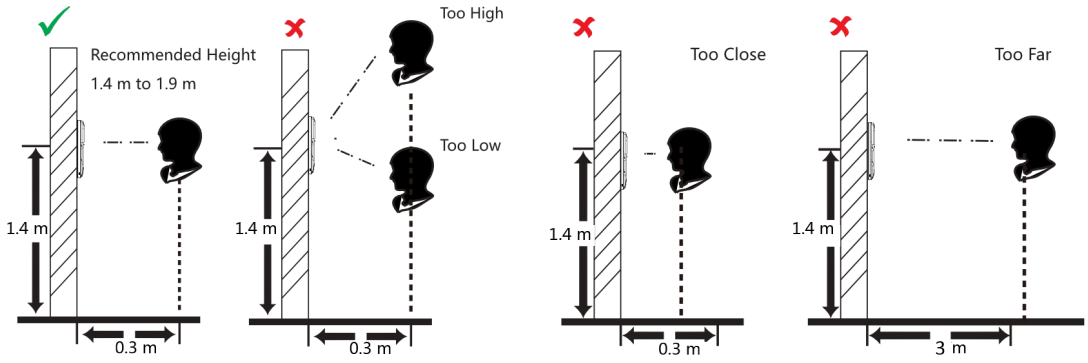
Others

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.

Appendix C. Tips When Collecting/Comparing Face Picture

The position when collecting or comparing face picture is as below:

Positions (Recommended Distance: 0.3 m)



Expression

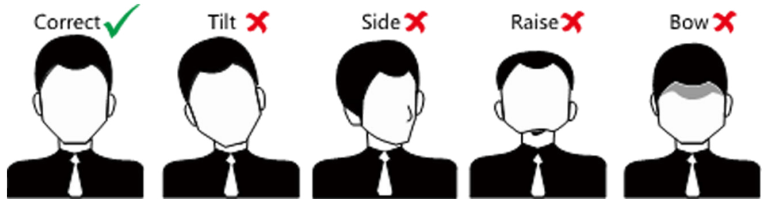
- Keep your expression naturally when collecting or comparing face pictures, just like the expression in the picture below.



- Do not wear hat, sunglasses, or other accessories that can affect the facial recognition function.
- Do not make your hair cover your eyes, ears, etc. and heavy makeup is not allowed.

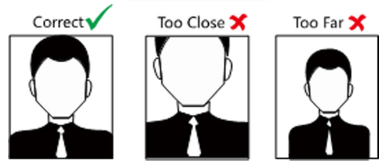
Posture

In order to get a good quality and accurate face picture, position your face looking at the camera when collecting or comparing face pictures.



Size

Make sure your face is in the middle of the collecting window.



Appendix D. Tips for Installation Environment

1. Light Source Illumination Reference Value



Candle: 10Lux

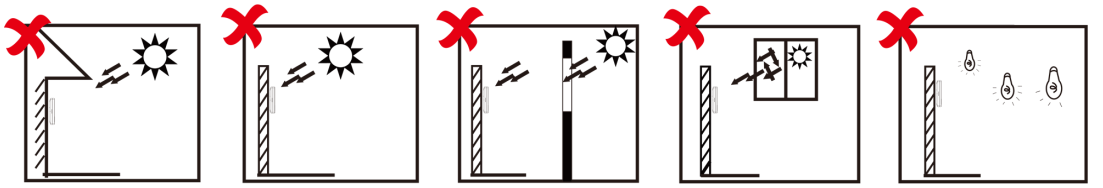


Bulb: 100~850Lux



Sunlight: More than 1200Lux

2. Avoid backlight, direct and indirect sunlight




See Far, Go Further