DS-K1T674 Series Face Recognition Terminal

User Manual

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.

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:

- In the use of the product, you must be in strict compliance with the electrical safety regulations of the nation and region.
- CAUTION: To reduce the risk of fire, replace only with the same type and rating of fuse.
- CAUTION: This equipment is for use only with Hikvision's bracket. Use with other (carts, stands, or carriers) may result in instability causing injury.
- To prevent possible hearing damage, do not listen at high volume levels for long periods.
- Please use the power adapter, which is provided by normal company. The power consumption cannot be less than the required value.
- Do not connect several devices to one power adapter as adapter overload may cause over-heat or fire hazard.
- Please make sure that the power has been disconnected before you wire, install or dismantle the device.
- When the product is installed on wall or ceiling, the device shall be firmly fixed.
- If smoke, odors or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service center.
- 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:

- + identifies the positive terminal(s) of equipment which is used with, or generates direct current. + identifies the negative terminal(s) of equipment which is used with, or generates direct current.
- No naked flame sources, such as lighted candles, should be placed on the equipment.
- The USB port of the equipment is used for connecting to a USB flash drive only.
- The serial port of the equipment is used for debugging only.

- Burned fingers when handling the fingerprint sensor metal. Wait one-half hour after switching off before handling the parts.
- Install the equipment according to the instructions in this manual. To prevent injury, this equipment must be securely attached to the floor/wall in accordance with the installation instructions.
- 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.
- 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.
- Please make sure that the biometric recognition accuracy will be affected by the collected pictures' quality and the light in the environment, which cannot be completely correct.

Contents

Chapter 1 Quick Operation 1

Chapter 2 Activation 2

2.1 Activate via Device 2

2.2 Activate via Web Browser 4

2.3 Activate Device via HiTools Delivery 4

2.4 Activate Device via iVMS-4200 Client Software 6

Chapter 3 Quick Operation 8

3.1 Select Language 8

3.2 Set Password Change Type 8

3.3 Set Network Parameters 10

3.4 Access to Platform 12

3.5 Set Administrator 14

3.6 Status Description and Control Center 16

Chapter 4 Basic Operation 17

4.1 Login 17

4.1.1 Login by Administrator 17

4.1.2 Login by Activation Password 20

4.1.3 Forgot Password 21

4.2 Communication Settings 23

4.2.1 Set Wired Network Parameters 23

4.2.2 Set Wi-Fi Parameters 25

4.2.3 Set RS-485 Parameters 27

4.2.4 Set Wiegand Parameters 29

4.2.5 Set ISUP Parameters 29

4.2.6 Platform Access 31

4.2.7 Enable Mobile Network 32

4.3 Person Management 32
4.3.1 Add Administrator 32
4.3.2 Add Face Picture 34
4.3.3 Add Fingerprint 36
4.3.4 Add Card 37
4.3.5 View PIN code 38
4.3.6 Set Authentication Mode 38
4.3.7 Edit Person 39
4.4 Data Management 39
4.4.1 Delete Data 39
4.4.2 Import Data 39
4.4.3 Export Data 40
4.5 Identity Authentication 41
4.5.1 Authenticate via Single Credential 41
4.5.2 Authenticate via Multiple Credential 42
4.6 System Settings 42
4.7 Password Management 44
4.8 Set Smart Parameters 44
4.8.1 Set Multiple Faces Recognition and Face Duplicate Check 44
4.8.2 Set Face Liveness Level 45
4.8.3 Set Face Recognition Distance 45
4.8.4 Set Face Recognition Interval 45
4.8.5 Set Face 1:1/1:N Security Level 45
4.8.6 Set ECO Mode 46
4.8.7 Enable NFC Card 46
4.8.8 Enable M1 Card and M1 Car d Encryption 46
4.8.9 Set Face with Mask Detection 47
4.9 Set Access Control Parameters 47

4.9.1 Set Terminal Authentication Mode 47
4.9.2 Set Card Reader Authentication Mode 48
4.9.3 Set Door Contact Parameters 48
4.9.4 Set Duration of Open Linked Gate 48
4.9.5 Enable Face Authentication Manually 48
4.9.6 Set Password Mode 49
4.10 Time and Attendance Status Settings 49
4.10.1 Disable Attendance Mode via Device 49
4.10.2 Set Manual Attendance via Device 50
4.10.3 Set Auto Attendance via Device 52
4.10.4 Set Manual and Auto Attendance via Device 54
4.11 Preference Settings 56
4.11.1 Set Theme Color 56
4.11.2 Set Theme Mode 56
4.11.3 Set Screen Content 57
4.11.4 Set Control Center Displayed Items 57
4.12 System Maintenance 57
4.12.1 View System Information 57
4.12.2 View Device Capacity 58
4.12.3 Upgrade 58
4.12.4 View User Manual 58
4.12.5 Restore Parameters 58
4.12.6 Reboot 59
4.13 Set Privacy Parameters 59
4.14 Video Intercom 60
4.14.1 Call Settings 60
4.14.2 Call Client Software from Device 61
4.14.3 Call Center from Device 61

4.14.4 Call Device from Client Software 62
4.14.5 Call Room from Device 62
4.14.6 Call Mobile Client from Device 63
4.14.7 Doorbell Call 63
Chapter 5 Quick Operation via Web Browser 64
5.1 Change Password 64
5.2 Select Language 64
5.3 Time Settings 64
5.4 Privacy Settings 65
5.5 Administrator Settings 65
5.6 No. and System Network 66
Chapter 6 Operation via Web Browser 68
6.1 Login 68
6.2 Forget Password 68
6.3 Help 68
6.3.1 Open Source Software Licenses 68
6.3.2 View Online Help Document 69
6.4 Logout 69
6.5 Quick Operation via Web Browser 69
6.5.1 Change Password 69
6.5.2 Select Language 69
6.5.3 Time Settings 69
6.5.4 Privacy Settings 70
6.5.5 Administrator Settings 70
6.5.6 No. and System Network 71
6.6 Person Management 72
6.7 Overview 74
6.8 Access Control Management 76

6.8.1 Search Event 76
6.8.2 Door Parameter Configuration 76
6.8.3 Authentication Settings 79
6.8.4 Authentication Linkage Settings 82
6.8.5 Set Authentication Plan 83
6.8.6 Set Face Parameters 83
6.8.7 Card Settings 87
6.8.8 Set Remote Verification 89
6.8.9 Privacy Settings 90
6.8.10 Call Settings 92
6.9 Device Management 97
6.10 System Configuration 97
6.10.1 View Device Information via PC Web 97
6.10.2 Set Time 97
6.10.3 Change Administrator's Password 98
6.10.4 Account Security Settings via PC Web 99
6.10.5 View Device Arming/Disarming Information via PC Web 99
6.10.6 Set Working Mode via PC Web 99
6.10.7 Network Settings 100
6.10.8 Set Video and Audio Parameters via PC Web 105
6.10.9 Image Parameter Settings 106
6.10.10 Alarm Settings via PC Web 108
6.10.11 Linkage Settings 108
6.10.12 Access Configuration 109
6.11 Time and Attendance Settings 112
6.11.1 Disable Attendance Mode via Web 112
6.11.2 Set Manual Attendance via Web 113
6.11.3 Set Auto Attendance via Web 113

6.11.4 Set Manual and Auto Attendance via Web 114
6.12 Preference Settings 115
6.12.1 Set Startup Image via PC Web 115
6.12.2 Set Standby Image via PC Web 115
6.12.3 Set Sleep Time via PC Web 115
6.12.4 Customize Authentication Desk via PC Web 116
6.12.5 Set Notice Publication via PC Web 116
6.12.6 Set Prompt Schedule via PC Web 118
6.12.7 Customize Prompt Voice via PC Web 119
6.12.8 Set Authentication Result Text via PC Web 119
6.12.9 Doorplate Settings 120
6.13 System and Maintenance 120
6.13.1 Reboot 120
6.13.2 Upgrade 120
6.13.3 Restoration 121
6.13.4 Export Device Parameters via PC Web 122
6.13.5 Import Device Parameters via PC Web 122
6.13.6 Device Debugging 122
6.13.7 View Log via PC Web 125
6.13.8 Advanced Settings via PC Web 125
6.13.9 Security Management 125
6.13.10 Certificate Management 125
Chapter 7 Other Platforms to Configure 128
Appendix A. Tips for Scanning Fingerprint 129
Appendix B. Tips When Collecting/Comparing Face Picture 131
Appendix C. Tips for Installation Environment 133
Appendix D. Legal Information 134

Chapter 1 Quick Operation

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



Figure 1-1 Quick Start Guide QR Code

Chapter 2 Activation

For the first-time access, you need to activate the device by setting an admin password. No operation is allowed before activation. The device supports multiple activation methods, such as activation via local device, web browser, HiTools Delivery, and iVMS-4200 Client.

After powering on the device, the system will switch to Device Activation page.

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

2.1 Activate via Device

If the device is not activated, you can activate the device after it is powered on.

On the Activate Device page, create a password and confirm the password. Tap **Activate** and the device will activated.

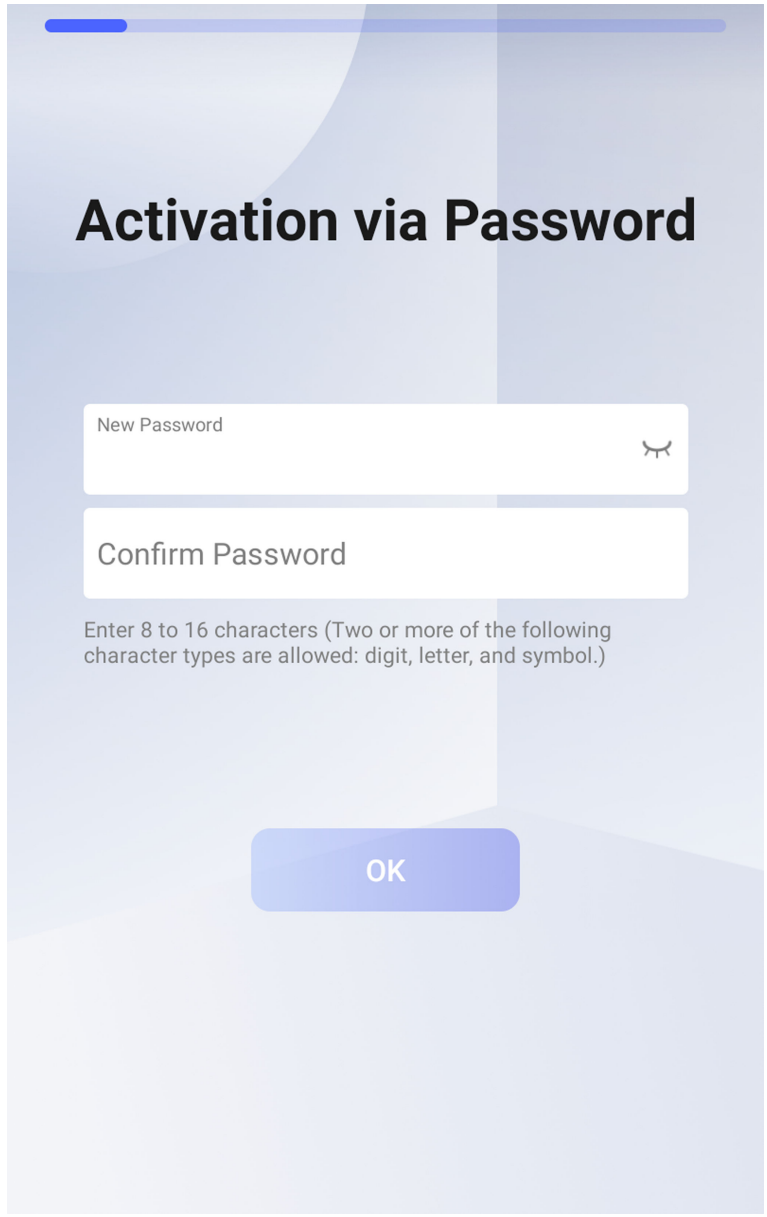


Figure 2-1 Activation Page

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.

After activation, you should select language, set password change type, set application mode, set network, set platform parameters, set privacy parameters, and set administrator.

2.2 Activate via Web Browser

You can activate the device via the web browser.

Steps

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

   Note

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

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

   Caution

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

   Note

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

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

2.3 Activate Device via HiTools Delivery

HiTools Delivery aims to streamline and enhance the activation, networking, and batch configuration for various devices. You can use the software to detect, activate, and modify the IP addresses of multiple devices over the LAN.

Before You Start

- Set the device and the computer that runs the software to the same network segment.
- Access the official website (***https://www.hikvision.com/en***) and enter **Support → Download → Software → HiTools → HiTools Delivery** to download HiTools Delivery and install it according to the prompts.

Steps

1. Run the software.
2. Click **Home Page → Search → Current Subnet** . Click **Refresh**, and the list will display all the online devices in the same network segment.
3. Select the inactive device(s) in the list. Set a new password according to the popup requirements and confirm the password.
4. Click **Activation**. The device activation status will change to **Activated** after successful activation.

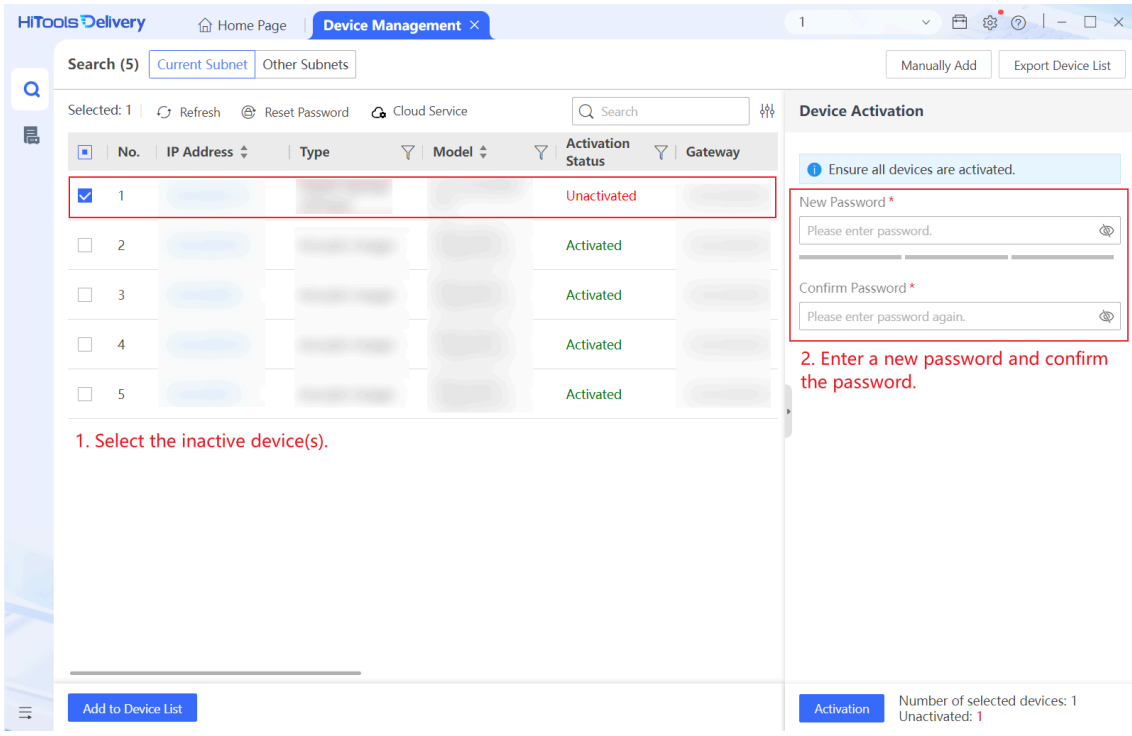


Figure 2-2 Activation

5. **Optional:** Change the IP address of the device.
   1) On **Current Subnet** interface, select multiple devices that need to change the IP addresses.
   2) On the right **Network Parameter** window, set the start IP address, port No., IPv4 subnet mask, IPv4 gateway, etc., and the selected devices will be automatically assigned to increasing IP addresses. Or check **Enable DHCP** to assign dynamic IP addresses.
   3) Enter the admin password and click **OK**.

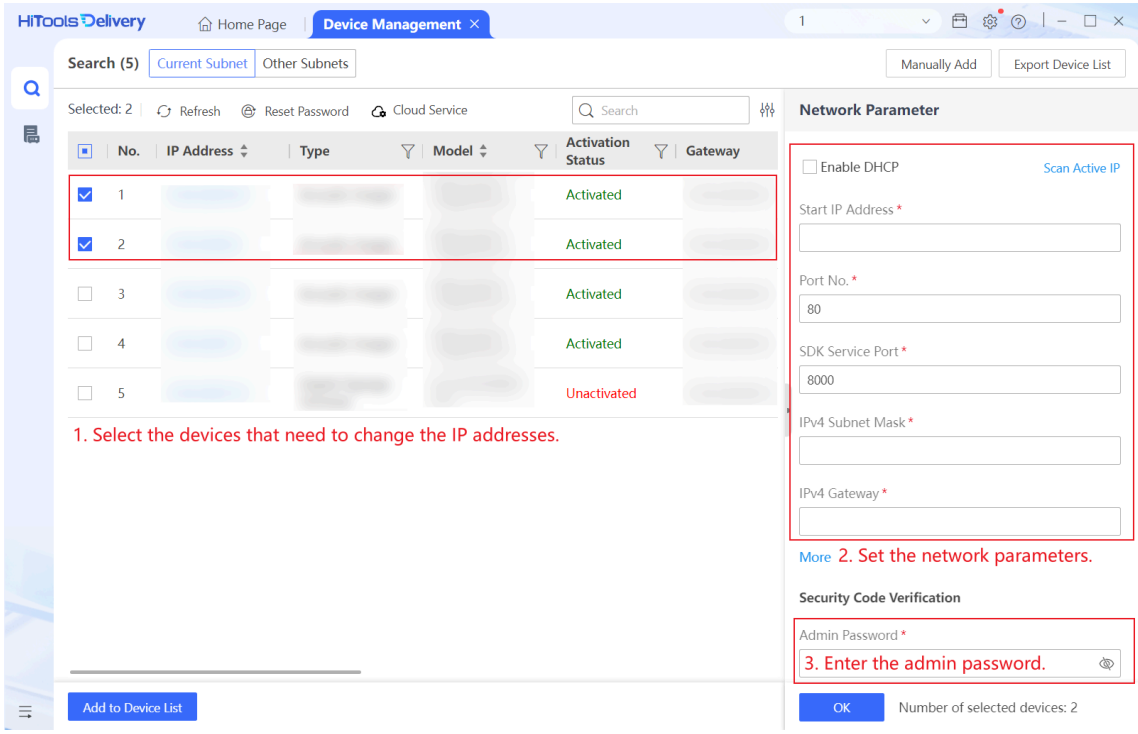


Figure 2-3 Modify Network Parameters

Note

- Set the device IP address to the same network segment with that of your computer.
- You can click **Scan Active IP** to detect and view the available IP addresses. Refer to the help of HiTools Delivery for details.
- You can also click **Home Page → Maintenance → Change IP** to change the IP addresses in batch by exporting and importing the template. Refer to the help of HiTools Delivery for details.

2.4 Activate Device via iVMS-4200 Client Software

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

Steps

Note

This function should be supported by the device.

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

The searched online devices are displayed in the list.

4. Check the device status (shown on **Security Level** column) and select an inactive device.
5. Click **Activate** to open the Activation dialog.
6. Create a password in the password field, and confirm the password.

Caution

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

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

Note

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

7. Click **OK** to activate the device.

Chapter 3 Quick Operation

3.1 Select Language

After activation, you should select a language.

Steps

1. Select a language according to the actual needs.
2. Click **Next**.

3.2 Set Password Change Type

After activating the device, you can set the password change type as reserved email address or security questions. Once you forgot the device password, you can change the password via the selected change type.

Change Password via Email Address

If you need to change password via reserved email, you can enter an email address, and tap **Next**.

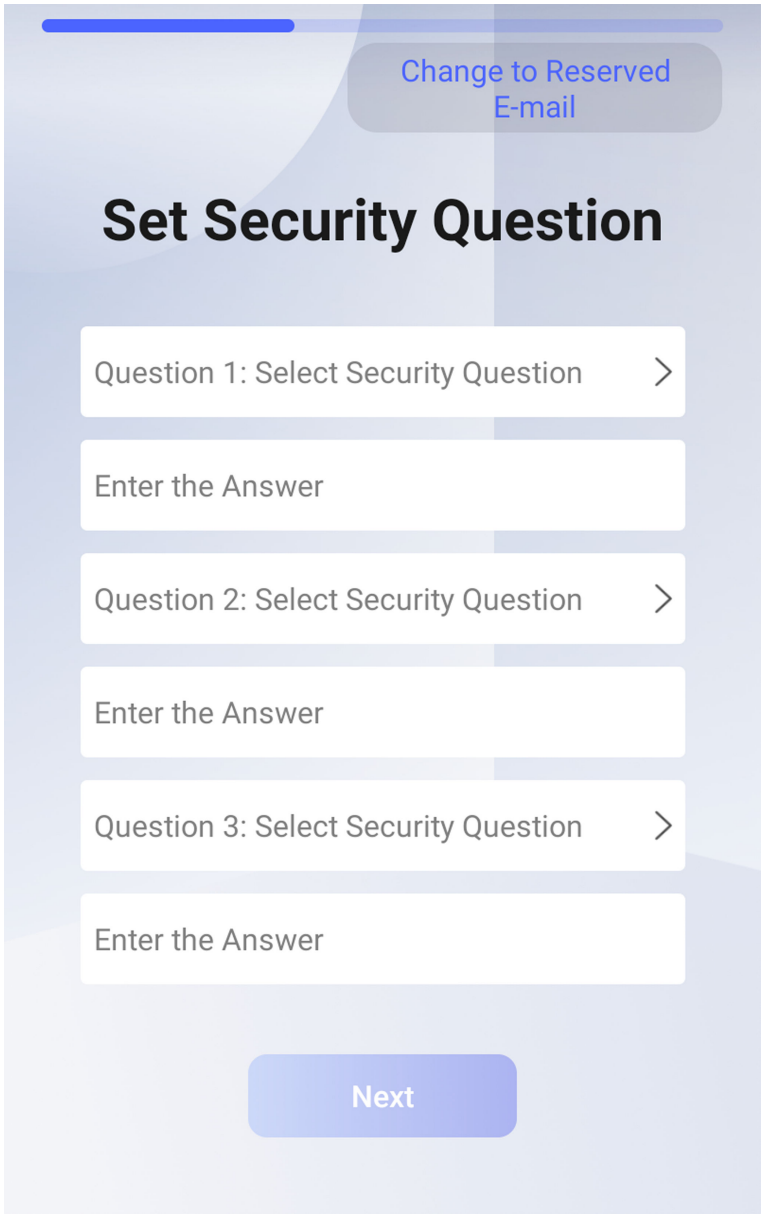


Figure 3-1 Password Change Page

Change via Security Questions

If you need to change password via security questions, you can tap **Change to Security Questions** on the right corner. Select the security questions and enter the answers. Click **Next**.

Note

You can only select one type to change password. If you need, you can enter the web page to set both of the changing types.

3.3 Set Network Parameters

You can set the network for the device.

Steps

Note

Parts of the device models supports wi-fi function. Refers to the actual device for details.

1. When you enter the Select Network page, tap **Wired Network** or **Wi-Fi** for your actual needs.

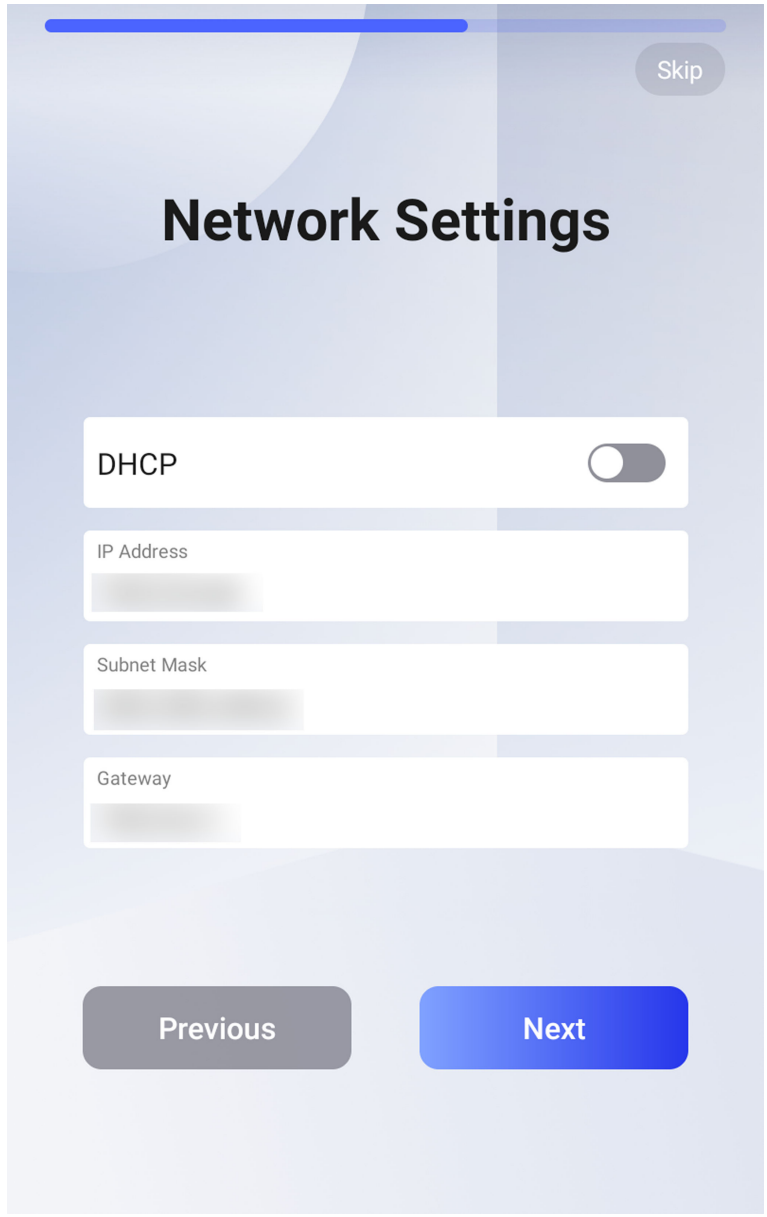


Figure 3-2 Select Network

Note

Disconnect the wired network before connecting a Wi-Fi.

2. Tap **Next**.

Wired Network

Note

Make sure the device has connected to a network.

If enable **DHCP**, the system will assign the IP address and other parameters automatically.

If disable **DHCP**, you should set the IP address, the subnet mask, and the gateway.

Note

IP address of 192.168.1.64, and 192.168.1.7 are not suggested to use.

Wi-Fi

Select a Wi-Fi and enter the Wi-Fi's password to get connected.

Or tap **Add Wi-Fi** and enter the Wi-Fi's name and the password to get connected.

3. **Optional:** Tap **Skip** to skip network settings.

3.4 Access to Platform

Enable the function and the device can communicate via Hik-Connect. You can add the device to Hik-Connect mobile client and so on.

Steps

Note

Parts of the device models supports function. Refers to the actual device for details.

1. Enable **Access to Hik-Connect**, and set the server IP and verification code.

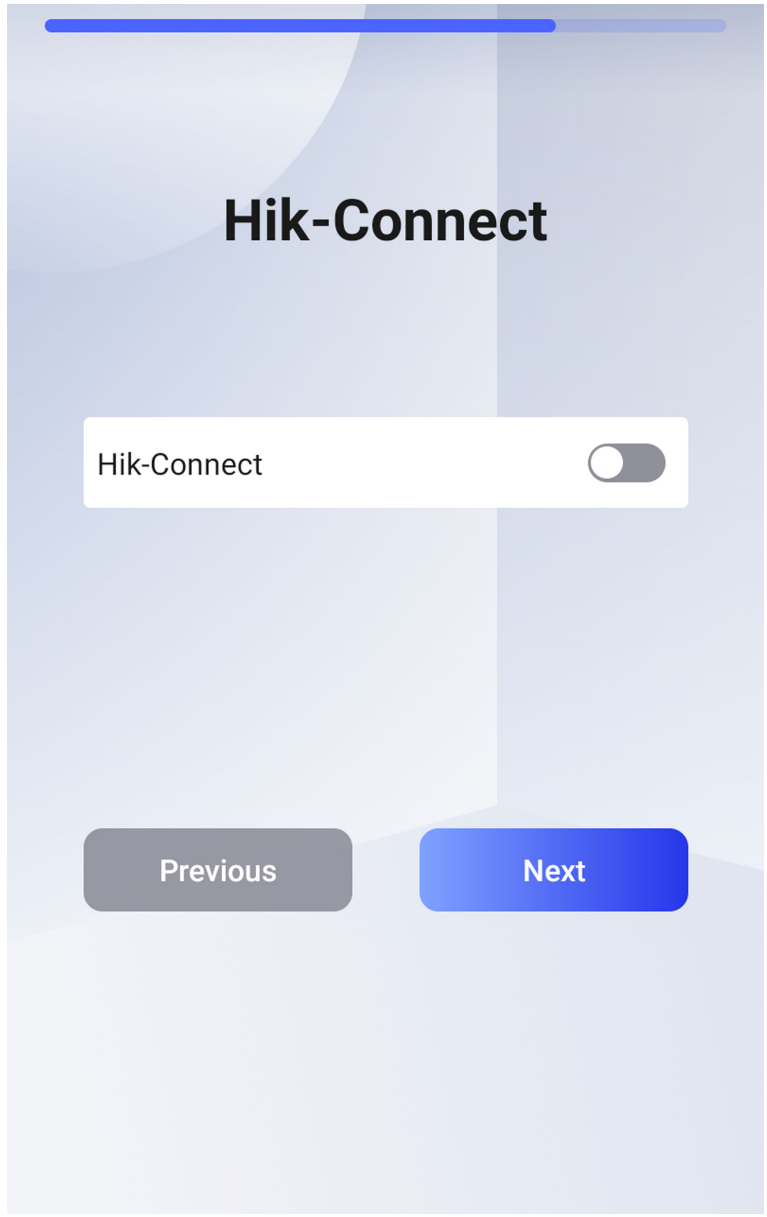


Figure 3-3 Access to Hik-Connect

2. Tap **Next**.
3. **Optional:** Tap **Skip** to skip the step.
4. **Optional:** Tap **Previous** to go to the previous page.

Note

If you tap **Previous** to return to the Wi-Fi configuration page, you need to tap the connected Wi-Fi or connect another Wi-Fi to enter the platform page again.

3.5 Set Administrator

After device activation, you can add an administrator to manage the device parameters.

Before You Start
Activate the device and select an application mode.

Steps
1. **Optional:** Tap **Skip** to skip adding administrator if required.
2. Enter the administrator's name (optional) and tap **Next**.

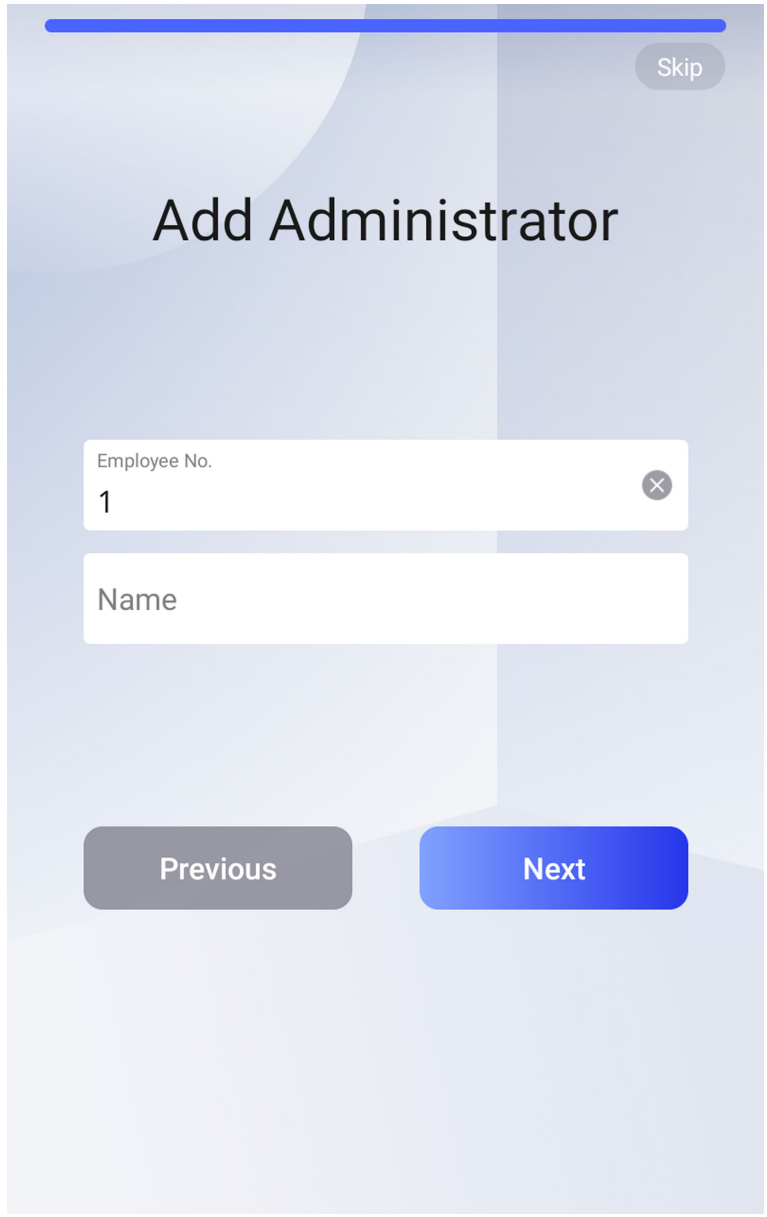


Figure 3-4 Add Administrator Page

3. Select a credential to add.

Note

Up to one credential should be added.

- : Face forward at the camera. Make sure the face is in the face recognition area. Click to capture and click to confirm.
- : Press your finger according to the instructions on the device screen. Click to confirm.
- : Enter the card No. or present card on the card presenting area. Click **OK**.

4. Click **OK**.

You will enter the authentication page.

3.6 Status Description and Control Center

On the authentication page, you can view the device status at the upper right corner of the device interface. You can also use finger to pull down the authentication page to enter the control center.

Control Center

Use finger to pull down the authentication page to enter the control center.

Status Icon Description

/

Device is armed/not armed.

/

Hik-Connect is enabled/disabled.

/ /

The device wired network is connected/not connected/connecting failed.

/ /

The device' Wi-Fi is enabled and connected/not connected/enabled but not connected.

3G/4G is enabled.

Shortcut Keys Description

Note

You can configure those shortcut keys displayed on the screen. For details, see ***System Settings*** .

Scan QR code to authenticate.

Note

The QR code can be obtained from the visitor terminal.

- Enter the device room No. and tap **OK** to call.
- Tap to call the center.

Note

The device should be added to the center, or the calling operation will be failed.

Enter password to authenticate.

Chapter 4 Basic Operation

4.1 Login

Login the device to set the device basic parameters.

4.1.1 Login by Administrator

If you have added an administrator for the device, only the administrator can login the device for device operation.

Steps

1. Long tap on the initial page and slide to the left/right by following the gesture to enter the admin login page.

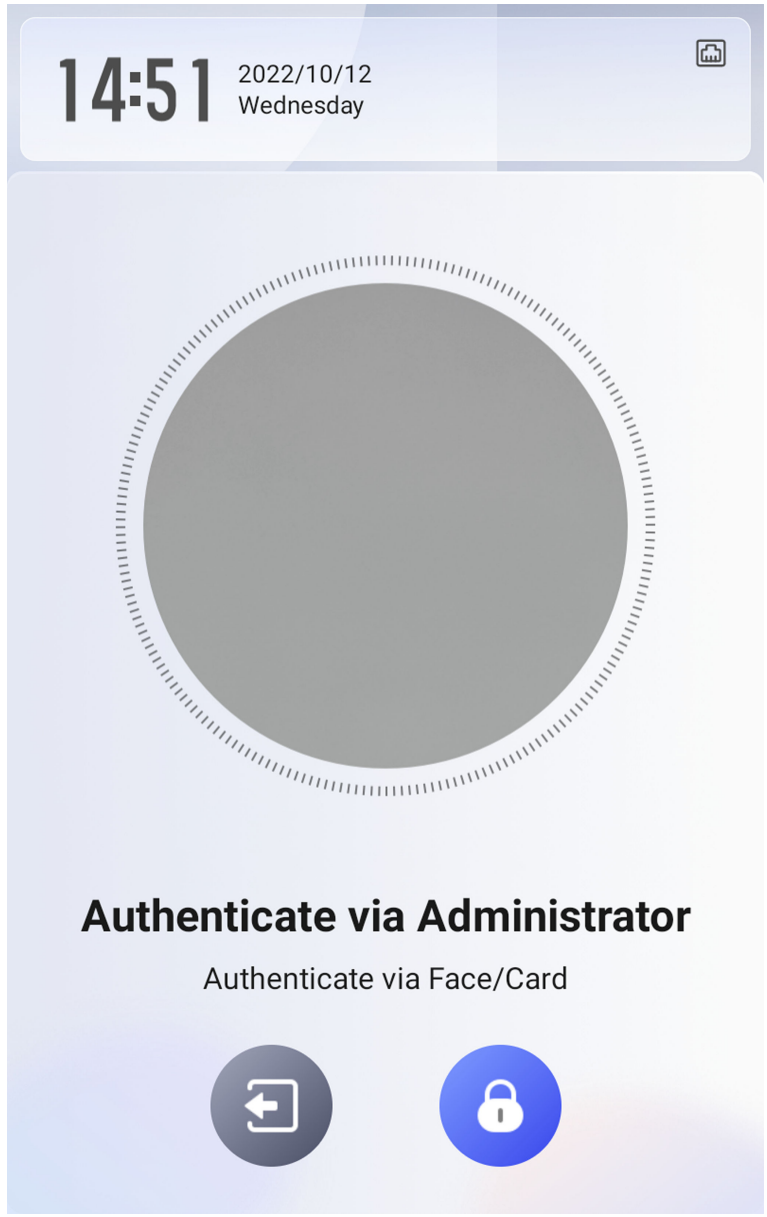


Figure 4-1 Admin Login

2. Authenticate the administrator's face or card to enter the home page.

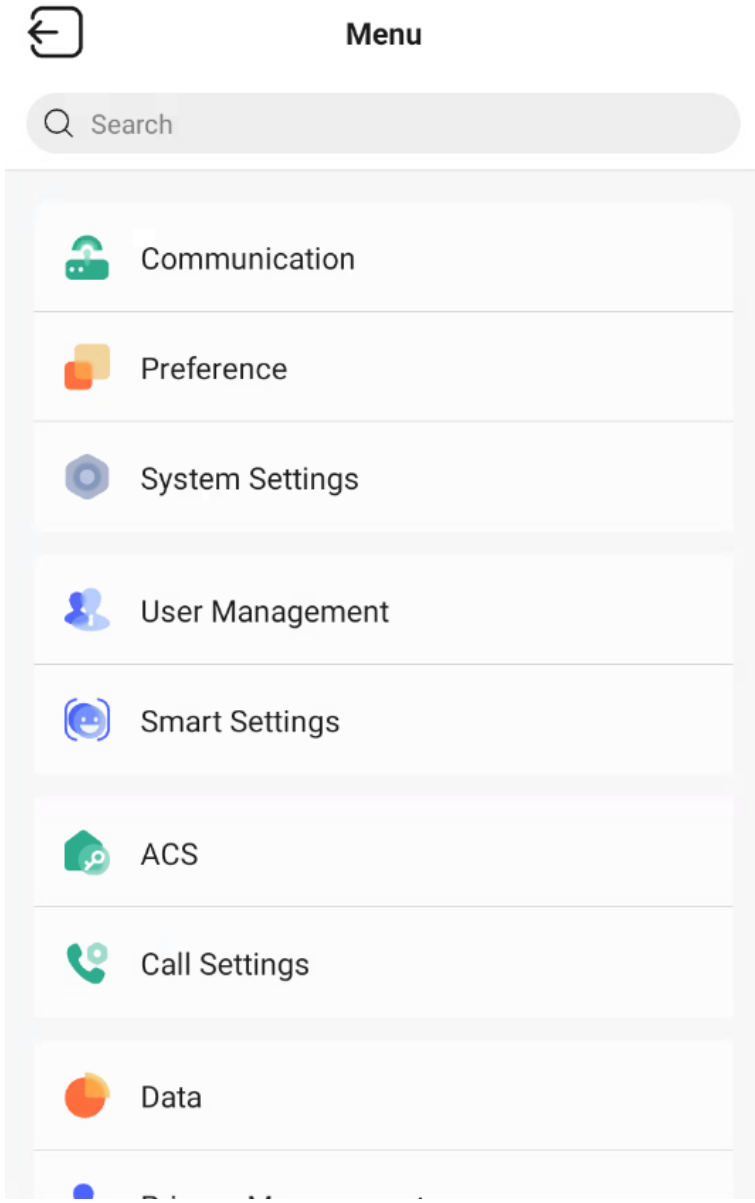


Figure 4-2 Home Page

Note

- The device will be locked for 30 minutes after 5 failed fingerprint or card attempts.
- After login to the main page, you can search function in the searching bar which locates on the top of the main page.

3. **Optional:** Tap and you can enter the device activation password for login.
4. **Optional:** Tap and you can exit the admin login page.

4.1.2 Login by Activation Password

You should login the system before other device operations. If you do not configure an administrator, you should follow the instructions below to login.

Steps

1. Long tap on the initial page for 3 s and slide to the left/right by following the gesture to enter password entering page.
2. Enter the password.
   - If you have added an administrator for the device, tap  and enter the password.
   - If you haven't added an administrator for the device, enter the password.
3. Tap **OK** to enter the home page.

Note

The device will be locked for 30 minutes after 5 failed password attempts.

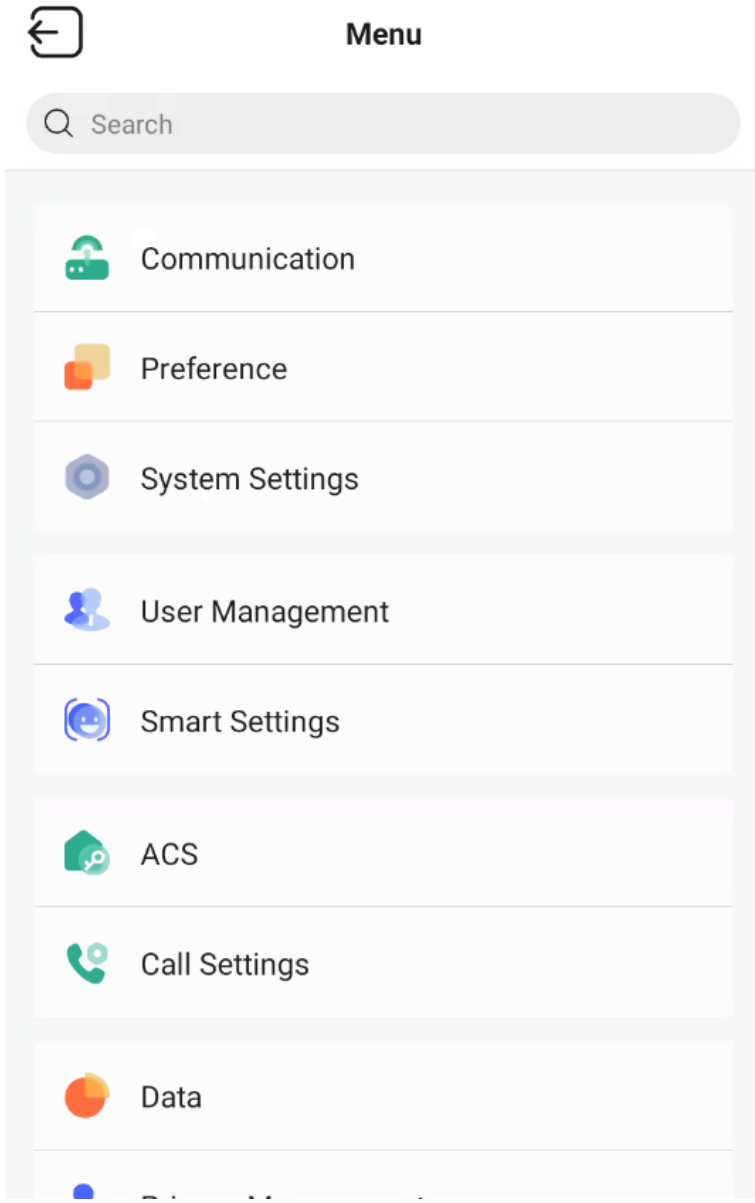


Figure 4-3 Home Page

4.1.3 Forgot Password

If you forget the password during authentication, you can change the password.

Steps

1. Hold the initial page for 3 s and slide to the left/right by following the gesture and log in the page.
2. **Optional:** If you have set an administrator, tap in the pop-up admin authentication page.

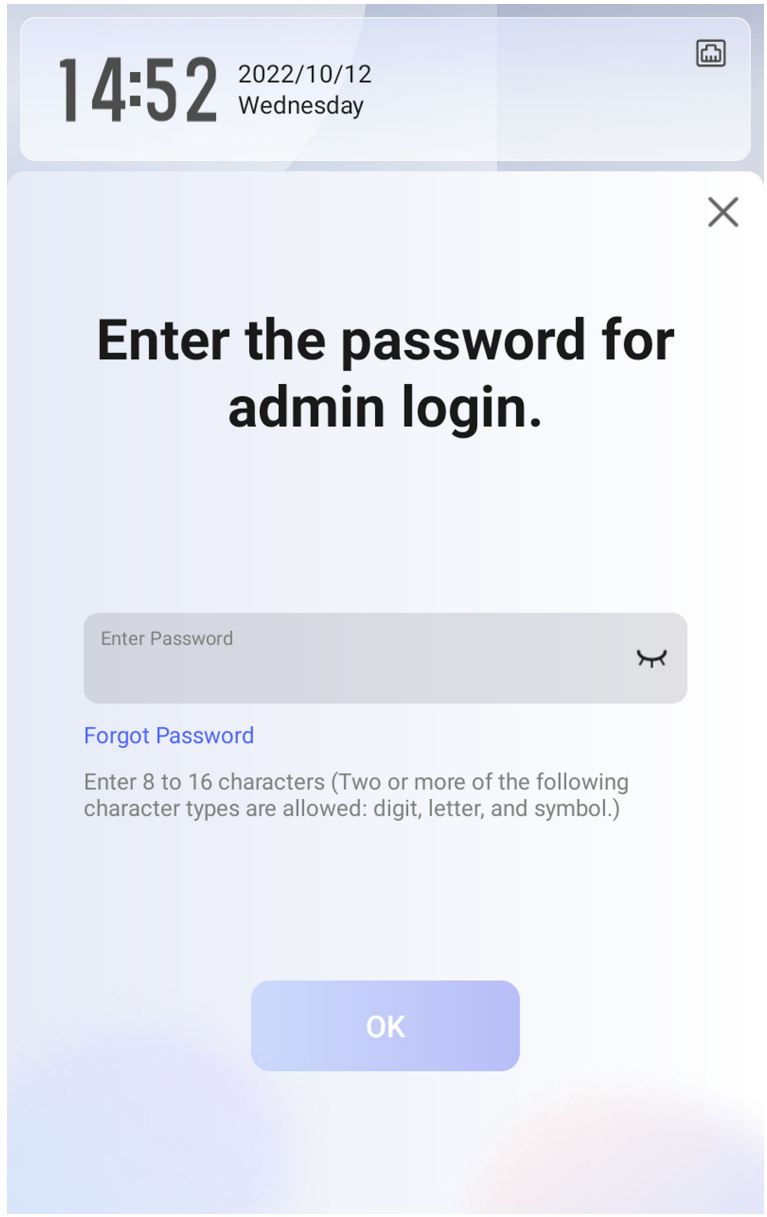


Figure 4-4 Password Authentication Page

3. Tap **Forgot Password**.
4. Answer the security questions that configured when activation.
5. Create a new password and confirm it.
6. Tap **OK**.

4.2 Communication Settings

You can set the network parameters, the Wi-Fi parameter, the RS-485 parameters, the Wiegand parameters, and enable 3G/4G on the communication settings page.

4.2.1 Set Wired Network Parameters

You can set the device wired network parameters, including the IP address, the subnet mask, the gateway, and DNS parameters.

Steps

1. Tap **Comm.** (Communication Settings) on the Home page to enter the Communication Settings page.
2. On the Communication Settings page, tap **Wired Network**.

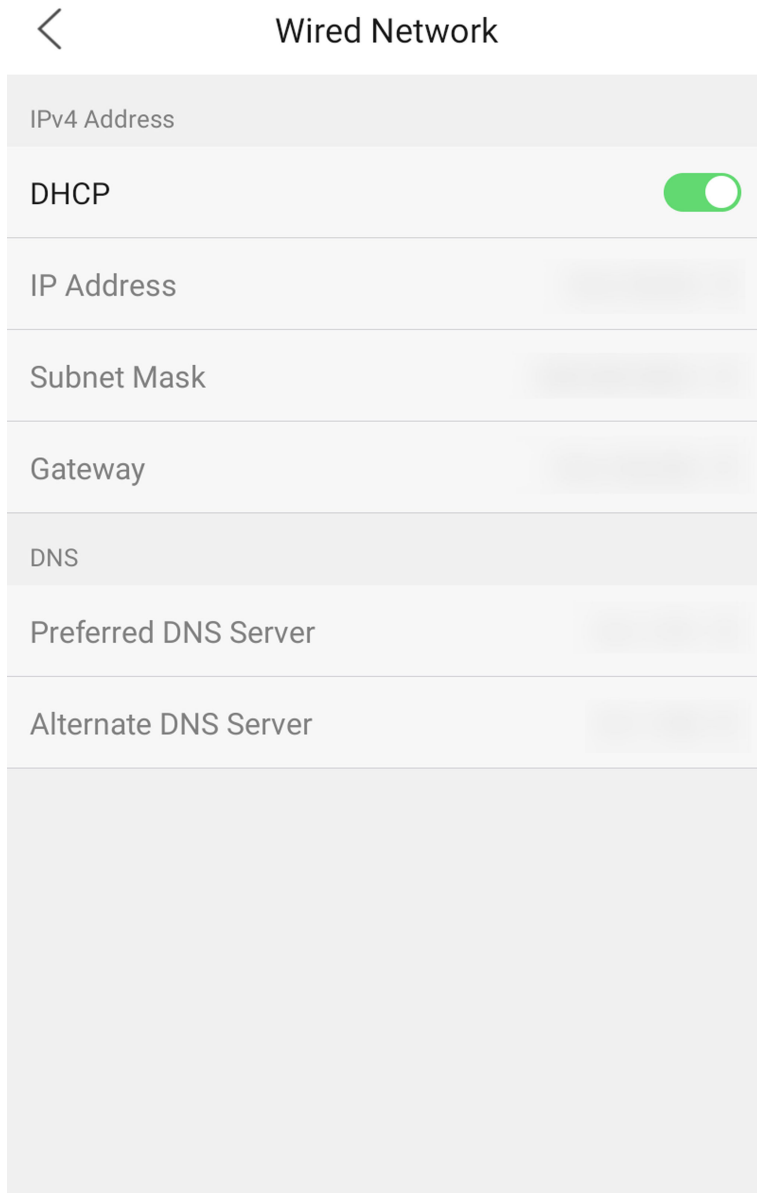


Figure 4-5 Wired Network Settings

3. Set IP Address, Subnet Mask, and Gateway.
   - Enable **DHCP**, and the system will assign IP address, subnet mask, and gateway automatically.
   - Disable **DHCP**, and you should set the IP address, subnet mask, and gateway manually.

   Note
   - The device's IP address and the computer IP address should be in the same IP segment.
   - IP address of 192.168.1.64, and 192.168.1.7 are not suggested to use.
4. Set the DNS parameters. You can enable **Auto Obtain DNS**, set the preferred DNS server and the alternate DNS server.

4.2.2 Set Wi-Fi Parameters

You can enable the Wi-Fi function and set the Wi-Fi related parameters.

Steps

Note

The function should be supported by the device.

1. Tap **Communication** on the Home page to enter the Communication Settings page.
2. On the Communication Settings page, tap **Wi-Fi** to enter the page of Wi-Fi.

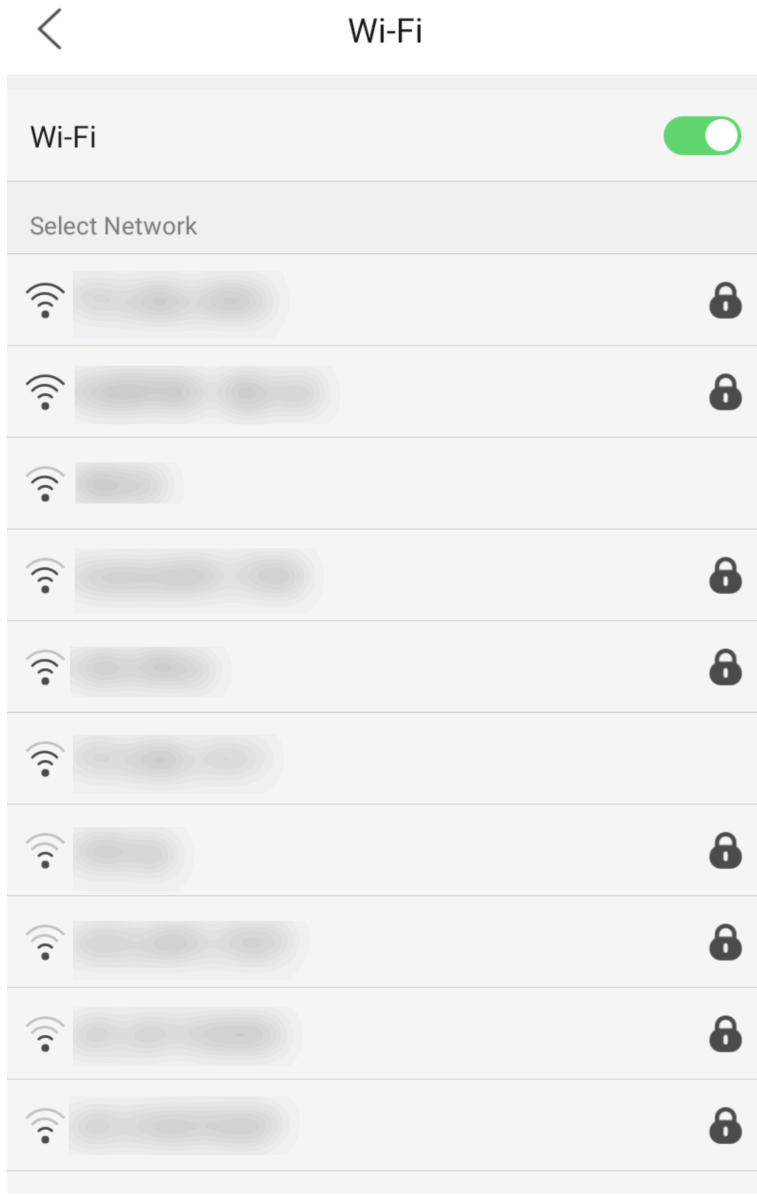


Figure 4-6 Wi-Fi Settings

3. Enable the Wi-Fi function.
4. Configure the Wi-Fi parameters.
   - Select a Wi-Fi from the list, and enter the Wi-Fi's password. Tap **OK**.
   - If the target Wi-Fi is not in the list,tap **Add Wi-Fi**. Enter the Wi-Fi's name and password. And tap **OK**.

Note

Only digits, letters, and special characters are allowed in the password.

5. Set the Wi-Fi's parameters.

- By default, DHCP is enable. The system will allocate the IP address, the subnet mask, and the gateway automatically.
- If disable DHCP, you should enter the IP address, the subnet mask, and the gateway manually.

6. Tap **OK** to save the settings and go back to the Wi-Fi tab.
7. Tap ✓ to save the network parameters.

4.2.3 Set RS-485 Parameters

The face recognition terminal can connect external access controller, secure door control unit or card reader via the RS-485 terminal.

Steps

1. Tap **Comm.** (Communication Settings) on the Home page to enter the Communication Settings page.
2. On the Communication Settings page, tap **RS-485** to enter the RS-485 tab.

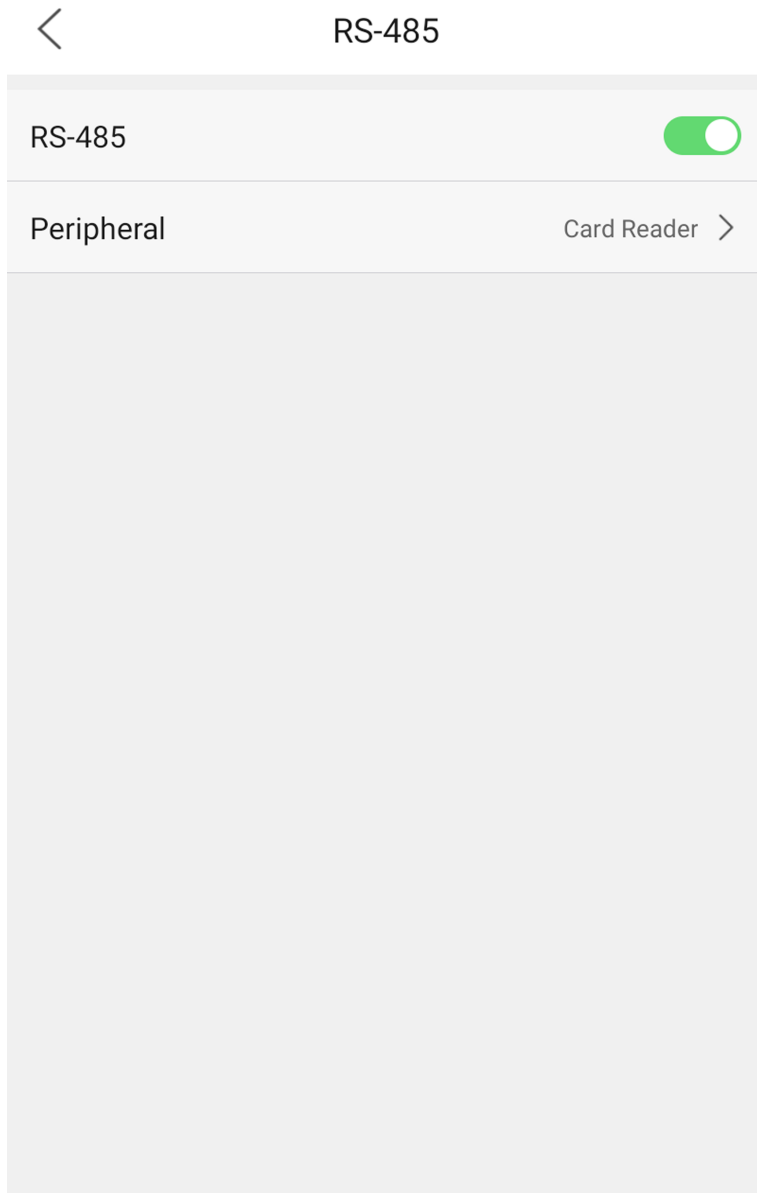


Figure 4-7 Set RS-485 Parameters

3. Enable **RS-485 Settings**.
4. Select an peripheral type according to your actual needs.

Note

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

5. Tap the back icon at the upper left corner and you should reboot the device if you change the parameters.

4.2.4 Set Wiegand Parameters

You can set the Wiegand transmission direction.

Steps

1. Tap **Communication** on the Home page to enter the Communication Settings page.
2. On the Communication Settings page, tap **Wiegand** to enter the Wiegand tab.
3. Enable the Wiegand function.
4. Select a transmission direction.
   - Output: A face recognition terminal can connect an external access controller. And the two devices will transmit the card No. via Wiegand 34.
   - Input: A face recognition terminal can connect a Wiegand card reader.
5. Tap ✓ to save the network parameters.

Note

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

4.2.5 Set ISUP Parameters

Set ISUP parameters and the device can upload data via ISUP protocol.

Before You Start

Make sure your device has connect to a network.

Steps

1. Tap **Comm.** → **ISUP** .

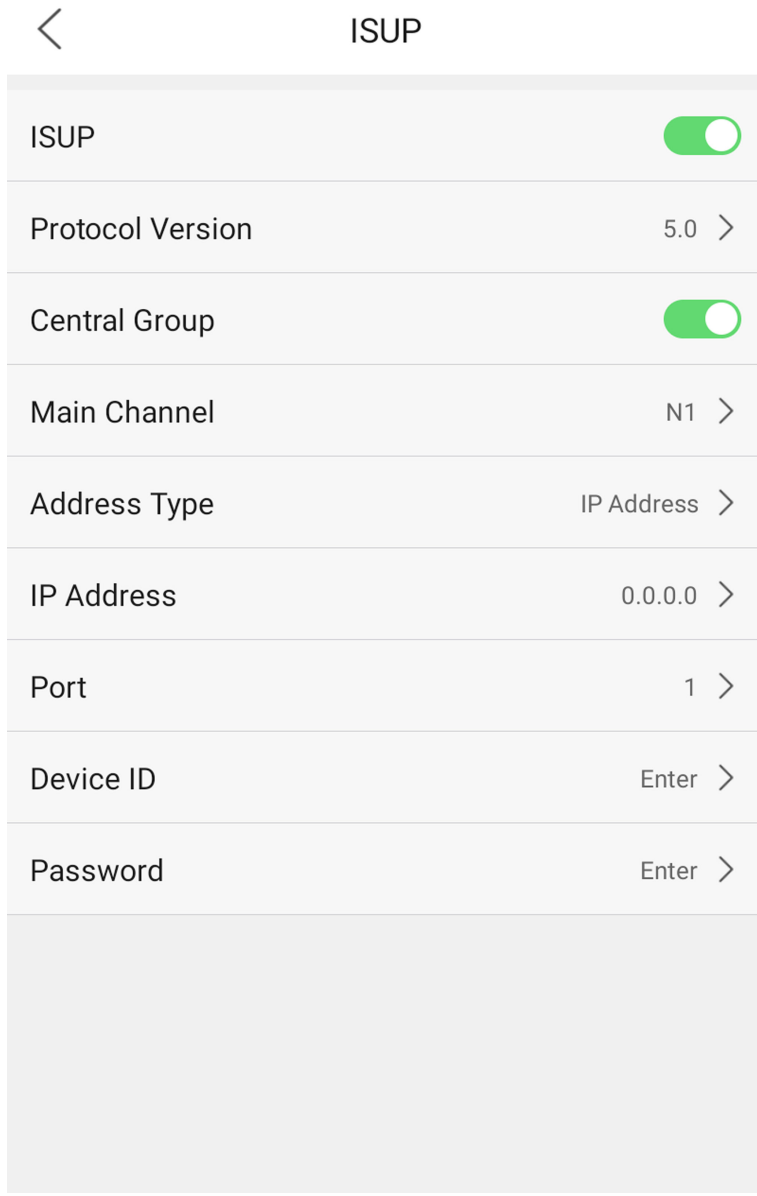


Figure 4-8 ISUP Settings

2. Enable the ISUP function and set the ISUP server parameters.

ISUP Version

Set the ISUP version according to your actual needs.

Central Group

Enable central group and the data will be uploaded to the center group.

Main Channel

Support N1 or None.

ISUP

Enable ISUP function and the data will be uploaded via ISUP protocol.

Address Type

Select an address type according to your actual needs.

IP Address

Set the ISUP server's IP address.

Port No.

Set the ISUP server's port No.

Note

Port No. Range: 0 to 65535.

Device ID

Set device serial no.

ISUP Key

If you choose V5.0, you should create an account and ISUP key. If you choose other version, you should create an ISUP account only.

Note

- Remember the ISUP account and ISUP key. You should enter the account name or the key when the device should communicate with other platforms via ISUP protocol.
- ISUP key range: 8 to 32 characters.

4.2.6 Platform Access

You can change the device verification code and set the server address before you add the device to the Hik-Connect mobile client.

Before You Start

Make sure your device has connected to a network.

Steps

1. Tap **Comm.** (Communication Settings) on the Home page to enter the Communication Settings page.
2. On the Communication Settings page, tap **Hik-Connect**.
3. Enable **Hik-Connect**
4. View connection status.
5. Enter **IP Address**.
6. Create the **Verification Code**, and you need to enter the verification code when you manage the devices via **Hik-Connect**.

4.2.7 Enable Mobile Network

You can enable **Mobile Network**function to connect the mobile network .

Note

You can set mobile network when the device supports this function.

Tap **Communication** on the main page to enter the Communication Settings page, and enable **Mobile Network**.

4.3 Person Management

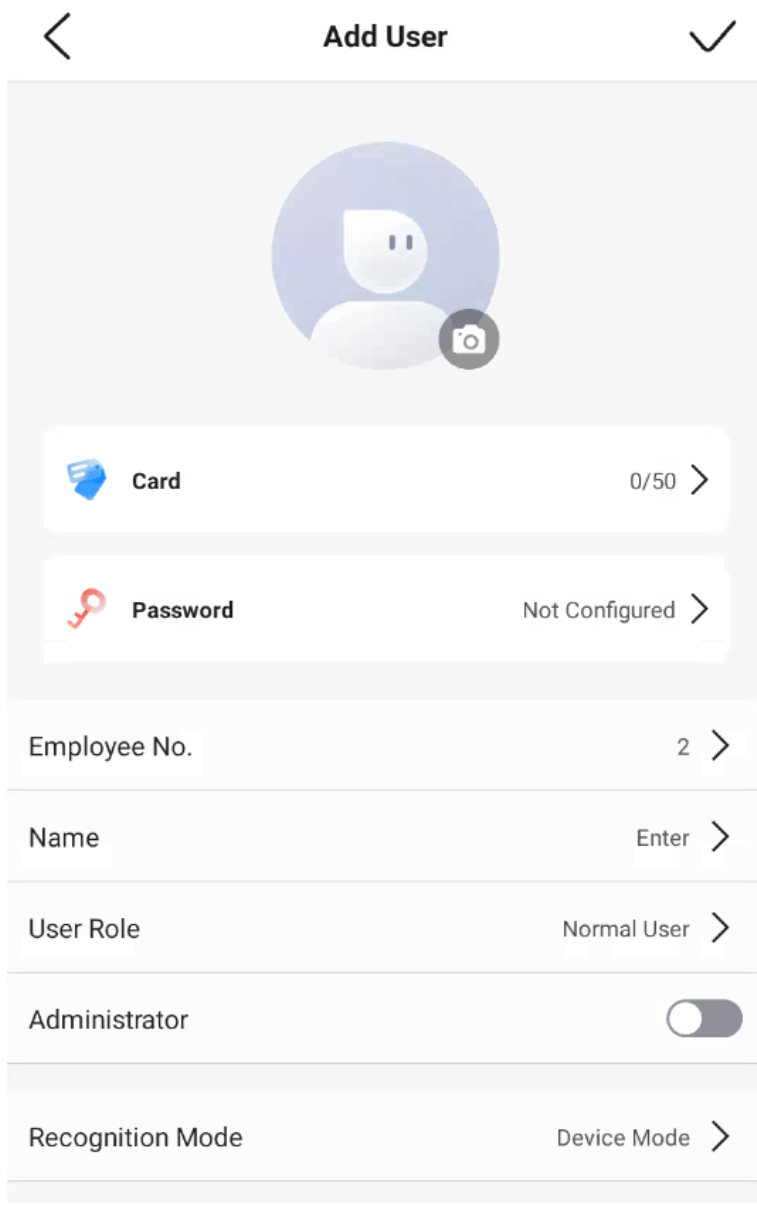
On the person management interface, you can add, edit, delete and search the person.

4.3.1 Add Administrator

The administrator can log in the device backend and configure the device parameters.

Steps

1. Long tap on the initial page for 3 s and slide to the left/right by following the gesture and enter the device backend.
2. Tap **Person → +** to enter the Add Person page.



3. Edit the employee ID.

Note

- The employee ID should be less than 32 characters. And it can be a combination of lower letters, upper letters, and numbers.
- The employee ID should not be duplicated.

4. Tap the Name field and input the person name on the soft keyboard.

Note

- Numbers, upper case letters, lower case letters, and special characters are allowed in the person name.
- Up to 32 characters are allowed in the person name.

5. **Optional:** Add a face picture, fingerprints, cards, PIN for the administrator.

Note

- For details about adding a face picture, see ***Add Face Picture*** .
- For details about adding a fingerprint, see ***Add Fingerprint*** .
- For details about adding a card, see ***Add Card*** .
- For details about adding a password, see ***View PIN code*** .

6. **Optional:** Set the administrator's authentication type.

Note

For details about setting the authentication type, see ***Set Authentication Mode*** .

7. Set the **Person Type** and **Person Role**.
8. You can enable **Attendance Check Only**.
9. Tap ✓ to save the settings.

4.3.2 Add Face Picture

Add person's face picture to the device. And the person can use the face picture to authenticate.

Steps

1. Long tap on the initial page for 3 s and slide to the left/right by following the gesture and log in the backend.
2. Tap **Person → +** to enter the Add Person page.
3. Edit the employee ID.

Note

- The employee ID should be less than 32 characters. And it can be a combination of lower letters, upper letters, and numbers.
- The employee ID should not be duplicated.

4. Tap the Name field and input the person name on the soft keyboard.

Note

- Numbers, upper case letters, lower case letters, and special characters are allowed in the person name.
- The suggested person name should be within 32 characters.

5. Tap the Face Picture field to enter the face picture adding page.

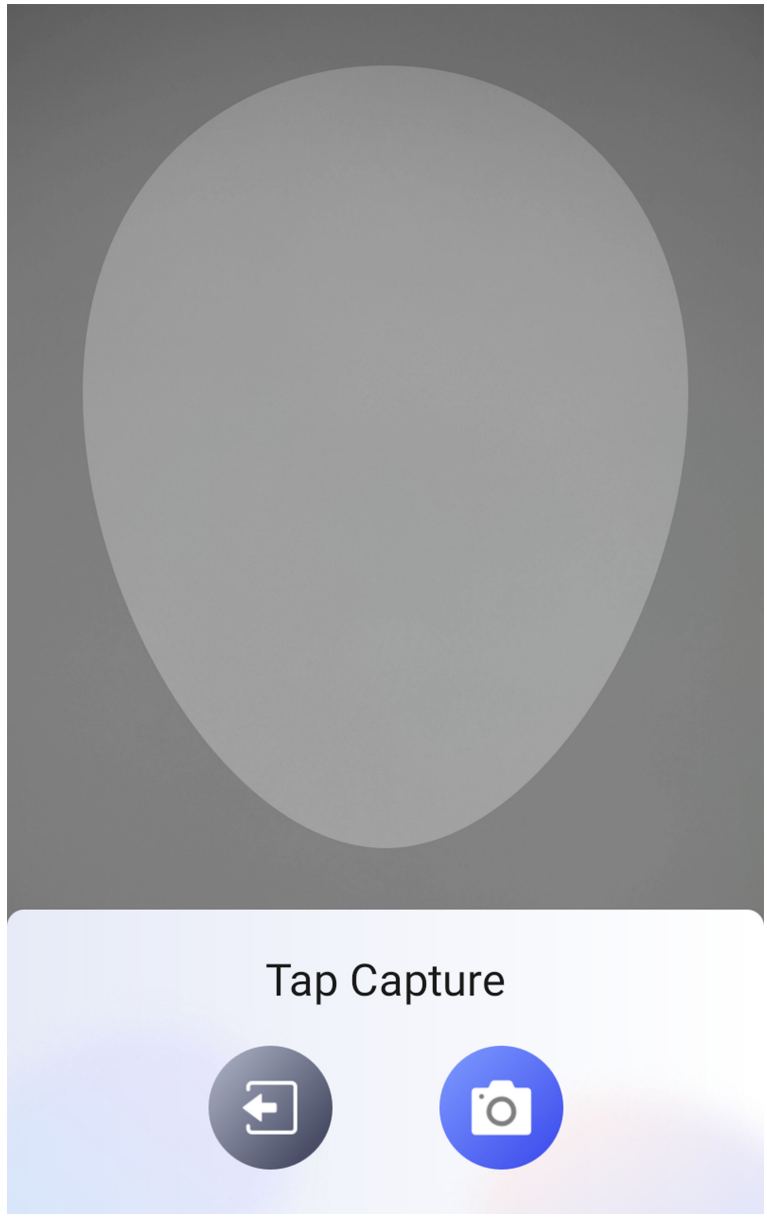


Figure 4-9 Add Face Picture

6. Look at the camera.

Note

- Make sure your face picture is in the face picture outline when adding the face picture.
- Make sure the captured face picture is in good quality and is accurate.
- For details about the instructions of adding face pictures, see ***Tips When Collecting/ Comparing Face Picture*** .

After completely adding the face picture, a captured face picture will be displayed at the upper right corner of the page.

7. Tap **Save** to save the face picture.
8. **Optional:** Tap **Try Again** and adjust your face position to add the face picture again.
9. Set the person type.

Basic Person

The person is the normal person. The person can only authenticate or take attendance on the initial page. You can also set the basic person as an **Administrator** by enable the administrator function.

Visitor

The person is a visitor.

Person in Blocklist

The person is in the blocklist. When the person starts authentication, an event will be upload.

Custom Type

Set the custom person type.

10. Tap ✓ to save the settings.

4.3.3 Add Fingerprint

Add a fingerprint for the person and the person can authenticate via the added fingerprint.

Steps

Note

The function should be supported by the device.

1. Long tap on the initial page for 3 s and slide to the left/right by following the gesture and enter the device backend.
2. Tap **Person → +** to enter the Add Person page.
3. Tap the Employee ID. field and edit the employee ID.

Note

- The employee ID should be less than 32 characters. And it can be a combination of lower letters, upper letters, and numbers.
- The employee ID should not start with 0 and should not be duplicated.

4. Tap the Name field and input the person name on the soft keyboard.

Note

- Numbers, upper case letters, lower case letters, and special characters are allowed in the person name.
- The suggested person name should be within 32 characters.

5. Tap the Fingerprint field to enter the Add Fingerprint page.
6. Follow the instructions to add a fingerprint.

Note

- The same fingerprint cannot be repeatedly added.
- Up to 10 fingerprints can be added for one person.
- You can also use the client software or the fingerprint recorder to record fingerprints. For details about the instructions of scanning fingerprints, see ***Tips for Scanning Fingerprint*** .

7. Tap ✓ to save the settings.

4.3.4 Add Card

Add a card for the person and the person can authenticate via the added card.

Steps

Note

The supported card type varies between different models.

1. Long press OK and login the device.
2. Select **Person → Add Person** to enter the Add person page.
3. Select the Employee ID field and edit the employee ID.

Note

- The employee ID should be less than 32 characters. And it can be a combination of lower letters, upper letters, and numbers.
- The employee ID should not be duplicated.

4. Select the Name field and input the person name on the keyboard.

Note

- Numbers, upper case letters, lower case letters, and special characters are allowed in the person name.
- The suggested person name should be within 128 characters.

5. Select the Card field and press OK to enter the Add Card page.
6. Configure the card No.
   - Enter the card No. manually.
   - Present the card over the card swiping area to get the card No.

Note

- The card No. cannot be empty.
- Up to 20 characters are allowed in the card No.
- The card No. cannot be duplicated.

7. Configure the card type.

8. Set the person role.
9. Press ESC and then press OK to save the settings.

4.3.5 View PIN code

Add a PIN code for the person and the person can authenticate via the PIN code.

Steps

1. Long tap on the initial page for 3 s and slide to the left/right by following the gesture and log in the backend.
2. Tap **Person → +** to enter the Add Person page.
3. Tap the Employee ID. field and edit the employee ID.

Note

- The employee ID should be less than 32 characters. And it can be a combination of lower letters, upper letters, and numbers.
- The employee ID should not be duplicated.

4. Tap the Name field and input the person name on the soft keyboard.

Note

- Numbers, upper case letters, lower case letters, and special characters are allowed in the person name.
- The suggested person name should be within 32 characters.

5. Tap the PIN code to view the PIN code.

Note

The PIN code cannot be edited. It can only be applied by the platform.

6. Tap ✓ to save the settings.

4.3.6 Set Authentication Mode

After adding the user's face picture, password, or other credentials, you should set the authentication mode and the user can authenticate his/her identity via the configured authentication mode.

Steps

1. Long tap on the initial page for 3 s and slide to the left/right by following the gesture and log in the backend.
2. Tap **Person → Add Person/Edit Person → Authentication Mode** .
3. Select Device or Custom as the authentication mode.

   Device

If you want to select device mode, you should set the terminal authentication mode in Access Control Settings page first. For details see *Setting Access Control Parameters*.

Custom

You can combine different authentication modes together according to your actual needs.

4. Tap ✓ to save the settings.

4.3.7 Edit Person

After adding the person, you can edit it.

Edit Person

On the Person Management page, select a person from the person List to enter the person Information page. Follow the steps in ***Person Management*** to edit the person parameters. Press ESC to save the settings.

Note

The employee ID cannot be edited.

4.4 Data Management

You can delete data, import data, and export data.

4.4.1 Delete Data

Delete user data.

On the Home page, tap **Data → Delete Data → User Data** . All user data added in the device will be deleted.

4.4.2 Import Data

Steps

1. Plug a USB flash drive in the device.
2. On the Home page, tap **Data → Import Data** .

Note

After insert the USB flash driver, you can tap **Import Data** on the **Data** page.

3. Tap **User Data**, **Face Data** or **Access Control Parameters** .

Note

The imported access control parameters are configuration files of the device.

4. Enter the created password when you exported the data. If you do not create a password when you exported the data, leave a blank in the input box and tap **OK** immediately.

Note

- If you want to transfer all user information from one device (Device A) to another (Device B), you should export the information from Device A to the USB flash drive and then import from the USB flash drive to Device B. In this case, you should import the user data before importing the profile photo.
- The supported USB flash drive format is FAT32.
- The imported pictures should be saved in the folder (named enroll_pic) of the root directory and the picture's name should be follow the rule below:
  Card No._Name_Department_Employee ID_Gender.jpg
- If the folder enroll_pic cannot save all imported pictures, you can create another folders, named enroll_pic1, enroll_pic2, enroll_pic3, enroll_pic4, under the root directory.
- The employee ID should be less than 32 characters. It can be a combination of lower letters, upper letters, and numbers. It should not be duplicated, and should not start with 0.
- Requirements of face picture should follow the rules below: It should be taken in full-face view, directly facing the camera. Do not wear a hat or head covering when taking the face picture. The format should be JPEG or JPG. The resolution should be 640 × 480 pixel or more than of 640 × 480 pixel. The picture size should be between 60 KB and 200 KB.

4.4.3 Export Data

Steps

1. Plug a USB flash drive in the device.
2. On the Home page, tap **Data → Export Data** .

Note

After insert the USB flash driver, you can tap **Export Data** on the **Data** page.

3. Tap **Face Data**, **Event Data**, **User Data**, or **Access Control Parameters**.

Note

The exported access control parameters are configuration files of the device.

4. **Optional:** Create a password for exporting. When you import those data to another device, you should enter the password.

Note

- The supported USB flash drive format is DB.
- The system supports the USB flash drive with the storage of 1G to 32G. Make sure the free space of the USB flash drive is more than 512M.
- The exported user data is a DB file, which cannot be edited.

4.5 Identity Authentication

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

You can authenticate identity via 1:1 matching or 1:N matching.

1:N Matching

Compare the captured face picture with all face pictures stored in the device.

1: 1 Matching

Compare the captured face picture with the linked face picture.

4.5.1 Authenticate via Single Credential

Set the user authentication type before authentication. For details, see ***Set Authentication Mode*** .

Authenticate face, fingerprint, card or QR code.

Face

Face forward at the camera and start authentication via face.

Fingerprint

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

Card

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

Note

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

QR Code

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

Note

- Authentication via QR code should be supported by the device.
- The dimension of the recognized QR code picture should be larger than 6 cm × 6 cm.

Password

Enter the password to authenticate via password.

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

4.5.2 Authenticate via Multiple Credential

Before You Start

Set the user authentication type before authentication. For details, see ***Set Authentication Mode*** .

Steps

1. If the authentication mode is Card and Face, Password and Face, Card and Password, Card and Face and Fingerprint, authenticate any credential according to the instructions on the live view page.

Note

- After enabling **Control Initial Authentication Type**on the web client, the initial authentication type will be fixed.
- The card can be normal IC card, or encrypted card.
- The card can be normal IC card, or encrypted card.
- If the QR Code Scanning function is enabled, you can put the QR code in front of the device camera to authenticate via QR code.
- The dimension of the recognized QR code picture should be larger than 6 cm × 6 cm.
- The dimension of the recognized QR code picture should be larger than 6 cm × 6 cm.

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

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

4.6 System Settings

You can set the sound settings, screen brightness, language and time settings.

Long tap on the initial page for 3 s and slide to the left/right by following the gesture and login the device home page. Tap **Basic**.

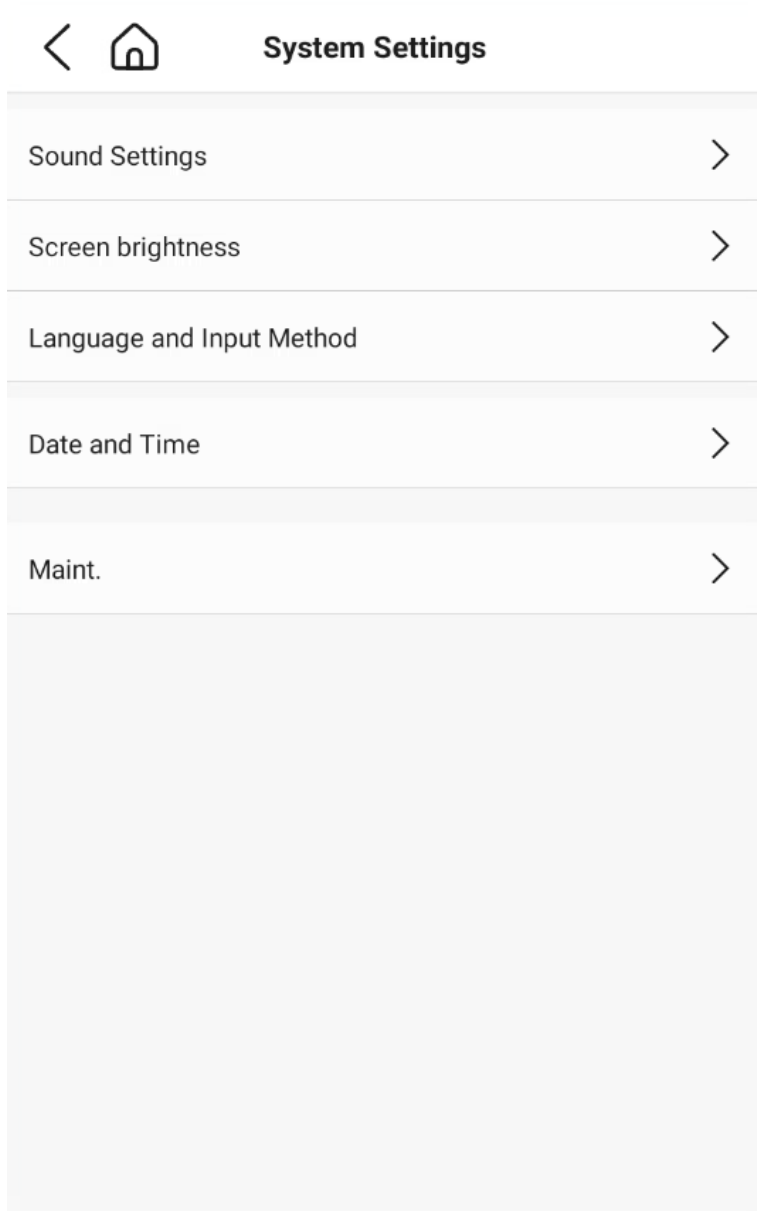


Figure 4-10 Basic Settings Page

Sound Settings

You can enable/disable the voice prompt function and adjust the voice volume.

Note

You can set the voice volume between 0 and 10.

Screen Brightness

You can adjust screen brightness.

Language and Input Method

Select the language according to actual needs.

Time Settings

Set the time zone, the device time and the DST.

4.7 Password Management

You can change device password.

Steps

1. Long tap on the initial page for 3 s and slide to the left/right by following the gesture and login the device home page. Tap **Privacy Management** .
2. Tap **Change Password**. Enter the old password.
3. Enter the new password and confirm it.
4. Tap **OK**.

Note

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 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.

Proper configuration of all passwords and other security settings is the responsibility of the service provider and/or end-user.

5. You can select **Password Change Type** and set the content.

4.8 Set Smart Parameters

4.8.1 Set Multiple Faces Recognition and Face Duplicate Check

You can recognition multiple faces at the same time and check face duplicate.

Long tap on the initial page for 3 s and slide to the left/right by following the gesture. Login and tap **Smart Settings → Face Recognition Settings → .** . After multiple faces recognition is enabled, multiple faces recognition is supported.

Long tap on the initial page for 3 s and slide to the left/right by following the gesture. Login and tap **Smart Settings → Face Duplicate Check → .** . After Face Duplicate Check is enabled, same or similar face will be checked.

4.8.2 Set Face Liveness Level

Set the matching security level when performing face anti-spoofing authentication

Long tap on the initial page for 3 s and slide to the left/right by following the gesture. Login and tap **Smart Settings → Face Recognition Settings** .

After enabling face anti-spoofing function, you can set the matching security level when performing face anti-spoofing authentication. The higher the level, the more strict of the recognition.

4.8.3 Set Face Recognition Distance

Set the valid distance between the person and the device camera.

Long tap on the initial page for 3 s and slide to the left/right by following the gesture. Login and tap **Smart Settings → Face Recognition Settings** .

Set the valid distance between the person and the device camera when authenticating.

4.8.4 Set Face Recognition Interval

You can set the time interval between 2 continuous face recognitions when authenticating.

Long tap on the initial page for 3 s and slide to the left/right by following the gesture. Login and tap **Smart Settings → Face Recognition Settings** .

Set the time interval between 2 continuous face recognitions when authenticating.

Note

You can input the number from 1 to 10.

4.8.5 Set Face 1:1/1:N Security Level

Set the face recognition threshold.

Long tap on the initial page for 3 s and slide to the left/right by following the gesture. Login and tap **Smart Settings → Face Recognition Settings** .

Set the parameters.

Face 1:1 Security Level

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.

Face 1:N Security Level

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.

4.8.6 Set ECO Mode

After enabling the ECO mode, the device will use the IR camera to authenticate faces in the low light or dark environment.

Long tap on the initial page for 3 s and slide to the left/right by following the gesture. Login and tap **Smart Settings → Face Recognition Settings** .

After enabling the ECO mode, the device will use the IR camera to authenticate faces in the low light or dark environment. And you can set the ECO mode threshold, ECO mode (1:N), and ECO mode (1:1).

ECO Threshold

When enabling the ECO mode, you can set the ECO mode's threshold. The larger the value, the easier the device entering the ECO mode.

ECO Mode (1:1)

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

ECO Mode (1:N)

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

4.8.7 Enable NFC Card

Enable NFC card function and you can present NFC card on the device to authenticate.

Steps

1. On the Home page, tap **Smart Settings → Card Settings** to enter the Access Control Settings page.
2. Enable the function and you can present the NFC card to authenticate.

4.8.8 Enable M1 Card and M1 Car d Encryption

Enable M1 card function and you can present M1 card on the device to authenticate. M1 card encryption can improve the security level of authentication.

Steps

1. On the Home page, tap **Smart Settings → Face Recognition Settings** to enter the Access Control Settings page.
2. Set the M1 card function.

Enable M1 Card

Enable the function and you can present the M1 card to authenticate.

M1 Card Encryption

Enable the function and set the sector ID.

Note

- The sector ID ranges from 1 to 100.
- By default, Sector 13 is encrypted. It is recommended to encrypt sector 13.

4.8.9 Set Face with Mask Detection

After enabling the face with mask detection, the system will recognize the captured face with mask picture.

Long tap on the initial page for 3 s and slide to the left/right by following the gesture. Login and tap **Smart Settings → Face Recognition Settings** .

After enabling the face with mask detection, the system will recognize the captured face with mask picture. You can set face with mask & face 1:N level and the strategy.

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.

4.9 Set Access Control Parameters

4.9.1 Set Terminal Authentication Mode

Set the device's authentication mode. You can also customize the authentication mode. if authenticating on the device, you should follow the device's authentication mode.

On the Home page, tap **ACS** (Access Control Settings) to enter the Access Control Settings page.

Select the face recognition terminal's authentication mode. You can also customize the authentication mode.

Note

- Only the device with the fingerprint module supports the fingerprint related function.
- Biometric recognition products are not completely applicable to anti-spoofing environments. If you require a higher security level, use multiple authentication modes.
- If you adopt multiple authentication modes, you should authenticate other methods before authenticating face.

4.9.2 Set Card Reader Authentication Mode

Set the card reader's authentication mode and if authenticating on the card reader, you should follow the card reader's authentication mode.

On the Home page, tap **ACS** (Access Control Settings) to enter the Access Control Settings page.

Select **Sub Card Reader Authentication**. If authenticating on the card reader, you should follow the card reader's authentication mode.

4.9.3 Set Door Contact Parameters

If connecting a door contact, you should confirm the NO or NC connection method. Select remain open or remain closed according to actual NO/NC connection method.

On the Home page, tap **ACS** (Access Control Settings) to enter the Access Control Settings page.

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

4.9.4 Set Duration of Open Linked Gate

Set the door unlocking duration.

On the Home page, tap **ACS** (Access Control Settings) to enter the Access Control Settings page.

Set the Duration of Open Linked Gate. If the door is not opened for the set time, the door will be locked. Available door locked time range: 1 to 255s.

4.9.5 Enable Face Authentication Manually

You can enable face authentication manually.

Steps

1. Login the device. For details, see ***Login*** .
2. Tap **ACS**.
3. Enable Face Authentication Manually. If the function is enabled, person needs to tap Authenticate to start authentication.

4. Select **Trigger Face Recognition Manually Mode**, you can select **Single Authentication** or **Continuous Authentication**.

4.9.6 Set Password Mode

You can set the password mode and choose whether to edit password on device / PC web, or platform.

Steps

1. Login the device. For details, see ***Login*** .
2. Tap **ACS**.
3. Tap **Password Mode** and set the mode.

   Platform-Applied Personal PIN

   The PIN is managed and distributed by the platform after the device accesses the platform.

   Device-Set Personal PIN

   The PIN is set on the device or PC Web.
4. Go back to the previous page to save the settings.

4.10 Time and Attendance Status Settings

You can set the attendance mode as check in, check out, break out, break in, overtime in, and overtime out according to your actual situation.

Note

The function should be used cooperatively with time and attendance function on the client software.

4.10.1 Disable Attendance Mode via Device

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

Tap **Attendance Status** to enter the Attendance Status page.

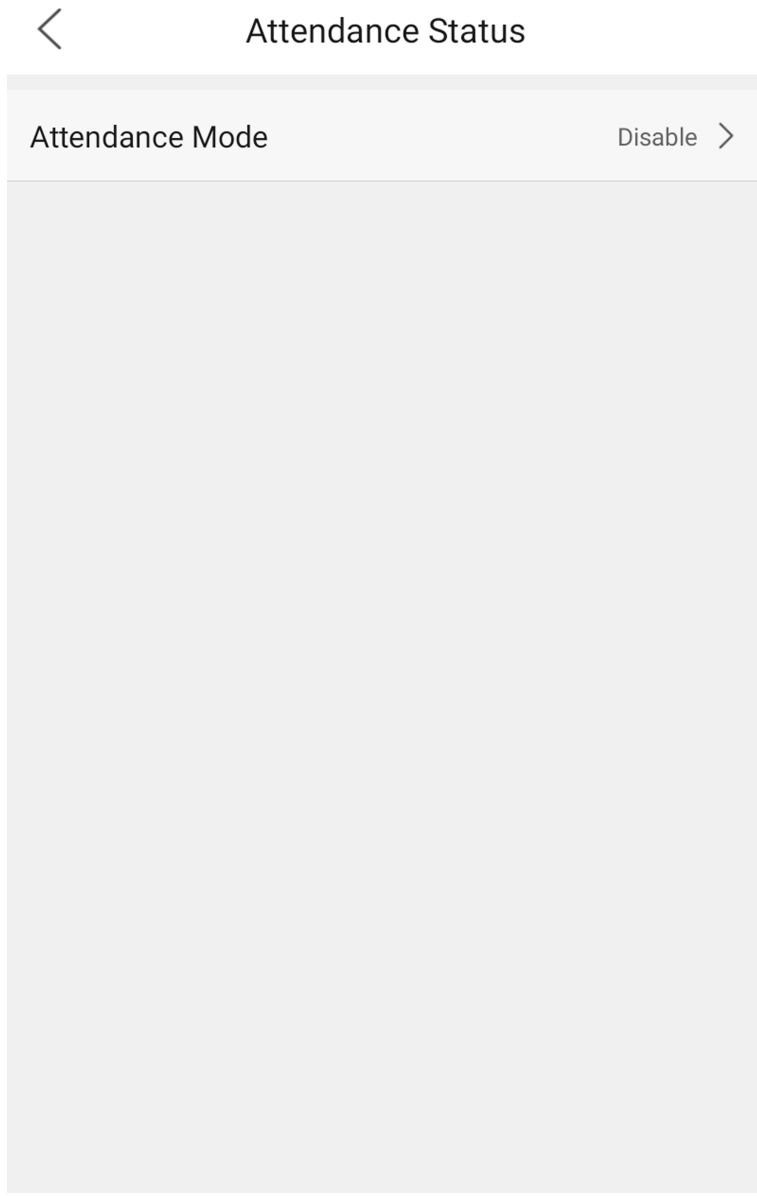


Figure 4-11 Disable Attendance Mode

Set the **Attendance Mode** as **Disable**.

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.

4.10.2 Set Manual Attendance via Device

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. Tap **Attendance Status** to enter the Attendance Status page.
2. Set the **Attendance Mode** as **Manual**.

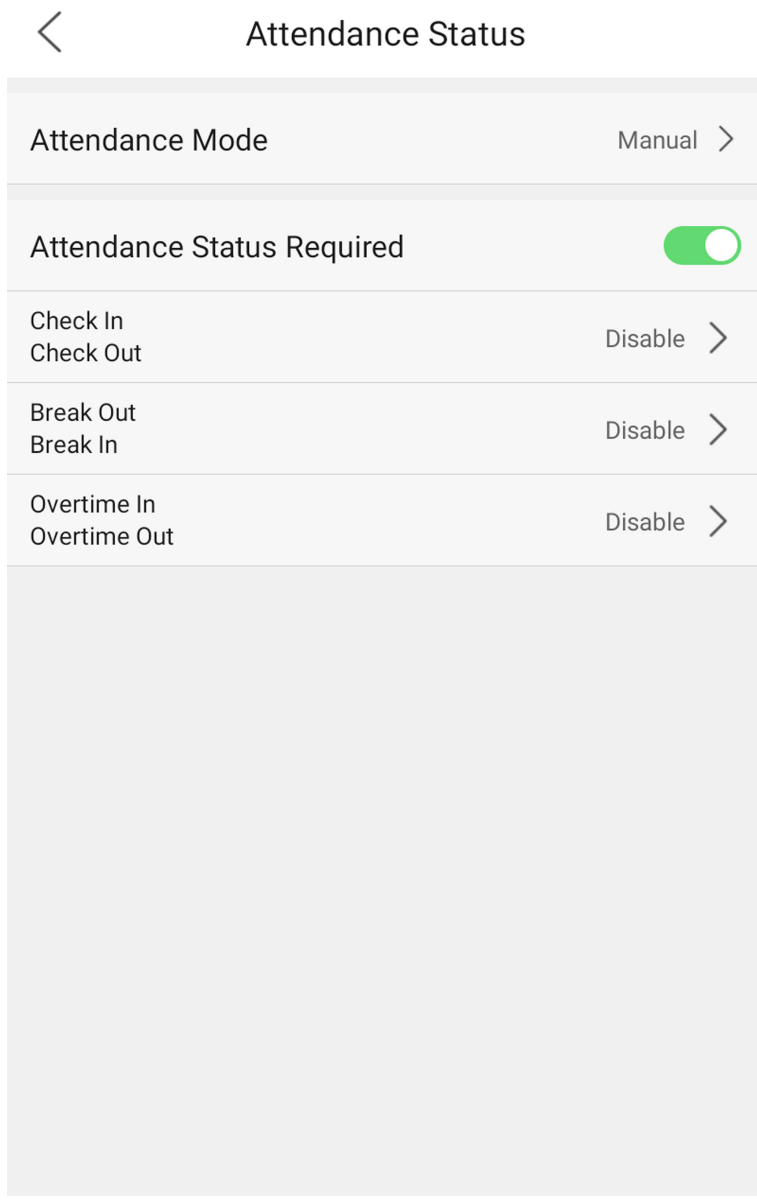


Figure 4-12 Manual Attendance Mode

3. Enable the **Attendance Status Required**.
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.

   The name will be displayed on the T & A Status page and the authentication result page.

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.

4.10.3 Set Auto Attendance via Device

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. Tap **Attendance Status** to enter the Attendance Status page.
2. Set the **Attendance Mode** as **Auto**.

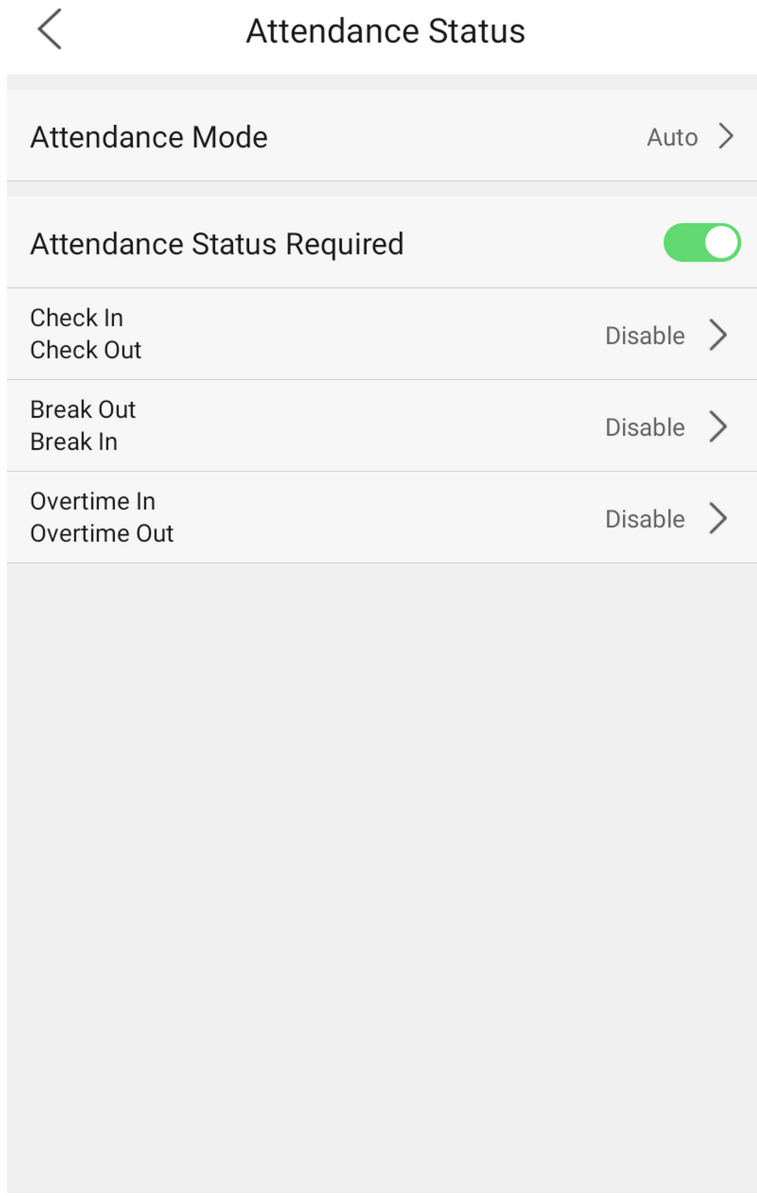


Figure 4-13 Auto Attendance Mode

3. Enable the **Attendance Status** 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.

   The name will be displayed on the T & A Status page and the authentication result page.
6. Set the status' schedule.

   1) Tap **Attendance Schedule**.

2) Select **Monday**, **Tuesday**, **Wednesday**, **Thursday**, **Friday**, **Saturday**, or **Sunday**.
3) Set the selected attendance status's start time of the day.
4) Tap **Confirm**.
5) Repeat step 1 to 4 according to your actual needs.

Note

The attendance status will be valid within the configured schedule.

Result

When you authenticate on the initial page, the authentication will be marked as the configured attendance status according to the configured schedule.

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.

4.10.4 Set Manual and Auto Attendance via Device

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. Tap **Attendance Status** to enter the Attendance Status page.
2. Set the **Attendance Mode** as **Manual and Auto**.

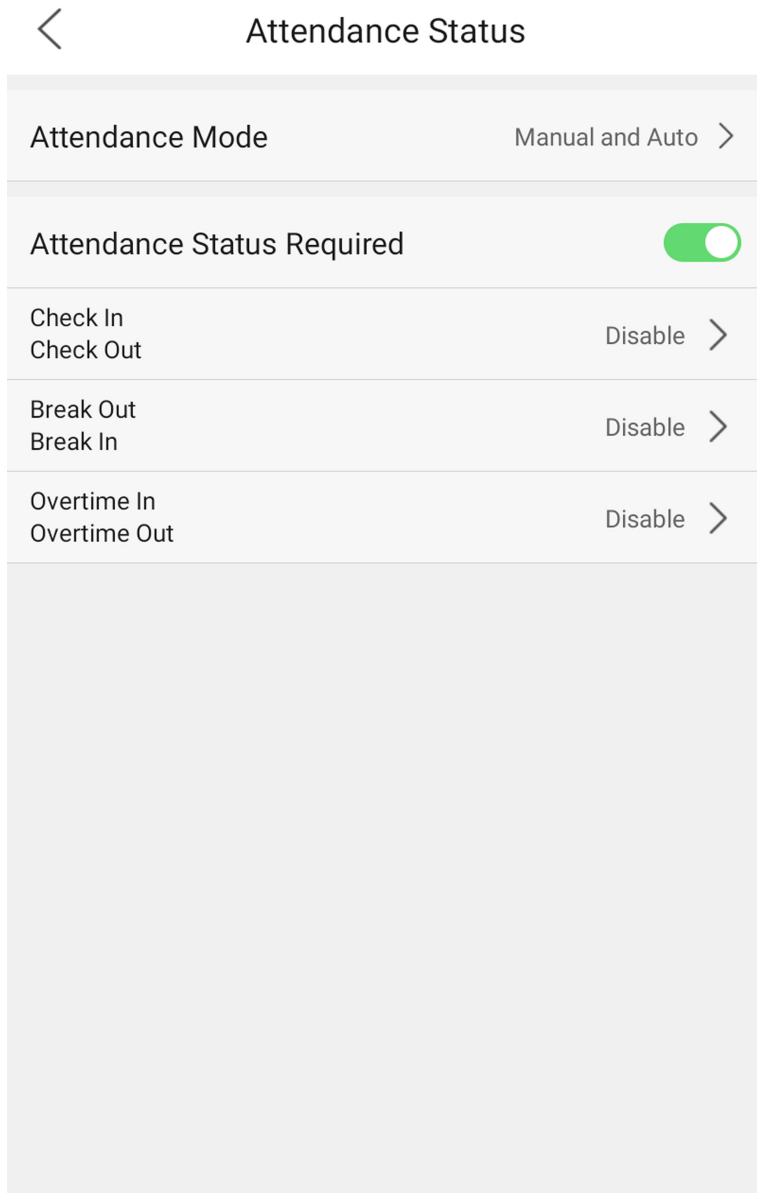


Figure 4-14 Manual and Auto Mode

3. Enable the **Attendance Status** 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.

   The name will be displayed on the T & A Status page and the authentication result page.
6. Set the status' schedule.

   1) Tap **Attendance Schedule**.

2) Select **Monday**, **Tuesday**, **Wednesday**, **Thursday**, **Friday**, **Saturday**, or **Sunday**.
3) Set the selected attendance status's start time of the day.
4) Tap **OK**.
5) Repeat step 1 to 4 according to your actual needs.

Note

The attendance status will be valid within the configured schedule.

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.

4.11 Preference Settings

4.11.1 Set Theme Color

You can configure the theme color to light or dark mode.

Steps
1. Tap **Preference** to enter the preference settings page.
2. You can set the theme color of the device as **Light Mode** or **Dark Mode**.

4.11.2 Set Theme Mode

You can set the theme mode.

Steps
1. Tap **Preference → Custom Home Page** to enter the preference settings page.
2. You can set the theme.

Business Scene

Highlight the released information. Not display authentication page. Applicable to scenes where information display is the primary focus.

Enterprise Scene

Supports face and card authentication. Applicable to enterprise office entrance/exit rapid door access and attendance scenes.

Office Scene

Displays doorplate information, personnel work status, and room usage status. Applicable to enterprise office scenes.

4.11.3 Set Screen Content

You can set the displayed Screen Content.

Steps

1. Tap **Screen Display** to enter the preference settings page.
2. Tap **Screen Content**, you can enable **Advertisement Allowed as Screen Saver**, and customize content in PC WEB **Preference → Notice Publication** .
3. You can set **Sleep Duration**.

4.11.4 Set Control Center Displayed Items

You can set the items that displayed in the control center.

Steps

1. Tap **Preference** to enter the preference settings page.
2. Set **Way to Control Center**.

4.12 System Maintenance

You can view the system information and the capacity. You can also upgrade the device, restore to factory settings, restore to default settings, and reboot the device.

4.12.1 View System Information

You can view the device system information.

Long tap on the initial page for 3 s and slide to the left/right by following the gesture. Login and tap **System Settings → Maint. → System Information** .

You can view the device model, serial No., versions, address, production data, and open source code license.

Note

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

4.12.2 View Device Capacity

You can view the number of user, face picture, card, event and fingerprint.

Long tap on the initial page for 3 s and slide to the left/right by following the gesture. Login and tap **System Settings → Maint. → Capacity** .

You can view the number of user, face picture, card, event and fingerprint.

Note

Parts of the device models support displaying the fingerprint number. Refers to the actual page for details.

4.12.3 Upgrade

Choose online upgrading or upgrading via the USB flash drive.

Long tap on the initial page for 3 s and slide to the left/right by following the gesture. Login and tap **System Settings → Maint. → Upgrade** .

Choose one of the following upgrade methods to upgrade.

Online Update

If the device has been connected to Hik-Connect and network, when there is a new installation package in Hik-Connect, you can tap **Device Upgrade → Online Update** to upgrade the device system.

Update via USB

Plug the USB flash drive in the device USB interface. Tap **Device Upgrade → Update via USB** , and the device will read the *digicap.dav* file in the USB flash drive to start upgrading.

4.12.4 View User Manual

View the device user manual.

Long tap on the initial page for 3 s and slide to the left/right by following the gesture. Login and tap **System Settings → Maint. → User Manual** .

Scan the QR code to obtain and view the user manual.

4.12.5 Restore Parameters

Restore to default settings or restore to factory settings.

Long tap on the initial page for 3 s and slide to the left/right by following the gesture. Login and tap **System Settings → Maint.** .

Restore to default settings or restore to factory settings.

Restore to Default Settings

All parameters, except for the communication settings, remotely imported user information, will be restored to the default settings. The system will reboot to take effect.

Restore to Factory Settings

All parameters will be restored to the factory settings. The system will reboot to take effect.

4.12.6 Reboot

Reboot device if needed.

Long tap on the initial page for 3 s and slide to the left/right by following the gesture. Login and tap **Maint.**.

Reboot the device.

4.13 Set Privacy Parameters

Set the event storage type, picture upload and storage parameters, and the picture clearing parameters.

Go to **Configuration → Security → Privacy Settings**

Event Storage Settings

Select a method to delete the event. You can select from **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.

Authentication Settings

Display Authentication Result

You can check **Face Picture**, **Name**, and **Employee ID**, to display the authentication result.

Name De-identification

You can check **Name De-identification**, and the whole name will not be displayed.

Authentication Result Display Duration

You can set the authentication result display duration.

Picture Uploading and Storage

Save Picture When Authenticating

Save picture when authenticating automatically.

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.

Clear All Pictures in Device

Note

All pictures cannot be restored once they are deleted.

Clear Registered Face Pictures

All registered pictures in the device will be deleted.

Clear Captured Pictures

All captured pictures in the device will be deleted.

4.14 Video Intercom

After adding the device to the client software, you can call the device from the client software, call the main station from the device, call the client software from the device, call the indoor station from the device, or call the specific room from the device.

4.14.1 Call Settings

The device can be used as an entrance station or door station, and the video intercom related parameters of the device can be configured

Steps

1. Tap **Call Settings**
2. Tap **Set No.**, and set **Community No.**, **Building No.**, **Unit No.** and **Floor No.**
3. Tap **Call Specific Room**, and set Call Indoor Station No.

4.14.2 Call Client Software from Device

Steps

1. Get the client software from the supplied disk or the official website, and install the software according to the prompts.
2. Run the client software and the control panel of the software pops up.
3. Click **Device Management** to enter the Device Management interface.
4. Add the device to the client software.

Note

For details about adding device, see *Add Device*.

5. Call the client software.
   1) Tap on the device initial page.
   2) Enter ***0*** in the pop-up window.
   3) Tap to call the client software.
6. Tap **Answer** on the pop-up page of the client software and you can start two-way audio between the device and the client software.

Note

If the device is added to multiple client softwares and when the device is calling the client software, only the first client software added the device will pop up the call receiving window.

4.14.3 Call Center from Device

Steps

1. Get the client software from the supplied disk or the official website, and install the software according to the prompts.
2. Run the client software and the control panel of the software pops up.
3. Click **Device Management** to enter the Device Management interface.
4. Add the main station and the device to the client software.

Note

For details about adding device, see *Add Device*.

5. Set the main station's IP address and SIP address in the remote configuration page.

Note

For details about the operation, see the user manual of the main station.

6. Call the center.
   - If you have configured to call center in the ***System Settings*** , you can tap to call the center.
   - If you have not configured to call center in the ***System Settings*** , you should tap → to call the center
7. Answers the call via the main station and starts two-way audio.

Note

The device will call the main station in priority.

4.14.4 Call Device from Client Software

Steps

1. Get the client software from the supplied disk or the official website, and install the software according to the prompts.
2. Run the client software and the control panel of the software pops up.
3. Click **Device Management** to enter the Device Management page.
4. Add the device to the client software.

Note

For details about adding device, see *Add Device*.

5. Enter the **Live View** page and double-click the added device to start live view.

Note

For details about operations in the **Live View** page, see *Live View* in the user manual of the client software.

6. Right click the live view image to open the right-click menu.
7. Click **Start Two-Way Audio** to start two-way audio between the device and the client software.

4.14.5 Call Room from Device

Steps

1. Get the client software from the supplied disk or the official website, and install the software according to the prompts.
2. Run the client software and the control panel of the software pops up.
3. Click **Device Management** to enter the Device Management interface.
4. Add the indoor station and the device to the client software.

Note

For details about adding device, see *Add Device*.

5. Link a user to an indoor station and set a room No. for the indoor station.
6. Call the room.
   - If you have configured a specified room No. in the ***System Settings*** , you can tap to call the room.
   - If you have not configured a specified room No. in the ***System Settings*** , you should tap on the authentication page of the device. Enter the room No. on the dial page and tap to call the room.
7. After the indoor station answers the call, you can start two-way audio with the indoor station.

4.14.6 Call Mobile Client from Device

Steps

1. Get the mobile mobile client from the supplied disk or the official website, and install the software according to the prompts.
2. Run the mobile client and add the device to the mobile client.

Note

For details, see the user manual of the mobile client.

3. Enter **Basic Settings → Shortcut Key** and enable **Call APP**.
4. Go back to the initial page and call the mobile client.
   1) Tap on the device initial page.
   2) Tap to call the mobile client.

4.14.7 Doorbell Call

Steps

1. Get the client software from the supplied disk or the official website, and install the software according to the prompts.
2. Run the client software and the control panel of the software pops up.
3. Click **Device Management** to enter the Device Management interface.
4. Add the device to the client software.

Note

For details about adding device, see *Add Device*.

5. Tap doorbell button to call.
   1) Tap on the device initial page.
   2) Tap to call.

Chapter 5 Quick Operation via Web Browser

5.1 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.

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

5.2 Select Language

You can select a language for the device system.

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

By default, the system language is English.

Note

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

5.3 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.

5.4 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.

5.5 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 50 cards can be supported.

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

Note

Up to 10 fingerprints are allowed.

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

Main Station IP

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

Private Server IP

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

Enable Protocol 1.0

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

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

Chapter 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.

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 Help

6.3.1 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.

6.3.2 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.

6.4 Logout

Log out the account.

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

6.5 Quick Operation via Web Browser

6.5.1 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.

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

6.5.2 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.

6.5.3 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.

6.5.4 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.

6.5.5 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 50 cards can be supported.

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

Note

Up to 10 fingerprints are allowed.

6.5.6 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. 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.

6.6 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.
If you select **Blocklist User**, the user will be reported when recognizing.
Select **Person Role**.
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.
You can enable **Attendance Check Only**. After enabling, this person won't be given access control permission.
Set the organization and door permission.
Select Cartoon avatar.
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.

Add PIN

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

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

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.

6.7 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.

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, mobile data, 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.

Note

Only device installed fingerprint can display the fingerprint capacity.

6.8 Access Control Management

6.8.1 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.

6.8.2 Door Parameter Configuration

Configure parameters for unlocking doors.

Select Door No.

Select a door to configure relative parameters.

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

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

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

View Device Online Status

View and refresh the device status.

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

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

Set Door Name

Create door name.

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

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

Set Open Duration via PC Web

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

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

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

Click **Save**.

Set Door Open Timeout Alarm via PC Web

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

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

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

Click **Save**.

Set 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 Magnetic Sensor Type via PC Web

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

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

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

Click **Save**.

Set Exit Button via PC Web

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

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

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

Click **Save**.

Set 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.

6.8.3 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**.

Control Initial Authentication Type

If disable the function, you can authenticate by any credential that in the selected authentication type for the first authentication. If enable the function, you should follow the displayed sequence.

Steps

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

2. Enable **Control Initial Authentication Type**. If disable the function, you can authenticate by any credential that in the selected authentication type for the first authentication. If enable the function, you should follow the displayed sequence.
3. Click **Save**.

Manually Trigger Authentication via Face on PC Web

After enabling**Manually Trigger Authentication via Face**, you need to touch the screen of the device manually for face recognition.

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

When the main card reader is selected as the Terminal, click to enable **Manually Trigger Authentication via Face** and choose authentication mode.

Single Recognition

After completing the previous facial recognition, no matter successful or failed, you need to tap the screen to trigger the next recognition.

Continuous

After triggering the recognition, you can recognize via face until the device enter into the sleeping mode.

Click **Save**.

Enable Multiple People Authentication via PC Web

When enabled, multiple people can simultaneously verify faces for authentication.

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

When you select the terminal as main card reader, enable **Multiple People Authentication**, and 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**.

6.8.4 Authentication Linkage Settings

You can set authentication linkage settings.

Steps

1. Click **Access Control → Parameter Settings → Authentication Settings** to enter the settings page.
2. Set linkage functions.

   Link to Call If Authenticated

   If you enable this and person passes authentication, it will automatically call Button Settings's calling target to open door remotely.

Link to Call If Authentication Failed

After enabling, if authentication failed attempts reached the set number, it will automatically call Button Settings's calling target to open door remotely.

3. Click **Save**.

6.8.5 Set Authentication Plan

You can set authentication plan.

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

Select the authentication type and drag the time period in the time bar.

Click **Save**.

6.8.6 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.

Enable/Disable Face Duplicate Check

After enabling face duplicate check and everytime adding person's face, the system will check the face's duplication. If a duplicated face is detected, a prompt will be on.

Note

The function is not supported when add face remotely or applying face in batch.

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

Enable **Face Duplicate Check**.

Click **Save**.

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.

Set Fingerprint Parameters via PC Web

You can set the fingerprint parameters of the device.

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

Select **Fingerprint Security Level**. The higher the level, the lower the fake recognition rate and the higher the rejection rate.

Click **Save**.

Enable/Disable ECO Mode via PC Web

If the ECO mode is enabled, you can authenticate faces in the low light or dark environment with IR camera.

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

If the ECO mode is enabled, you can authenticate faces in the low light or dark environment with IR camera. You can set the ECO mode (1:N) and ECO mode (1:1).

If the face with mask detection is enabled, you can set face mask detection parameters also.

ECO Mode (1:1) Threshold

Set the matching threshold when authenticating via ECO mode 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.

ECO Mode (1:N) Threshold

Set the matching threshold when authenticating via ECO mode 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 with Mask 1:1 Match Threshold (ECO)

Set the matching threshold when authenticating with face mask via ECO mode 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 1:N Match Threshold (ECO)

Set the matching threshold when authenticating with face mask via ECO mode 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**.

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:N Match Threshold (ECO)**, **Face with Mask 1:1 Match Threshold** and **Face with Mask 1:N Match Threshold (ECO)**.

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.

Face with Mask 1:1 Match Threshold (ECO)

Set the matching value when authenticating with face mask via ECO mode 1:1 matching mode. The larger the threshold, the lower the recognition error rate and the higher the rejection rate when authenticating faces. The maximum value is 100.

Face with Mask 1:N Match Threshold (ECO)

Set the matching value when authenticating with face mask via ECO mode 1:N matching mode. The larger the threshold, the lower the recognition error rate and the higher the rejection rate when authenticating faces. The maximum value is 100.

Click **Save**.

6.8.7 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.

Enable/Disable CPU Card via Web Client

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

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

Click to **Enable CPU Card**.

Click to **Enable CPU Card Read Content**. After enabling, the device can read content from CPU card.

Click **Save**.

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.

6.8.8 Set Remote Verification

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

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

Click**Save** after parameters are configured.

Remote Verification

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

Verifying Person Type Remotely

Select **Verifying Person Type Remotely**.

Verify Credential Locally

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

Timeout Duration of Remote Verification

Set Timeout Duration of Remote Verification.

Offline Remote Verifying Unlocking

You can enable **Offline Remote Verifying Unlocking**.

Result Return Mode

Set **Result Return Mode**.

6.8.9 Privacy Settings

Set Event Storage Type via PC Web Browser

You can configure the event storage type.

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

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

Delete Old Events Periodically

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

Delete Old Events by Specified Time

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

Overwriting

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

Click **Save**.

Set 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.

You can select **Authentication Result Profile Photo** according to your actual needs.

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

Upload Captured Picture During Call

If enabled, pictures will be captured automatically during calls and will be uploaded automatically.

Click **Save**.

Clear Device Pictures via PC Web

You can clear all registered, authenticated or captured face or pictures.

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

Click **Clear** to clear all registered, authenticated, captured face pictures or palm print pictures.

Set PIN Mode via PC Web

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

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

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

Platform-Applied Personal PIN

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

Device-Set Personal PIN

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

Click **Save**.

6.8.10 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 **Video Intercom → Call Settings → Device No.** .

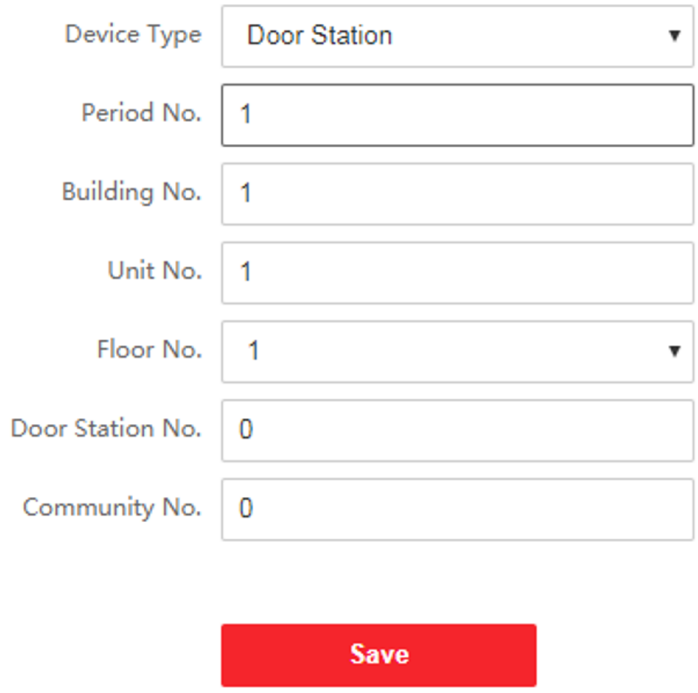


Figure 6-1 Device No. Settings

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 **Video Intercom → 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.

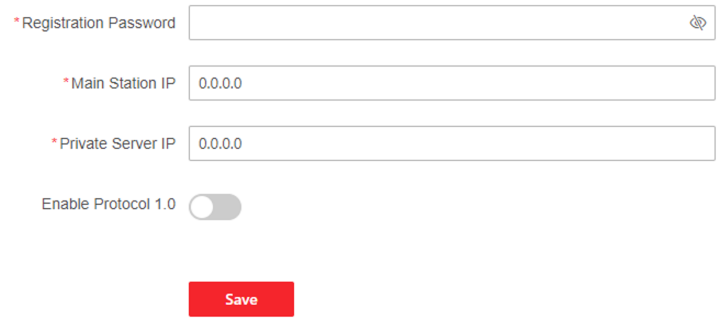


Figure 6-2 Video Intercom Network

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 **Video Intercom → Call Settings → Call Settings** .

Enter the **Max. Communication Time**. You can enable **Auto Answer**.

Note

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

Click **Save**.

Press Button to Call via PC Web

Steps

1. Click **Access Control → Call Settings → Press Button to Call** to enter the settings page.

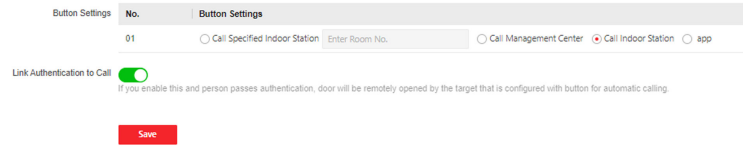


Figure 6-3 Press Button to Call

2. Select **Call Specified Indoor Station**, **Call Management Center**, **Call Indoor Station** or **APP** at your needs.

Note

If you select **Call Specified Indoor Station**, you need to enter the **Room No.** of the indoor station.

3. Enable **Link Authentication to Call** according to your needs. After enabled, when person passes authentication, the door will be remotely opened by the target that is configured with button for automatic calling.
4. Click **Save**.

Call Priority

You can set call priority.

Steps

1. Click **Video Intercom → Call Settings → Call Priority** to enter the settings page.
2. Check the **Call Type** and set the **Ring Duration** of each 3 priorities.
3. Click **Save** to enable the settings.

Note

The higher the level, the easier the device to be called. After the call time is over, the next level of call is triggered.

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.

6.9 Device Management

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

Steps

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

Delete Device	Check devices need to delete, and click **Delete**.
Import Device	Plug the USB flash drive (containing device information) to the device, click **Import** to import the device information.
Export Device	Click **Export** to export the device information files to the USB flash drive.

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, local RS-485 number, 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, local RS-485 number, 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** .

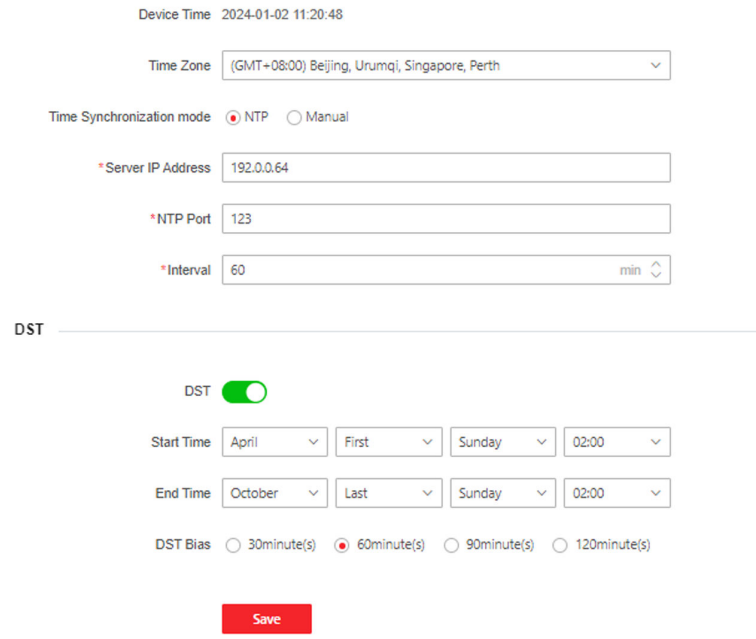


Figure 6-5 Time Settings

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 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.

6.10.7 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** .

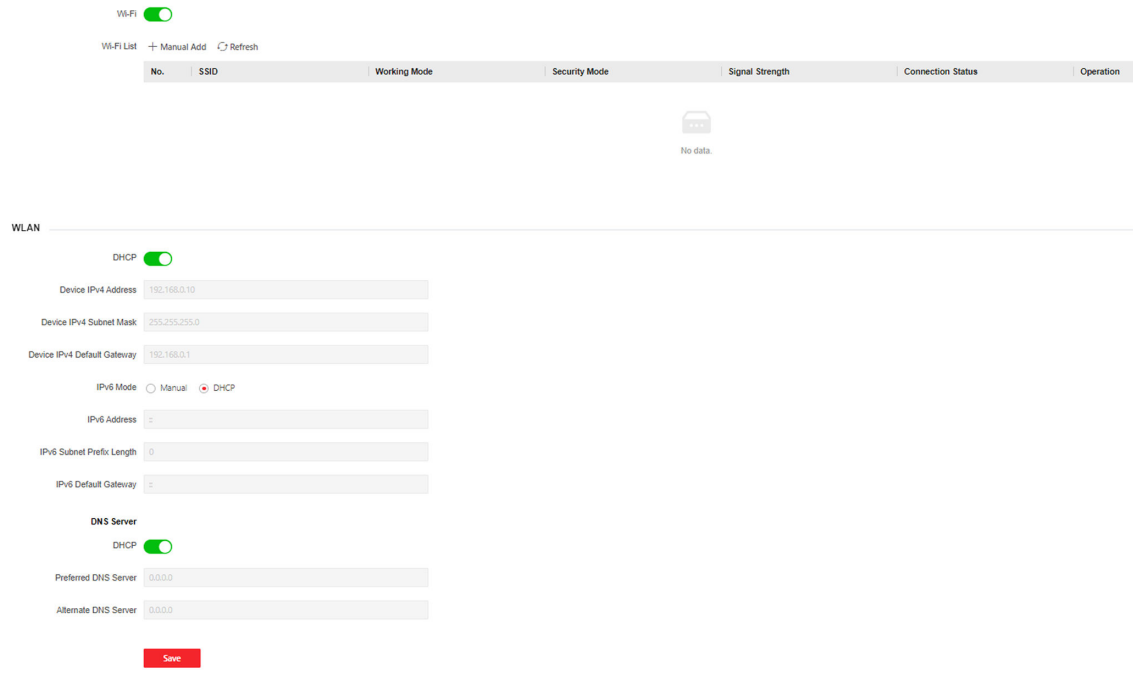


Figure 6-6 Wi-Fi Settings Page

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 Mobile Data

Set the mobile data parameters for the device.

Note

If the wi-fi function is enabled, the 3G/4G function cannot be used.

Click **System and Maintenance → Network → Network Settings → Mobile Data** .

Enable 3G/4G

If the device supports 3G/4G communication function, you can enable it.

Dialing Mode/Dialing No.

Select the dialing mode as **Manual**. And set the dialing No.

User Name/Password/APN/PIN

If you need, you can set the user name, password, APN, and PIN for mobile number.

Enable/Disable Bluetooth via PC Web

You can enable device bluetooth to connect a bluetooth sound.

Steps

1. Click **Access Control → System Configuration → Network → Network Settings → Bluetooth** to enter the settings page.
2. In the bluetooth parameter configuration section, enable **Open**.
3. Enter the external sound in the **Device Name**. After the bluetooth is connected, 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**.

Set OTAP via PC Web

Connect the device to the platform through the OTAP protocol to obtain device information, upload operation status and alarm information, restart and upgrade the device.

Steps

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

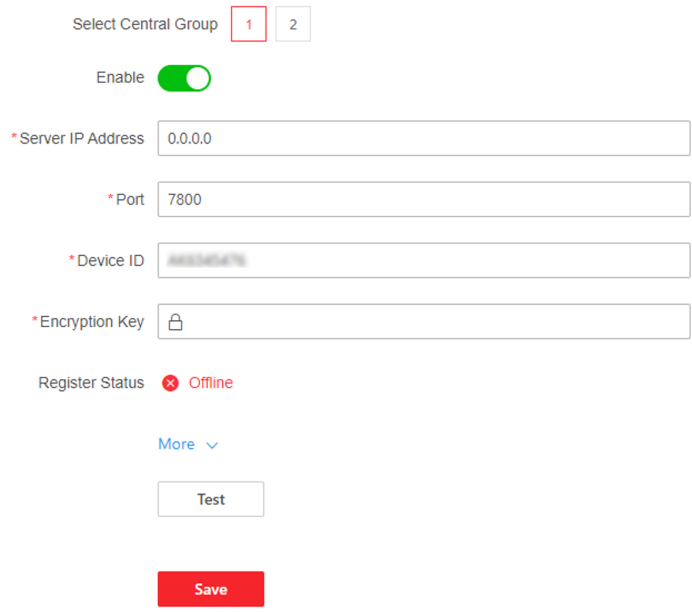


Figure 6-7 Set OTAP

2. Click to **Enable** OTAP.
3. Set **Server IP Address**, **Port**, **Device ID** and **Encryption Key**.
4. Click **Test** to ensure the device can connect to the server and register successfully. Refresh the page or restart the device to see the **Register Status**.
5. Click **More** to view the network type and access priority. Drag the operation icon upward or downward to adjust the network priority.
6. 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. Select **Call Type**, and select VoIP.
3. Enable **VoIP Gateway**.
4. Set **Register User Name**、**Registration Password**、**Server IP Address**、**Server Port**、**Expiry Time**、**Register Status**、**Number**、**Display User Name.** and **Center No.**
5. Click **Save**.

6.10.8 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 Web Browser

You can set device volume.

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

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

Slide to enable voice prompt function.

You can enable **Audio Mixing**, and set **Output Sub-Volume**.

Select **SIP Audio Encoding**.

Click **Save**.

6.10.9 Image Parameter Settings

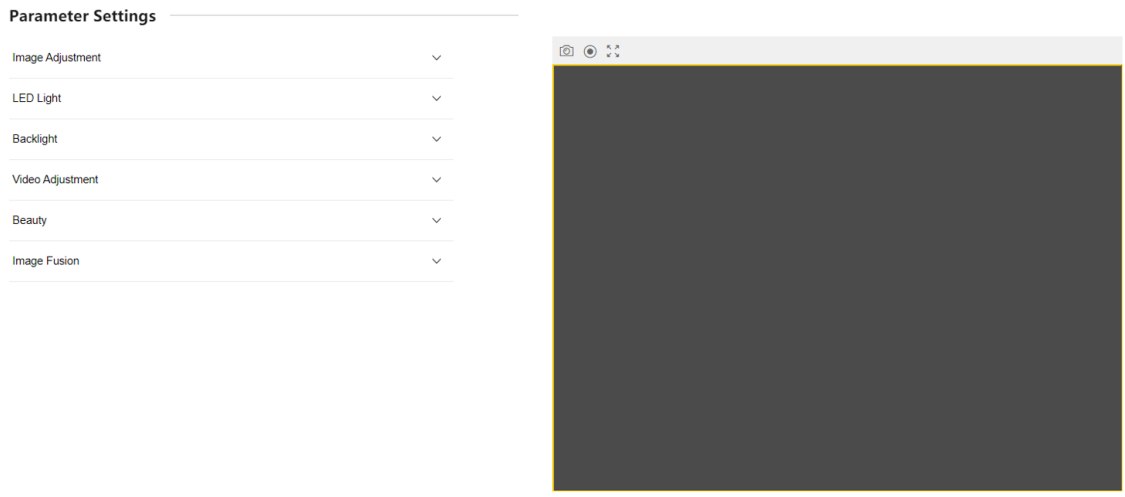


Figure 6-8 Display Settings

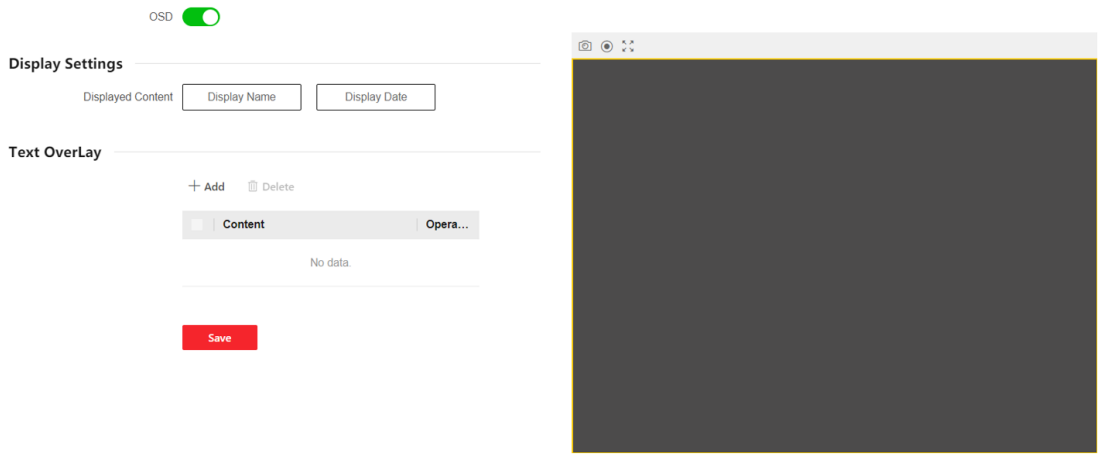


Figure 6-9 OSD Settings

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.

6.10.10 Alarm Settings via PC Web

Set the alarm output parameters.

Steps

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

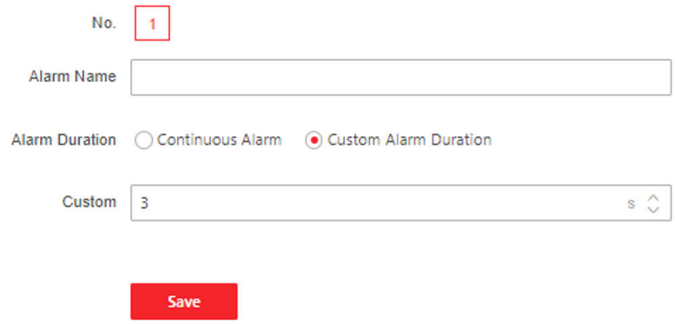


Figure 6-10 Alarm Settings

Continuous Alarm

When the alarm is triggered, it will alarm continuously.

Custom Alarm Duration

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

6.10.11 Linkage Settings

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

Steps

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

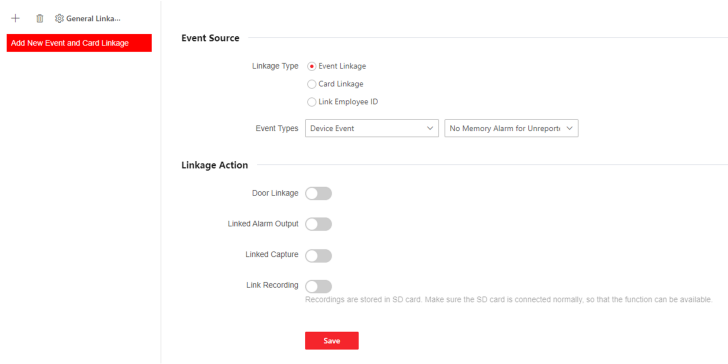


Figure 6-11 Linkage Settings

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

   Note

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

6.10.12 Access Configuration

Set RS-485 Parameters via PC Web

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

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

Select **RS-485 Protocol**.

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

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

No.

Set the RS-485 No.

Peripheral Type

Select a peripheral from the drop-down list according the actual situation.

Note

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

RS-485 Address

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

Note

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

Baud Rate

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

Set Wiegand Parameters via PC Web

You can set the Wiegand transmission direction.

Steps

Note

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

1. Click **System and Maintenance → System Configuration → Access Configuration → Wiegand Settings** .

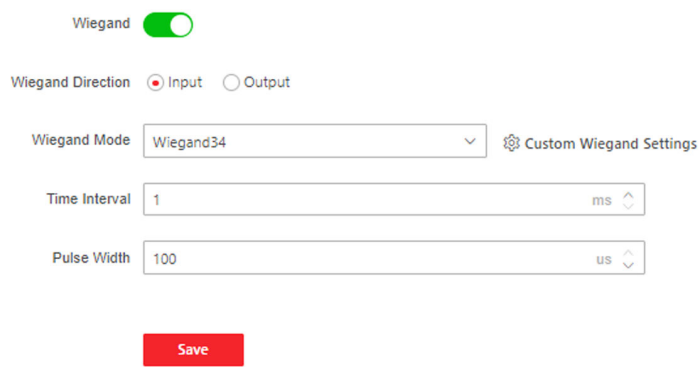


Figure 6-12 Wiegand Page

2. Check **Wiegand** to enable the Wiegand function.

3. Set a transmission direction.

Input

The device can connect a Wiegand card reader.

Output

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

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

Note

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

Elevator Control via Web

Steps

1. Click **System and Maintenance → System Configuration → Elevator Control** .

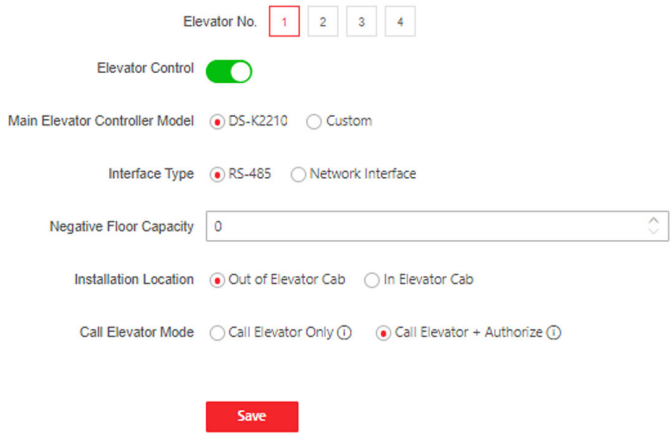


Figure 6-13 Elevator Control

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

Main Elevator Controller Model

Select an elevator No. for configuration.

Interface Type

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

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

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

Negative Floor Capacity

Set the negative floor number.

Installation Location

Select installation location as **Out of Elevator Cab** or **In Elevator Cab**.

Call Elevator Mode

Select call elevator mode.

Call Elevator Only

After the person passes authentication, the device will call elevator to its floor.

Call Elevator + Authorize

After the person passes authentication, the device will call elevator to its floor and authorize the permission of the floor linked to the person's room. The person can get to the target floor by pressing corresponding floor No.

Note

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

6.11 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.

6.11.1 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.

6.11.2 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.

6.11.3 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.

6.11.4 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.

6.12 Preference Settings

6.12.1 Set Startup Image via PC Web

Set startup image.

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

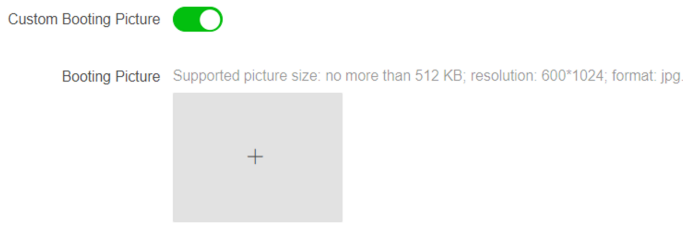


Figure 6-14 Startup Image

Enable **Custom Booting Picture**, click **+** and select a booting picture from local browse.

Note

Supported picture size: no more than 512 KB; resolution: 600*1024; format: jpg.

Click **Save**.

6.12.2 Set Standby Image via PC Web

Set the standby image parameters, including the time to enter standby, screen saver picture, displayed effect, and slide show interval.

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

Time to Enter Standby

The device will show the standby image after the configured time duration.

Advertisement Allowed as Screen Saver

you can enable **Advertisement Allowed as Screen Saver**, and customize content in PC WEB **Preference → Notice Publication** .

6.12.3 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 6-15 Sleep Settings

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

Click **Save**.

6.12.4 Customize Authentication Desk via PC Web

Customize the modules on the authentication page/desk.

Steps

1. Go to **System and Maintenance → Preference → Custom Home Page** .
2. Select **Application Mode**.

   Business Scene

   Highlight the released information. Not display authentication page. Applicable to scenes where information display is the primary focus.

   Professional Scene

   Supports multi-factor authentication and one-tap emergency calling, designed for high-security access control scenes.

   Community Scene

   Supports intercom calls and PIN entry. Authorized person can unlock directly via authentication. Applicable to building community and neighborhood scenes.

   Enterprise Scene

   Supports face and card authentication. Applicable to enterprise office entrance/exit rapid door access and attendance scenes.

   Office Scene

   Displays doorplate information, personnel work status, and room usage status. Applicable to enterprise office scenes.
3. Click **Apply**.

6.12.5 Set Notice Publication via PC Web

You can set the notice publication for the device.

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

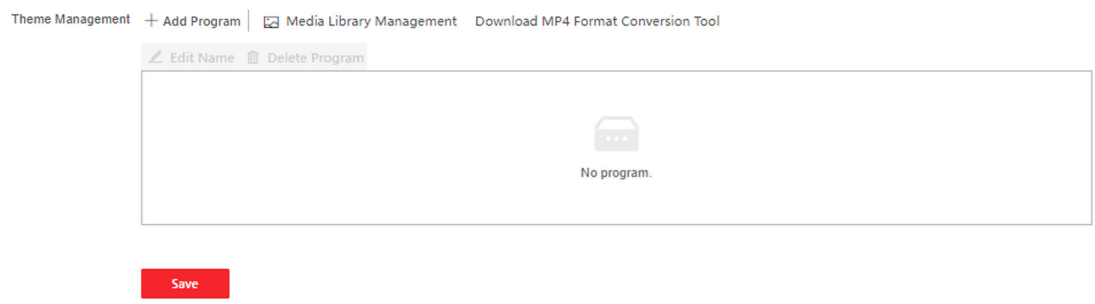


Figure 6-16 Notice Publication

Download MP4 Format Conversion Tool

You can click **Download MP4 Format Conversion Tool** if you need to change the format.

Material Management

You can click **+ Add Theme**, and set **Theme Name** and **Theme Type**.

Click **Upload**, and click **+** to upload the picture or video from the local PC.

Note

By now, there is only one theme can be added.

Add Program

You can set the program name and select program type.

Picture

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

Welcome Message

If you select welcome message, you can set the template, content, font size and color of main and sub title. You can also custom the background picture.

Standard

If you select standard, you can set the background color and picture.

Play Schedule

After you have created a theme, you can select the theme and draw a schedule on the time line.

Select the drawn schedule, and you can edit the exact start and end time.

Select the drawn schedule and you can click **Delete** or **Delete All** to delete the schedule.

Slide Show Interval

Drag the block or enter the number to set the slide show interval. The picture and video will be changed according to the interval.

6.12.6 Set Prompt Schedule via PC Web

Customize the output audio content when authentication succeeded and failed.

Steps

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

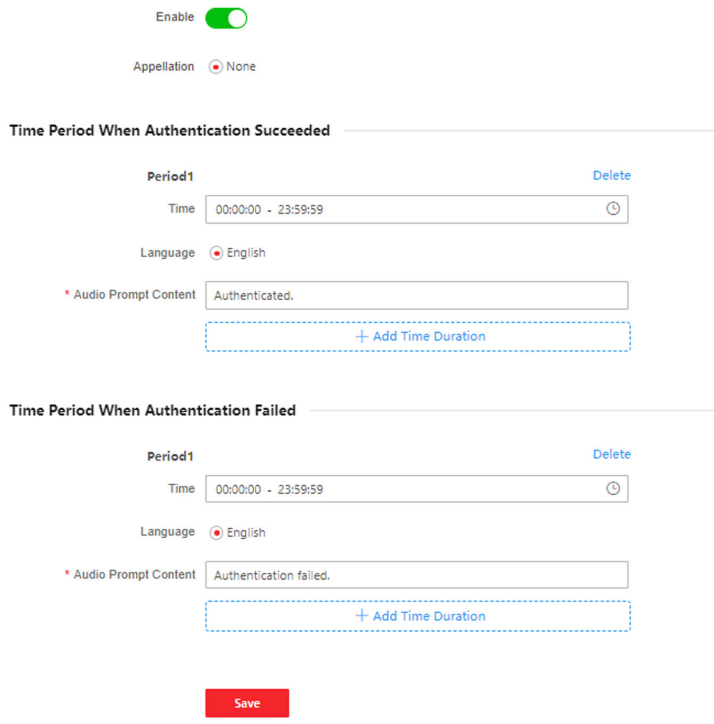


Figure 6-17 Prompt Schedule

2. Enable the function.
3. Set the appellation.
4. Select time schedule.
5. Set the time period when authentication succeeded.
   1) Click **Add Time Duration**.
   2) Set the time duration.

   Note

   If authentication is succeeded in the configured time duration, the device will broadcast the configured content.
   3) Set the audio prompt content.
   4) **Optional:** Repeat substep 1 to 3.
   5) **Optional:** Click to delete the configured time duration.
6. Set the time duration when authentication failed.

1) Click **Add Time Duration**.
2) Set the time duration.

Note

If authentication is failed in the configured time duration, the device will broadcast the configured content.

3) Set the audio content.
4) **Optional:** Repeat substep 1 to 3.
5) **Optional:** Click to delete the configured time duration.

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

6.12.7 Customize Prompt Voice via PC Web

You can customize prompt voices for the device.

Steps

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

Custom Type	Importing Status	Operation
Call Center	Not Imported	
Nobody Answered	Not Imported	
Thanks	Not Imported	
Authenticating Failed	Not Imported	
The Door Is Open	Not Imported	
Please Wear the Safety Helmet	Not Imported	
Please Wear the Mask	Not Imported	

Figure 6-18 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.

6.12.8 Set Authentication Result Text via PC Web

Steps

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

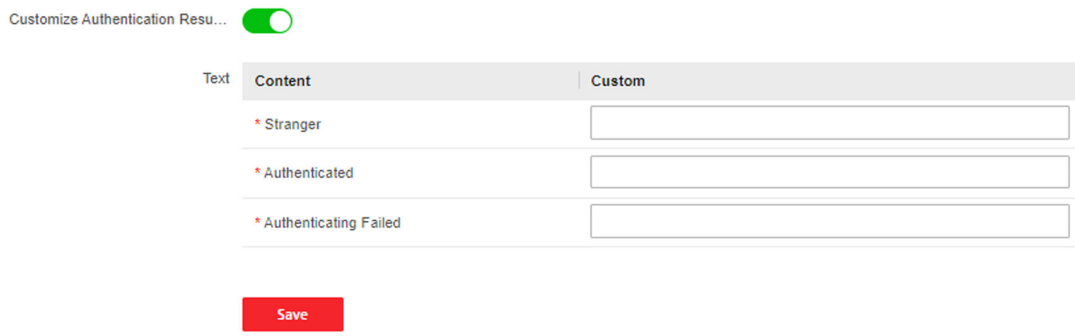


Figure 6-19 Authentication Result Text

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

6.12.9 Doorplate Settings

You can set doorplate parameters.

Steps

1. Tap **Preference → Custom Home Page** to enter the preference settings page.
2. You can set Basic Doorplate Settings and Office Status Settings information according to your needs.
3. Click **Save**.

6.13 System and Maintenance

6.13.1 Reboot

You can reboot the device.

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

Click **Restart** to reboot the device.

6.13.2 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.

Upgrade Keyfob

Note

- Make sure that the peripheral module is online.
- When upgrading the keyfob, keep only one face recognition terminal around and don't move the keyfob.

Click **System and Maintenance → Maintenance → Upgrade** . In the Upgrade Settings drop-down list, select **Keyfob**. Select the upgrade file from your local PC. Click **Upgrade → OK** . Press any button of the keyfob to upgrade.

6.13.3 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.

6.13.4 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.

6.13.5 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**.

6.13.6 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** .

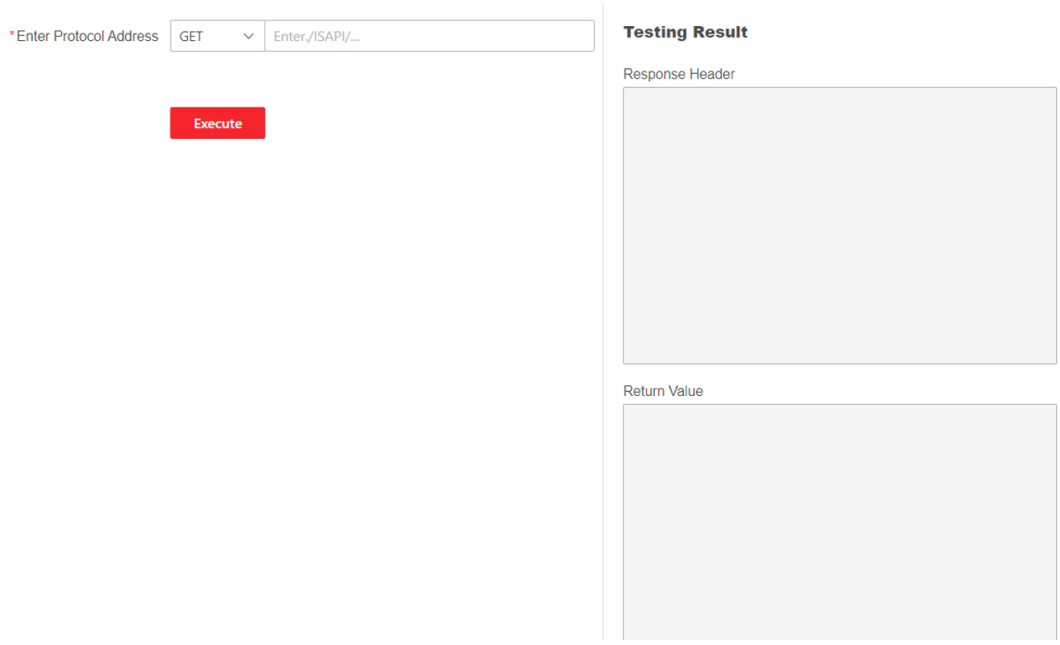


Figure 6-20 Protocol Testing

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** .

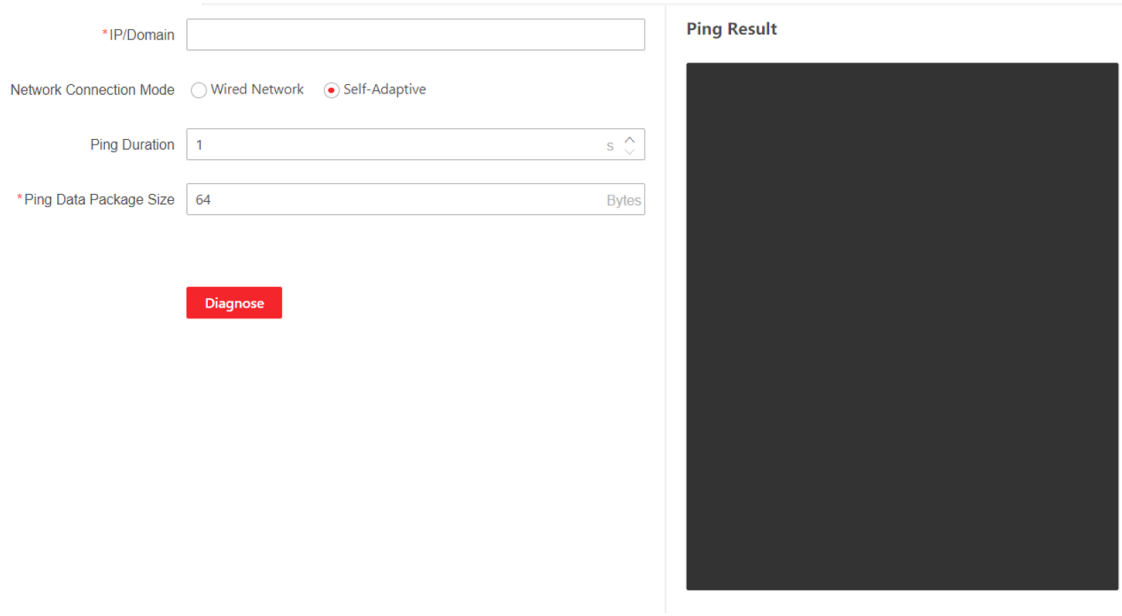


Figure 6-21 Network Diagnosis

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.

6.13.7 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.

6.13.8 Advanced Settings via PC Web

You can configure face 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**, **Anti-Spoofing Detection Threshold 1:N of Face with Mask**.

Enable **Lock Face for Anti-Spoofing Protection**, 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.

6.13.9 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**.

6.13.10 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 an asking file in the local computer.
7. Send the asking file to a certification authority for signature.
8. Import the signed certificate.
   1) Select a certificate type in the **Import Key** area, and select a certificate from the local, and click **Import**.
   2) Select a certificate type in the **Import Communication Certificate** area, and select a certificate from the local, and click **Import**.

Import Other Authorized Certificate

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

Steps

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

Import CA Certificate

Before You Start

Prepare a CA certificate in advance.

Steps

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

Note

The input certificate ID cannot be the same as the existing ones.

3. Upload a certificate file from the local.
4. Click **Import**.

Chapter 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/59d800fb

HikCentral Access Control (HCAC)

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

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

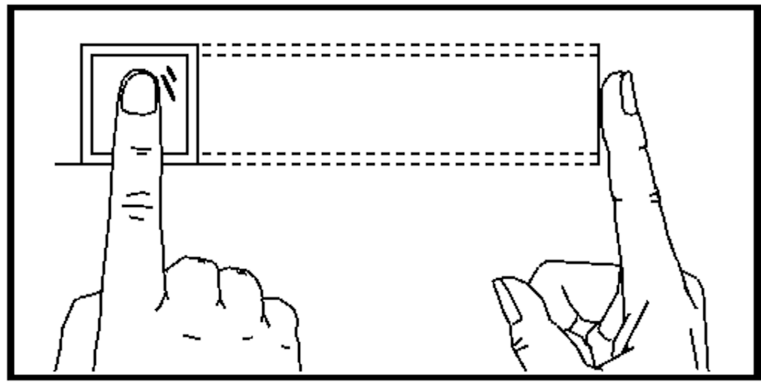
Appendix A. Tips for Scanning Fingerprint

Recommended Finger

Forefinger, middle finger or the third finger.

Correct Scanning

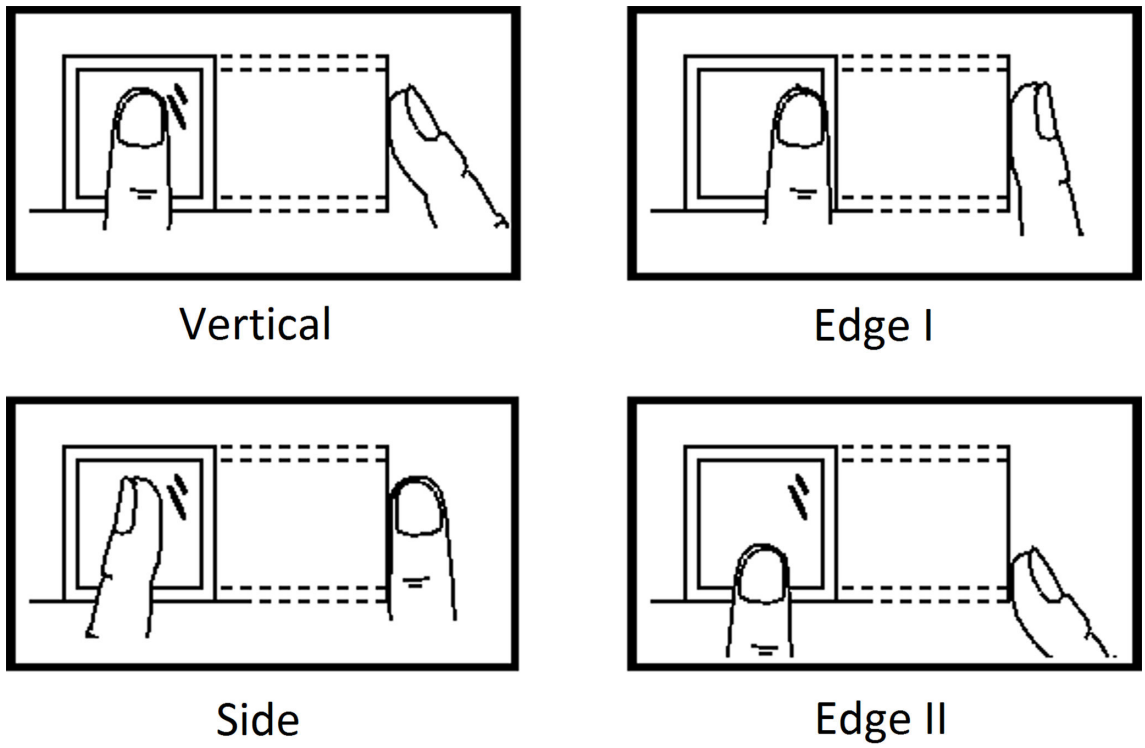
The figure displayed below is the correct way to scan your finger:



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.

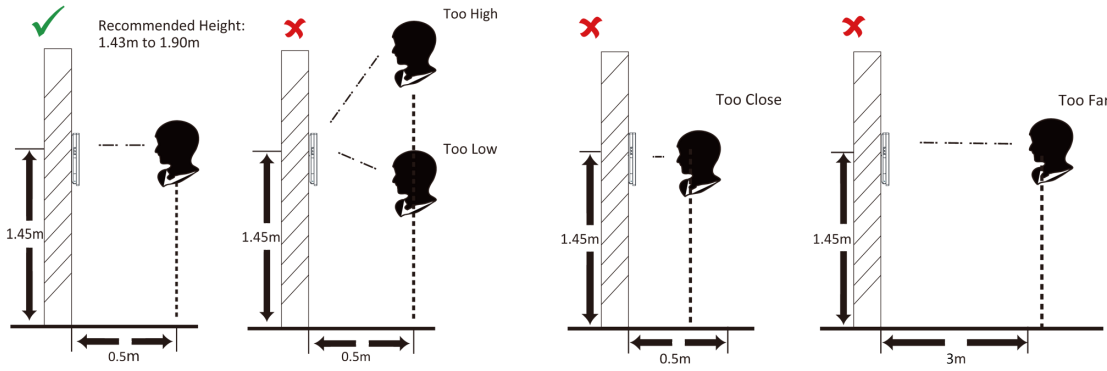
Others

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 B. Tips When Collecting/Comparing Face Picture

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

Positions (Recommended Distance: 0.5 m)



Expression

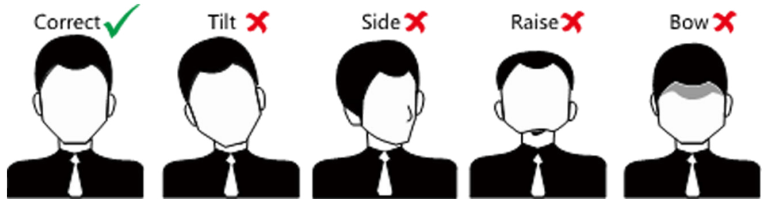
- Keep your expression naturally when collecting or comparing face pictures, just like the expression in the picture below.



- 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.

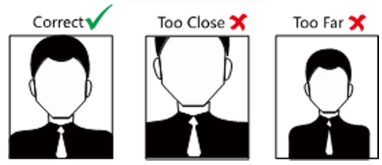
Posture

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 C. Tips for Installation Environment

1. Light Source Illumination Reference Value



Candle: 10Lux

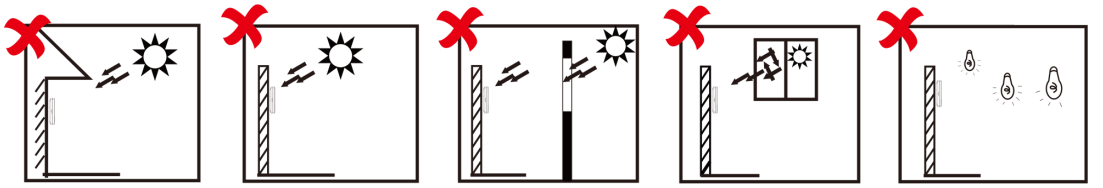


Bulb: 100~850Lux



Sunlight: More than 1200Lux

2. Avoid backlight, direct and indirect sunlight



Appendix D. 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.


See Far, Go Further