



DS-K1T331 Series Face Recognition Terminal

User Manual

Legal Information

©2023 Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

About this Manual

The Manual 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 Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of this Manual at the Hikvision website (<https://www.hikvision.com/>).

Please use this Manual with the guidance and assistance of professionals trained in supporting the Product.

Trademarks

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.

Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS MANUAL 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 MANUAL AND THE APPLICABLE LAW, THE LATTER PREVAILS.

Data Protection

During the use of device, personal data will be collected, stored and processed. To protect data, the development of Hikvision devices incorporates privacy by design principles. For example, for device with facial recognition features, biometrics data is stored in your device with encryption method; for fingerprint device, only fingerprint template will be saved, which is impossible to reconstruct a fingerprint image.

As data controller, you are advised to collect, store, process and transfer data in accordance with the applicable data protection laws and regulations, including without limitation, conducting security controls to safeguard personal data, such as, implementing reasonable administrative and physical security controls, conduct periodic reviews and assessments of the effectiveness of your security controls.

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



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

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



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



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



Safety Instruction

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

The precaution measure is divided into Dangers and Cautions:

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

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

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

Danger:

- All the electronic operation should be strictly compliance with the electrical safety regulations, fire prevention regulations and other related regulations in your local region.
- 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.
- 1. Risk of explosion if the battery is replaced by an incorrect type
 2. Improper replacement of the battery with an incorrect type may defeat a safeguard (for example, in the case of some lithium battery types).
 3. This equipment is not suitable for use in locations where children are likely to be present.
 4. Do not dispose of the battery into fire or a hot oven, or mechanically crush or cut the battery, which may result in an explosion.
 5. Do not leave the battery in an extremely high temperature surrounding environment, which may result in an explosion or the leakage of flammable liquid or gas.
 6. Do not subject the battery to extremely low air pressure, which may result in an explosion or the leakage of flammable liquid or gas.
 7. Dispose of used batteries according to the instructions
- If the product does not work properly, please contact your dealer or the nearest service center. Never attempt to disassemble the device yourself. (We shall not assume any responsibility for problems caused by unauthorized repair or maintenance.)

Cautions:

- Do not drop the device or subject it to physical shock, and do not expose it to high electromagnetism radiation. Avoid the equipment installation on vibrations surface or places subject to shock (ignorance can cause equipment damage).
- Do not place the device in extremely hot (refer to the specification of the device for the detailed operating temperature), cold, dusty or damp locations, and do not expose it to high electromagnetic radiation.
- The device cover for indoor use shall be kept from rain and moisture.
- Exposing the equipment to direct sun light, low ventilation or heat source such as heater or radiator is forbidden (ignorance can cause fire danger).
- Do not aim the device at the sun or extra bright places. A blooming or smear may occur otherwise (which is not a malfunction however), and affecting the endurance of sensor at the same time.
- Please use the provided glove when open up the device cover, avoid direct contact with the device cover, because the acidic sweat of the fingers may erode the surface coating of the device cover.
- Please use a soft and dry cloth when clean inside and outside surfaces of the device cover, do not use alkaline detergents.
- Please keep all wrappers after unpack them for future use. In case of any failure occurred, you need to return the device to the factory with the original wrapper. Transportation without the original wrapper may result in damage on the device and lead to additional costs.
- Improper use or replacement of the battery may result in hazard of explosion. Replace with the same or equivalent type only. Dispose of used batteries according to the instructions provided by the battery manufacturer.
- Biometric recognition products are not completely applicable to anti-spoofing environments. If you require a higher security level, use multiple authentication modes.
- Input voltage should meet both the SELV (Safety Extra Low Voltage) and the Limited Power Source with 100~240 VAC or 12 VDC according to the IEC60950-1 standard. Please refer to technical specifications for detailed information.

Contents

Chapter 1 Overview	1
1.1 Overview	1
1.2 Features	1
Chapter 2 Appearance	2
Chapter 3 Installation	3
3.1 Installation Environment	3
3.2 Base Mounting	3
3.3 Install with Gang Box	4
Chapter 4 Wiring	10
4.1 Terminal Description	10
4.2 Wire Normal Device	11
4.3 Wiring with Power Cable	12
Chapter 5 Activation	13
5.1 Activate via Device	13
5.2 Activate via Web Browser	14
5.3 Activate via SADP	14
5.4 Activate Device via iVMS-4200 Client Software	16
Chapter 6 Quick Operation	17
6.1 Select Language	17
6.2 Set Password Change Type	17
6.3 Set Network Parameters	18
6.4 Access to Platform	19
6.5 Remote Operation via APP	20
6.6 Privacy Settings	21
6.7 Set Administrator	22
Chapter 7 Basic Operation	24

7.1 Login	24
7.1.1 Login by Administrator	24
7.1.2 Login by Activation Password	25
7.1.3 Forgot Password	26
7.2 Communication Settings	28
7.2.1 Set Wired Network Parameters	28
7.2.2 Set Wi-Fi Parameters	29
7.2.3 Set RS-485 Parameters	30
7.2.4 Set ISUP Parameters	31
7.2.5 Platform Access	32
7.3 User Management	33
7.3.1 Add Administrator	33
7.3.2 Add Face Picture	35
7.3.3 Add Card	37
7.3.4 View PIN code	38
7.3.5 Set Authentication Mode	38
7.3.6 Search and Edit User	39
7.4 Data Management	39
7.4.1 Delete Data	39
7.4.2 Import Data	40
7.4.3 Export Data	40
7.5 Authenticate via Face	41
7.6 Basic Settings	41
7.7 Set Biometric Parameters	42
7.8 Set Access Control Parameters	44
7.9 Time and Attendance Status Settings	46
7.9.1 Disable Attendance Mode via Device	46
7.9.2 Set Manual Attendance via Device	47

7.9.3 Set Auto Attendance via Device	48
7.9.4 Set Manual and Auto Attendance via Device	50
7.10 System Maintenance	51
7.11 Preference Settings	53
Chapter 8 Quick Operation via Web Browser	55
8.1 Select Language	55
8.2 Time Settings	55
8.3 Privacy Settings	55
8.4 Administrator Settings	56
Chapter 9 Operation via Web Browser	57
9.1 Login	57
9.2 Forgot Password	57
9.3 Live View	57
9.4 Person Management	59
9.5 Search Event	60
9.6 Configuration	60
9.6.1 View Device Information	60
9.6.2 Set Time	60
9.6.3 Set DST	61
9.6.4 Change Administrator's Password	61
9.6.5 View Device Arming/Disarming Information	61
9.6.6 Network Settings	61
9.6.7 Set Video and Audio Parameters	64
9.6.8 Set Image Parameters	65
9.6.9 Access Control Settings	66
9.6.10 Card Settings	69
9.6.11 Time and Attendance Status Settings	70
9.6.12 Set Privacy Parameters	72

9.6.13 Set Biometric Parameters	73
9.6.14 Preference Settings	75
9.6.15 Upgrade and Maintenance	77
9.6.16 Device Debugging	79
9.6.17 Log Query	80
9.6.18 Security Mode Settings	80
9.6.19 Certificate Management	80
Chapter 10 Other Platforms to Configure	82
Appendix A. Tips When Collecting/Comparing Face Picture	83
Appendix B. Tips for Installation Environment	85
Appendix C. Dimension	86
Appendix D. Communication Matrix and Device Command	87

Chapter 1 Overview

1.1 Overview

Face recognition terminal is a kind of access control device for face recognition, which is mainly applied in security access control systems, such as logistic centers, airports, university campuses, alarm centrals, dwellings, etc.

1.2 Features

- 3.97-inch LCD touch screen
- 2 MP wide-angle dual-lens
- Face anti-spoofing
- Face recognition distance: 0.3 m to 1.5 m
- Suggested height for face recognition: between 1.4 m and 1.9 m
- Deep learning algorithm
- 1000 face capacity, 1500 card capacity (when connecting external card reader), 150,000 event capacity, and 20,000 captured pictures storage
- Face recognition duration < 0.2 s/User; face recognition accuracy rate $\geq 99\%$
- Capture linkage and captured pictures storage
- Transmits card and user data from or to the client software via TCP/IP protocol and saves the data on the client software
- Imports pictures from the USB flash drive to the device or export pictures, events, from the device to the USB flash drive
- Stand-alone operation
- Manage, search and set device data after logging in the device locally
- Connects to one external card reader via RS-485 protocol
- Connects to secure door control unit via RS-485 protocol to avoid the door opening when the device is destroyed
- Audio prompt
- Watchdog design and tamper function
- Support English, Spanish (South America), Arabic, Thai, Indonesian, Russian, Vietnamese, Portuguese (Brazil)

Chapter 2 Appearance

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

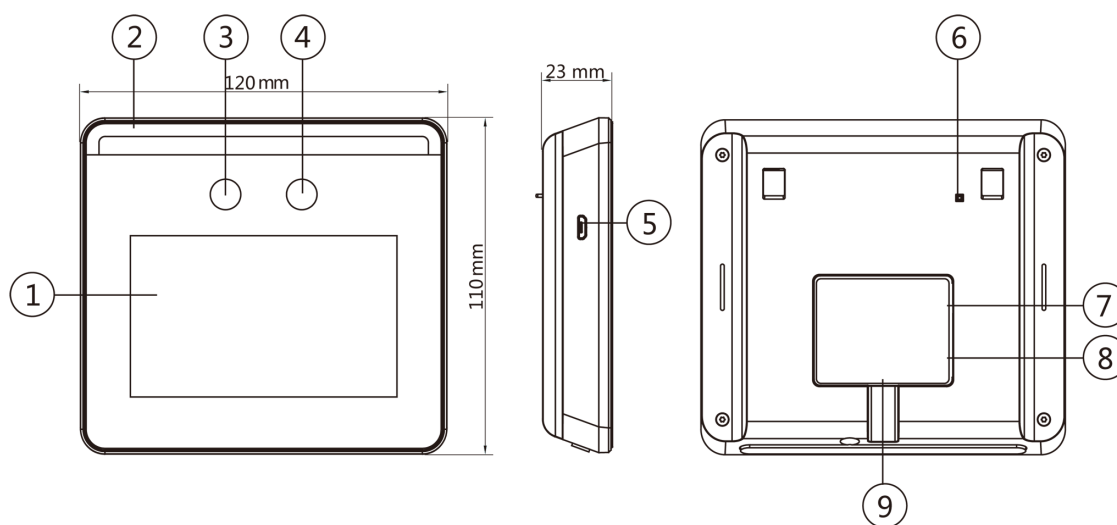


Figure 2-1 Face Recognition Terminal Diagram

Table 2-1 Description of Face Recognition Terminal

No.	Name	Description
1	Display Screen	3.97-inch LCD touch screen.
2	Supplement Light	Supplement light camera.
3	Camera 1	Recording or capturing videos or pictures.
4	Camera 2	Recording or capturing videos or pictures.
5	microUSB Interface	Connect to USB flash drive via a microUSB to USB cable.
6	Tamper	After installation, if the device is disassembled, a tamper alarm will be triggered.
7	Network Interface	Connect to Ethernet.
8	Wiring Terminals	Connect to other external devices, including RS-485 card reader, door lock, etc.
9	Debugging Port	The debug terminal is used for debugging only.

Chapter 3 Installation

3.1 Installation Environment

- Avoid backlight, direct sunlight, and indirect sunlight.
- For better recognition, there should be light source in or near the installation environment.
- The minimum bearing weight of the wall or other places should be 3 times heavier than the device weight.
- There shall be no strong reflective objects (such as glass doors/walls, stainless steel objects, acrylic and other glossy plastics, lacquer, ceramic tiles, etc.) within 1 m of the field of view of the device.
- Avoid device reflection.
- Face recognition distance shall be greater than 30 cm.
- Keep the camera clean.



For details about installation environment, see *Tips for Installation Environment*.

3.2 Base Mounting

Place the device on the desk or other flats by using the mounting bracket.

Steps

1. Route the cables through the cable hole of the bracket, and connect the terminals with external devices' cables.
2. Align the device two holes with the two buckles on the bracket.
3. Hang the device on the bracket and make sure the buckle in the middle of the bracket is inserted in the groove on the device back.

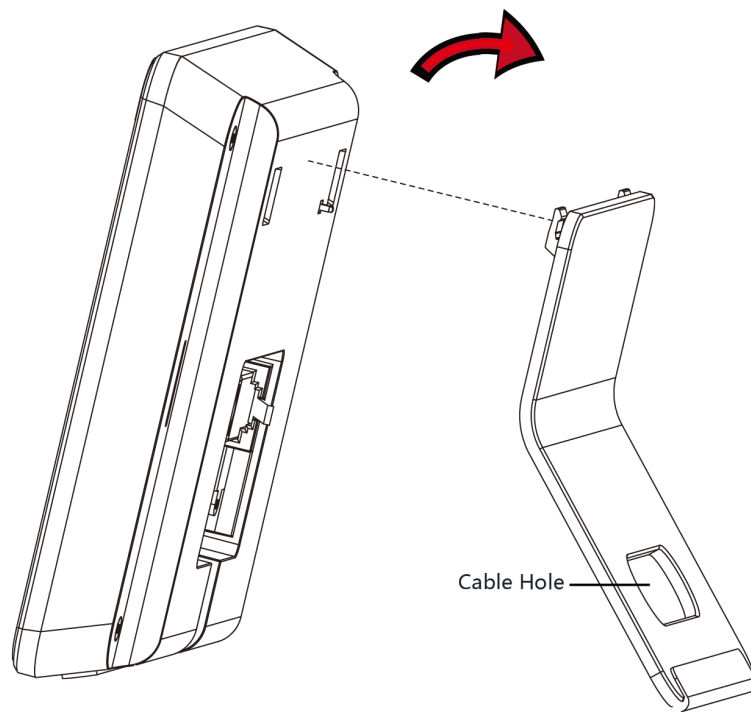


Figure 3-1 Base Mounting

4. Place the assembled device and bracket on the desk or other flats.

3.3 Install with Gang Box

Steps

1. According to the datum line on the mounting template, stick the mounting template on the wall or other surface, 1.45 meters higher than the ground.

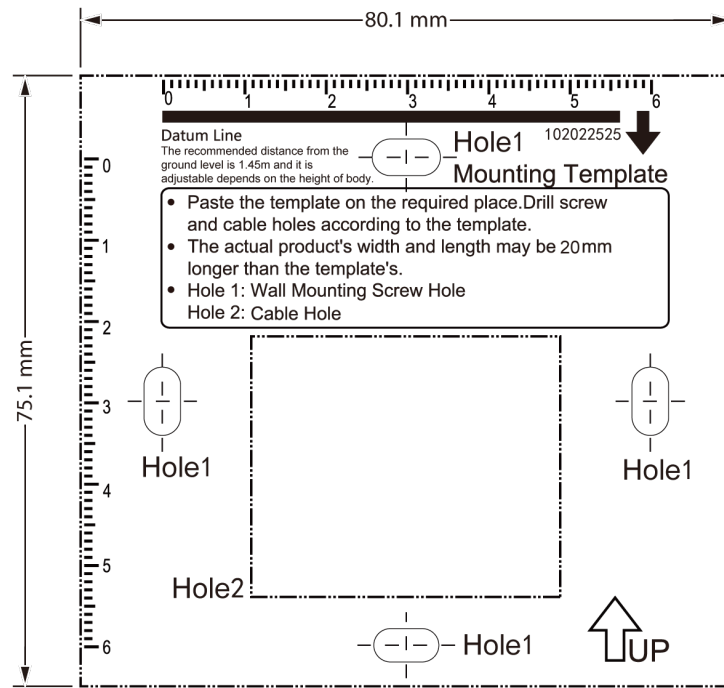


Figure 3-2 Mounting Template

2. Drill holes on the wall or other surface according to the mounting template and install the gang box.

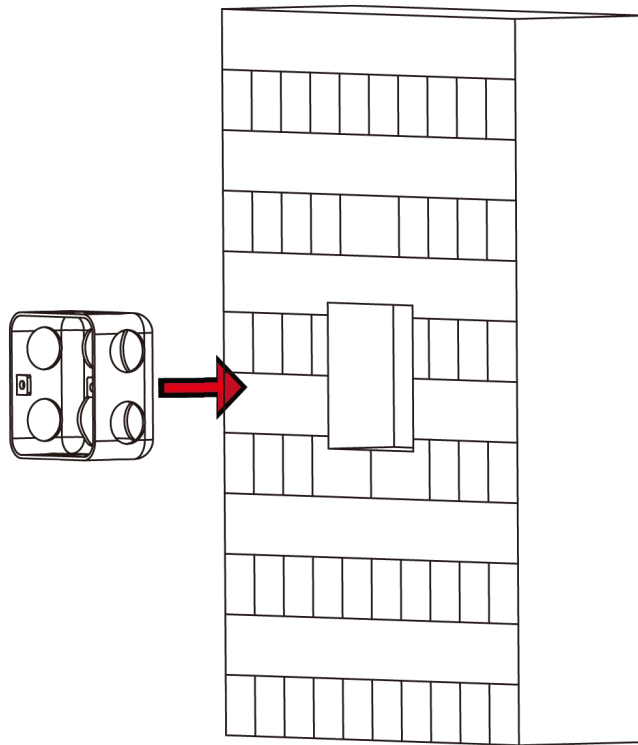


Figure 3-3 Install Gang Box

- 3.** Use two supplied screws (SC-KM4x25-SUS or KA4x22-SUS) to secure the mounting plate on the gang box.

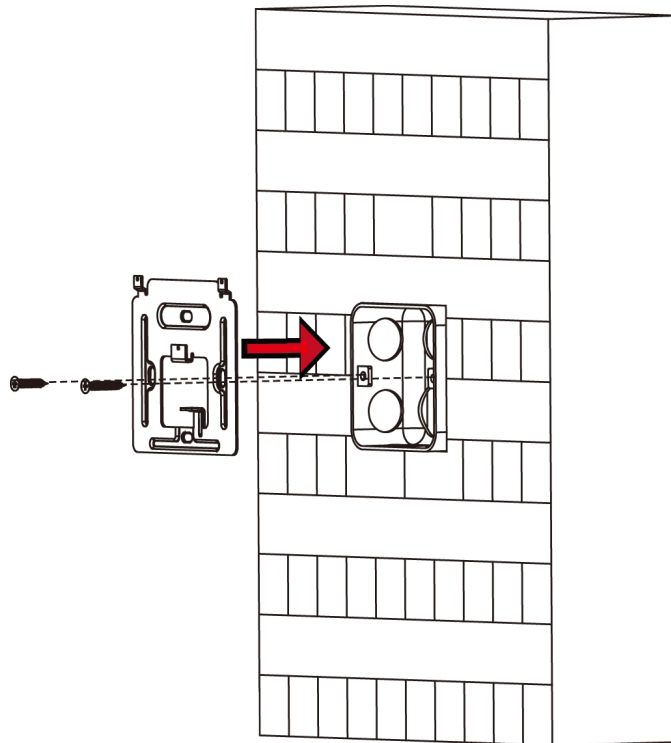


Figure 3-4 Install Mounting Plate

4. Route the cables through the cable hole of the mounting plate, and connect the terminals with the external devices' cables.
5. Align the device with the mounting plate and hang the device on the mounting plate.

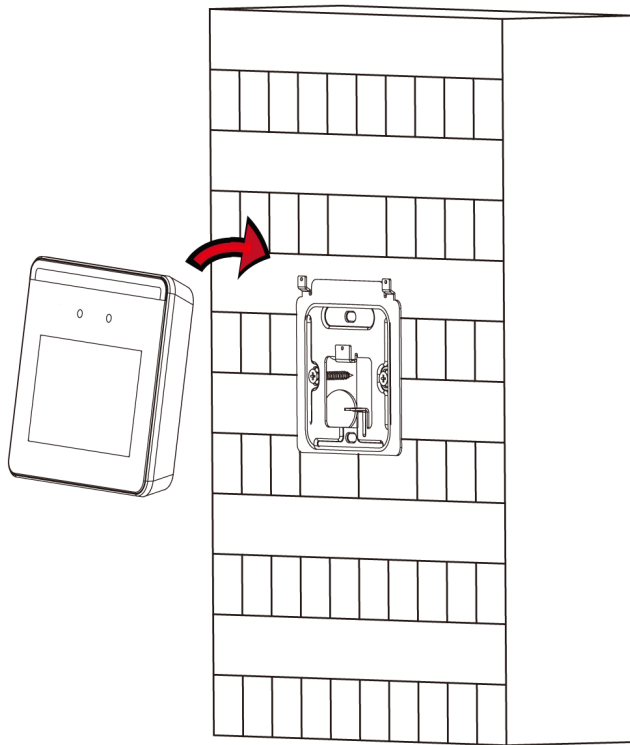


Figure 3-5 Install Device

6. Use one supplied screw to secure the device and the mounting plate.

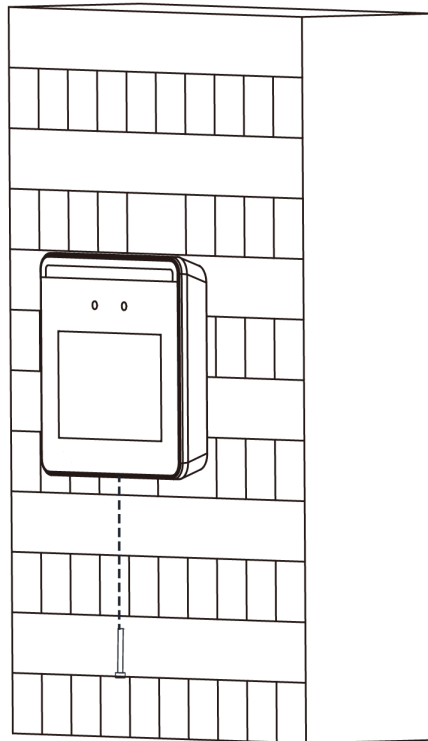


Figure 3-6 Secure Device

 **Note**

- The installation height here is the recommended height. You can change it according to your actual needs.
 - For easy installation, drill holes on mounting surface according to the supplied mounting template.
-

Chapter 4 Wiring

- If the device should connect with peripherals, it supports wiring with the RS-485 card reader, the door lock, the exit button, and the power supply.

Note

If the cable size is 18 AWG, you should use a 12 V power supply. And the distance between the power supply and the device should be no more than 80 m.

- If the device has no peripherals to be wired, it supports wiring with the power supply by using the supplied adaptor.

4.1 Terminal Description

The terminals contains power input, RS-485, and door lock.

The terminal's diagram is as follows:

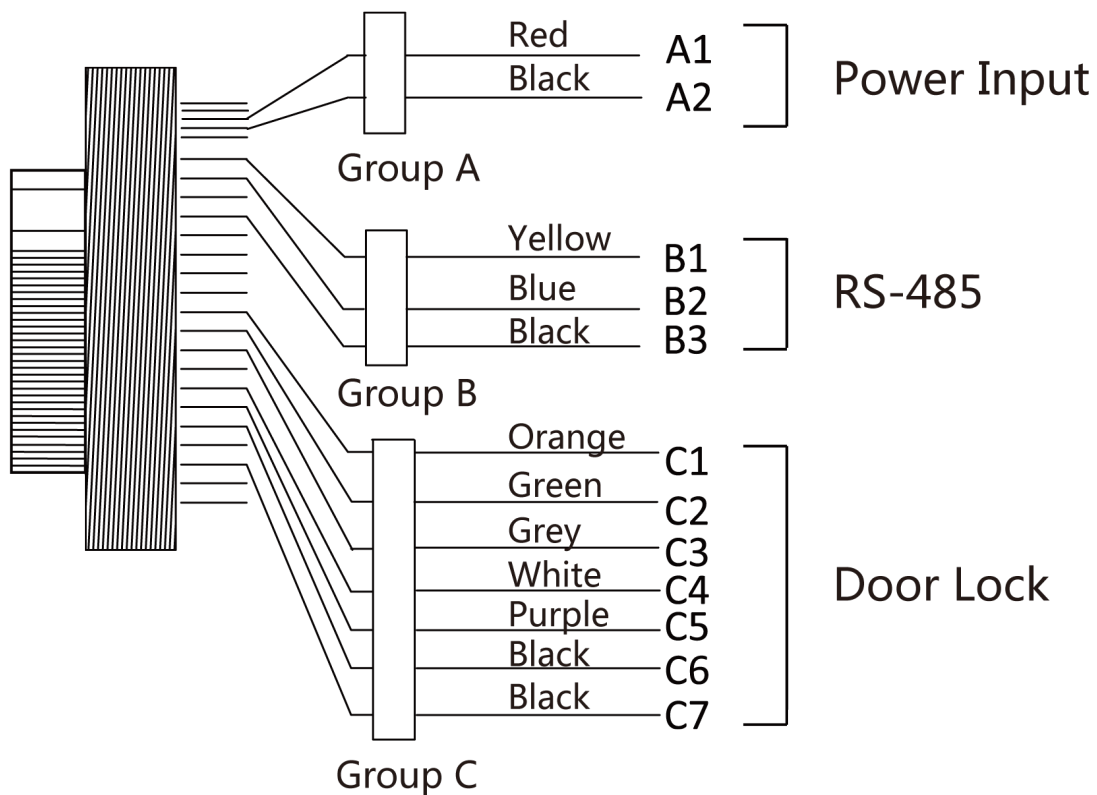


Figure 4-1 Terminal Diagram

The descriptions of the terminals are as follows:

Table 4-1 Terminal Descriptions

Group	No.	Function	Color	Name	Description
Group A	A1	Power Input	Red	+12 V	12 VDC Power Supply
	A2		Black	GND	Ground
Group B	B1	RS-485	Yellow	485+	RS-485 Wiring
	B2		Blue	485-	
	B3		Black	GND	Ground
Group C	C1	Door Lock	Orange	NC	Lock Wiring (NC)
	C2		Green	COM	Common
	C3		Grey	NO	Lock Wiring (NO)
	C4		White	SENSOR	Door Contact (Sensor)
	C5		Purple	BTN	Exit Door Wiring
	C6		Black	GND	Ground
	C7		Black	GND	Ground

4.2 Wire Normal Device

You can connect the terminal with normal peripherals.

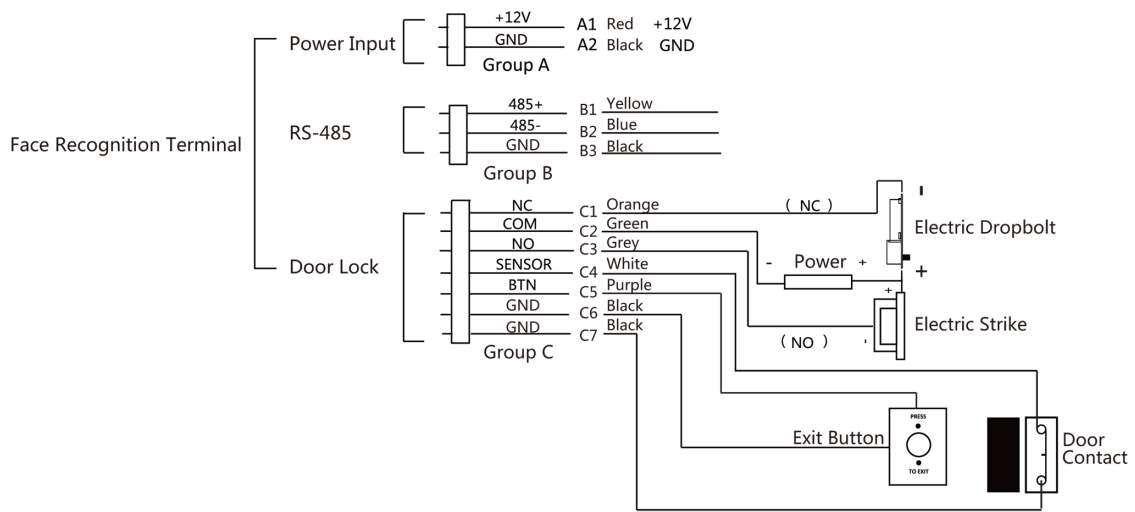


Figure 4-2 Device Wiring

Note

- The power input should be 12 VDC, 1.5 A, 18 W.
- Do not wire the device to the electric supply directly.

4.3 Wiring with Power Cable

Wire the device with power supply directly by using the supplied power cable if the device has no other peripherals to be wired.

The wiring diagram is shown below:

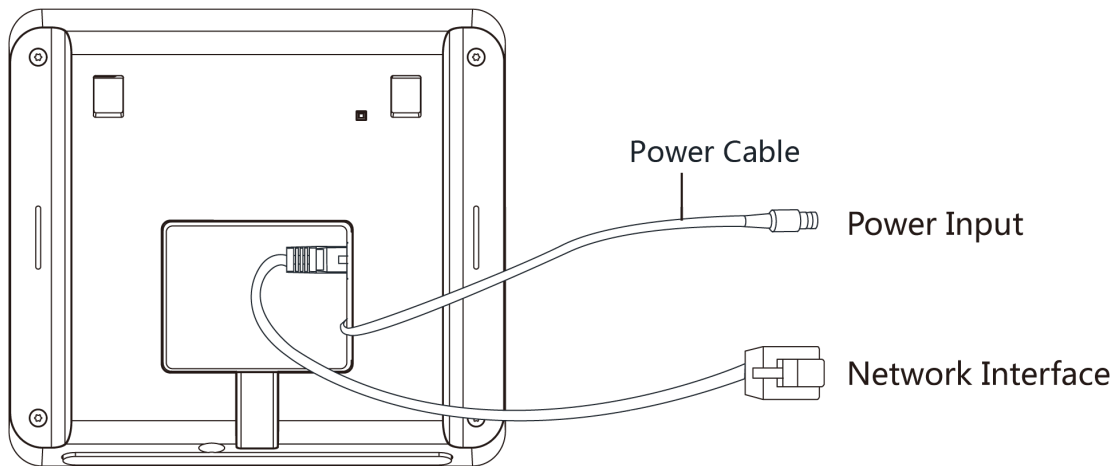


Figure 4-3 Wiring with Power Cable

Chapter 5 Activation

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

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

The default values of the device are as follows:

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

5.1 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 be activated.

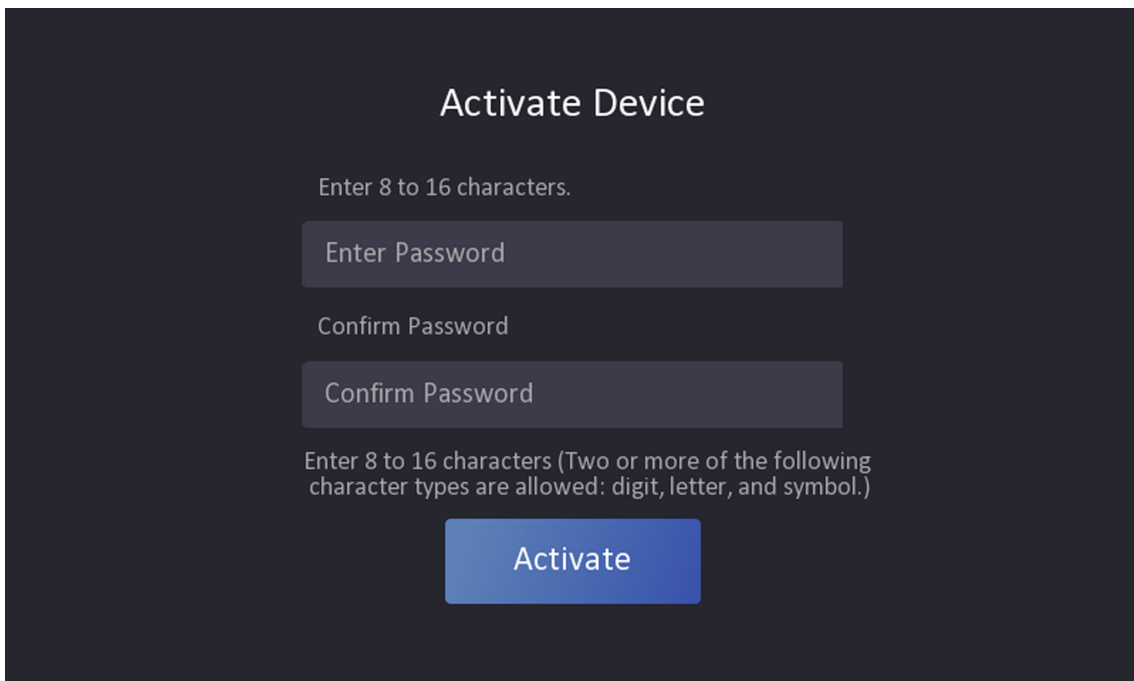


Figure 5-1 Activation Page

 **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.

5.2 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.

5.3 Activate via SADP

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

Before You Start

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

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

Steps

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

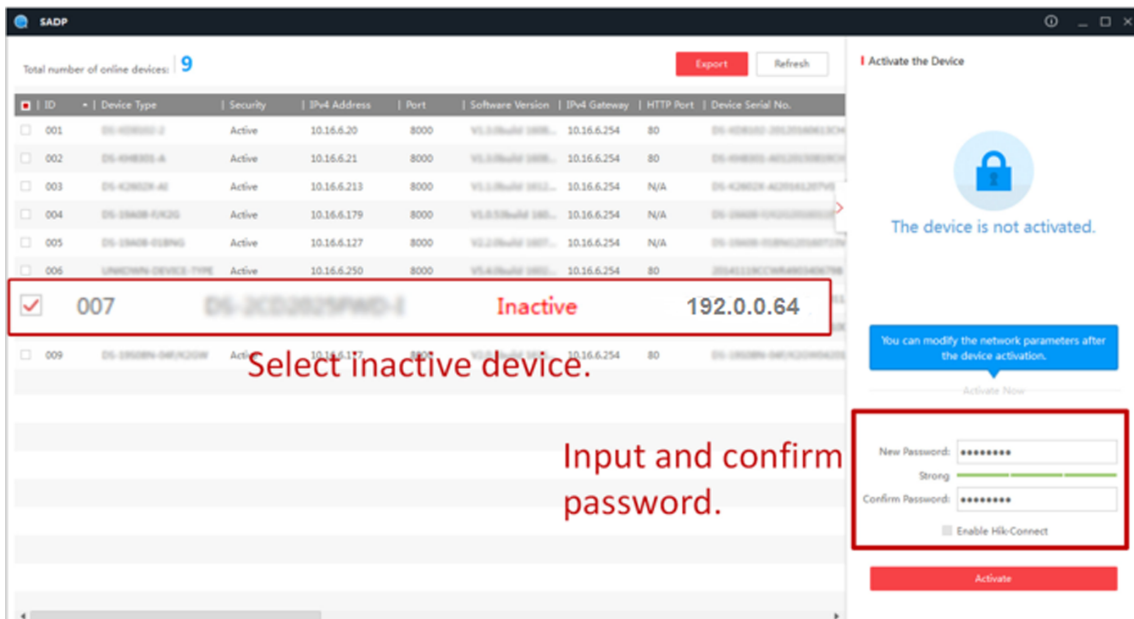
Caution

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

Note

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

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



The screenshot shows the SADP software interface. On the left, a table lists devices with columns for ID, Device Type, Security, IP Address, Port, Software Version, IP Address Gateway, HTTP Port, and Device Serial No. Device 007 is highlighted in red, with a red box around its row. A red text overlay says "Select inactive device." Below the table, another red text overlay says "Input and confirm password." On the right, a dialog box titled "Activate the Device" is shown. It contains a blue padlock icon and the text "The device is not activated." Below this, a blue box says "You can modify the network parameters after the device activation." There is an "Activate Now" button. At the bottom of the dialog, there are two password input fields: "New Password:" and "Confirm Password:", both containing asterisks. A "Strong" password strength indicator is shown between the fields. Below the password fields, there is a checkbox labeled "Enable Hik-Connect" and a red "Activate" button.

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

5. Modify IP address of the device.
 - 1) Select the device.

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


5.4 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 6 Quick Operation

6.1 Select Language

After activation, you should select a language.

Steps

1. Select a language according to the actual needs.

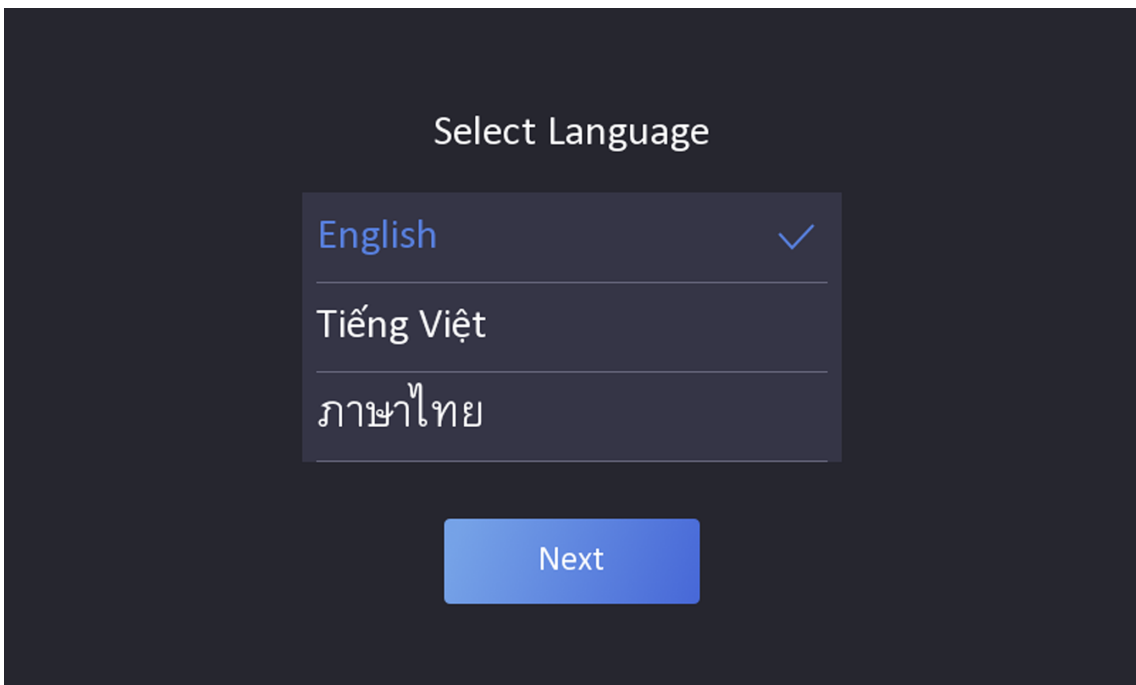


Figure 6-1 Select Language

2. Click **Next**.

6.2 Set Password Change Type

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**.

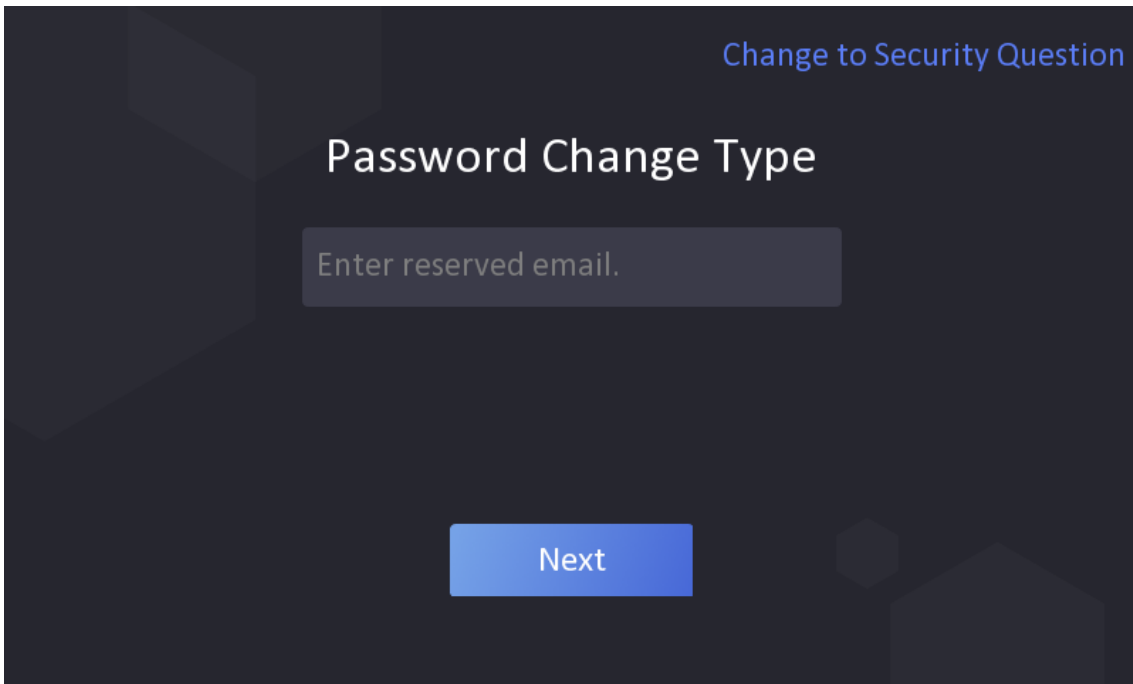


Figure 6-2 Password Change Page

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.

6.3 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.

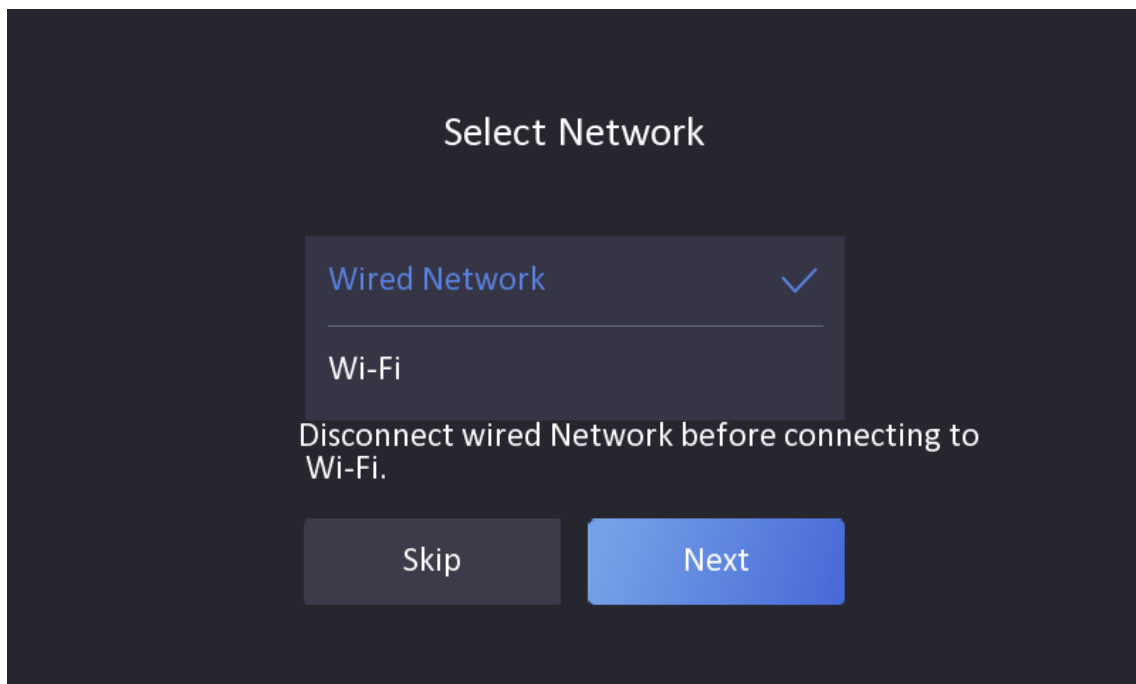


Figure 6-3 Select Network

 **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.

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.

6.4 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.

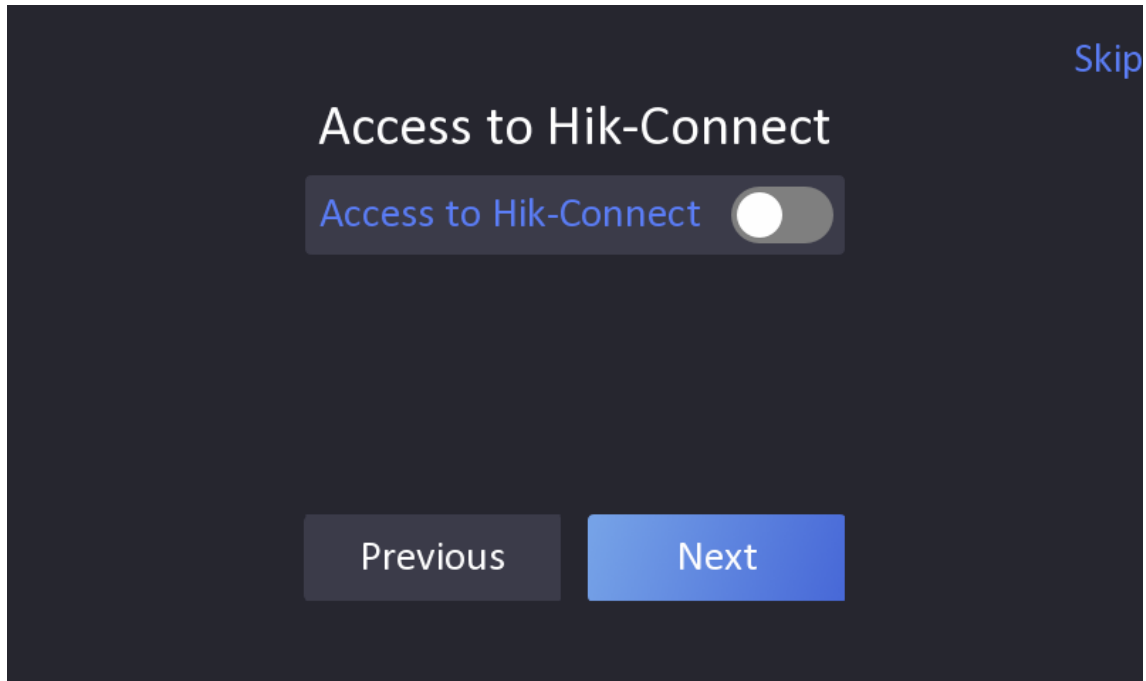


Figure 6-4 Access to Hik-Connect

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.

6.5 Remote Operation via APP

You can add the device to your mobile client for remote operation.

Download Hik-Connect to your mobile client and run the APP. Scan the QR Code in the following picture to add the device to your mobile client for remote operation.

Following the instruction in your mobile client to add the device.



Figure 6-5 Operate Remotely via APP

6.6 Privacy Settings

You should set the privacy parameters, including the picture uploading and storage.

Select parameters according to your actual needs.

Upload Pic. When Auth. (Upload Captured Picture When Authenticating)

Upload the pictures captured when authenticating to the platform automatically.

Save Pic. When Auth. (Save Captured Picture When Authenticating)

If you enable this function, you can save the picture when Authenticating to the device.

Save Registered Pic. (Save Registered Picture)

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

Upload Pic. After Linked Capture (Upload Picture After Linked Capture)

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

Save Pic. After Linked Capture (Save Pictures After Linked Capture)

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

Tap **Next** to complete the settings.

6.7 Set Administrator

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

Before You Start

Activate the device.

Steps

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

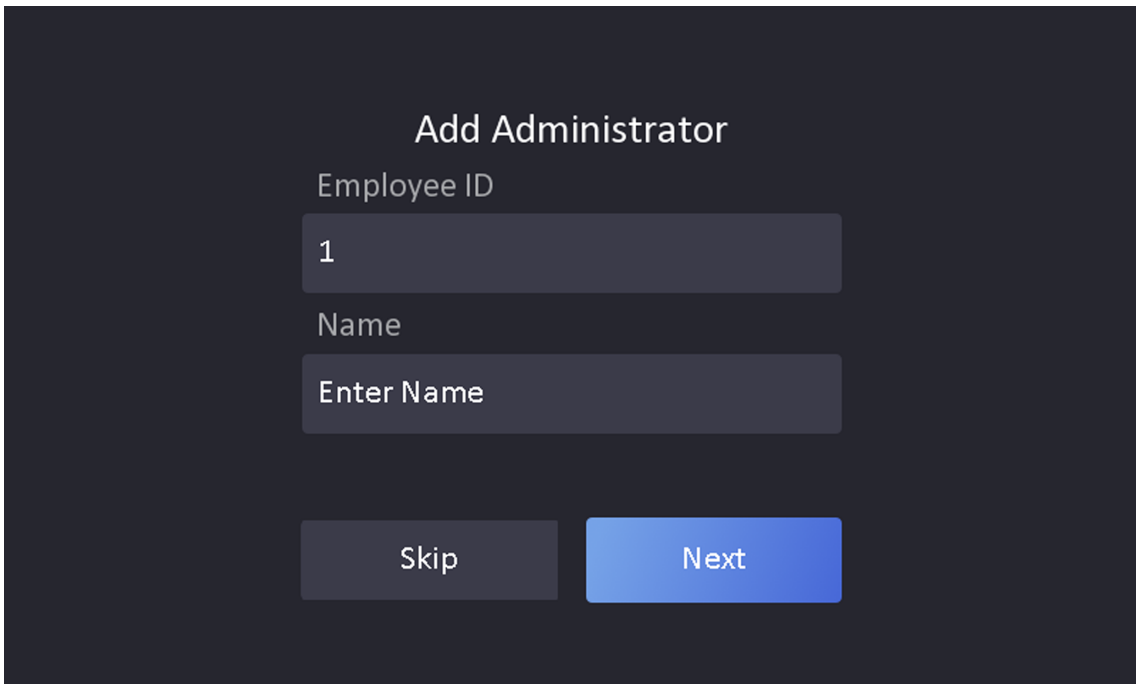






Figure 6-6 Add Administrator Page

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.
-  : Enter the card No. or present card on the card presenting area. Click **OK**.

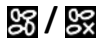
4. Click **OK**.

You will enter the authentication page.

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.

Shortcut Keys Description



Note

You can configure those shortcut keys displayed on the screen. For details, see [***Preference Settings***](#).



Enter password to authenticate.

Chapter 7 Basic Operation

7.1 Login

Login the device to set the device basic parameters.

7.1.1 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 for 3 s and slide to the left/right by following the gesture to enter the admin login page.

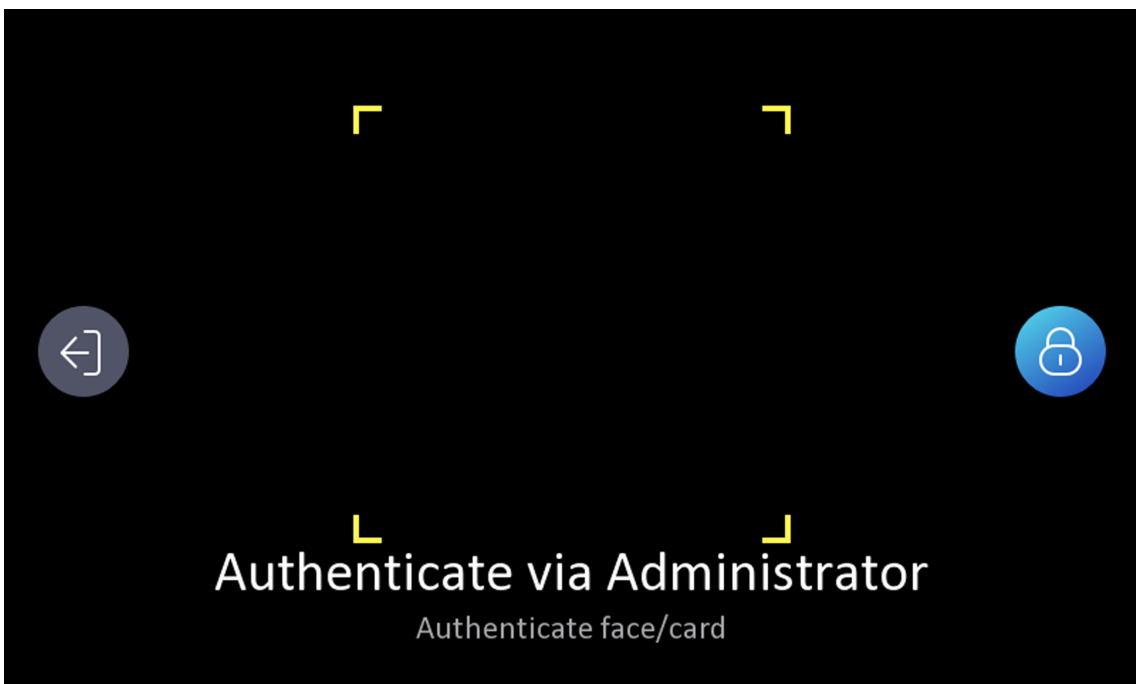


Figure 7-1 Admin Login

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

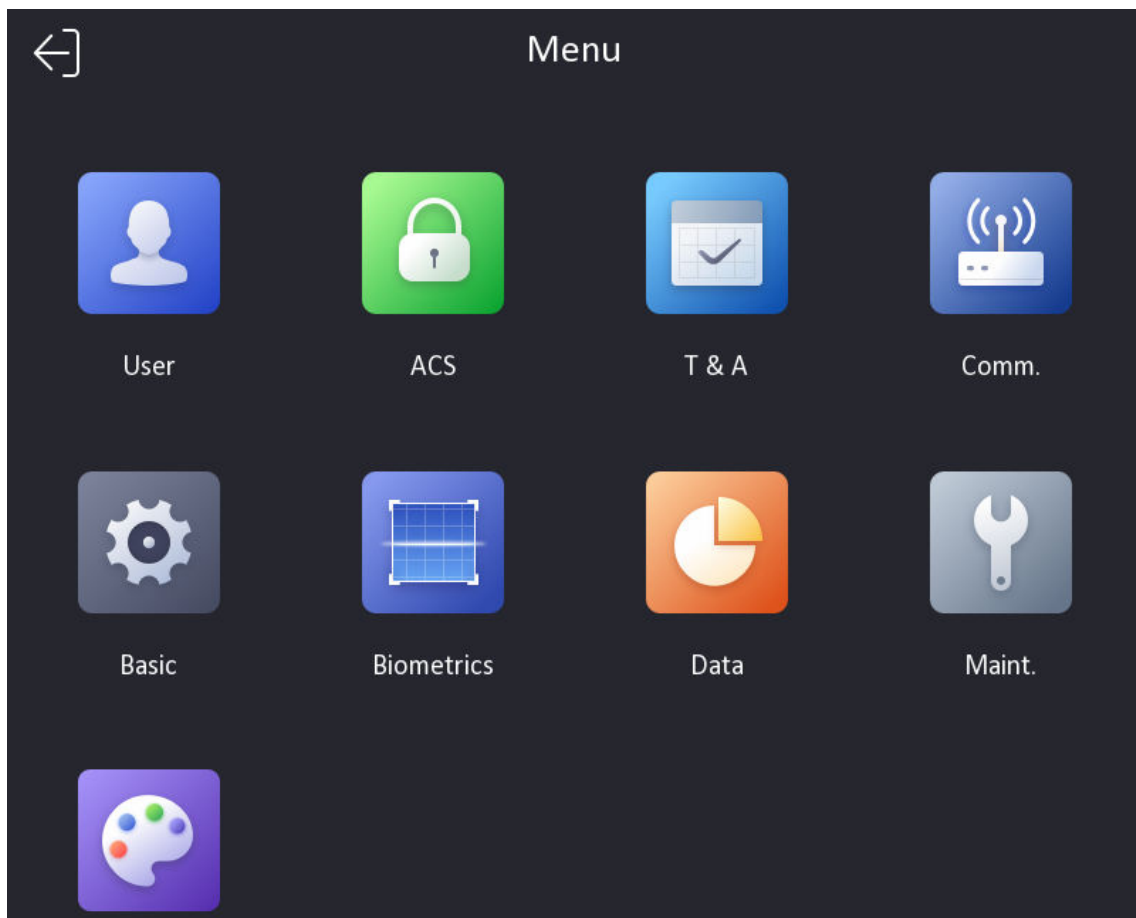




Figure 7-2 Home Page

 **Note**


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

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

7.1.2 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.

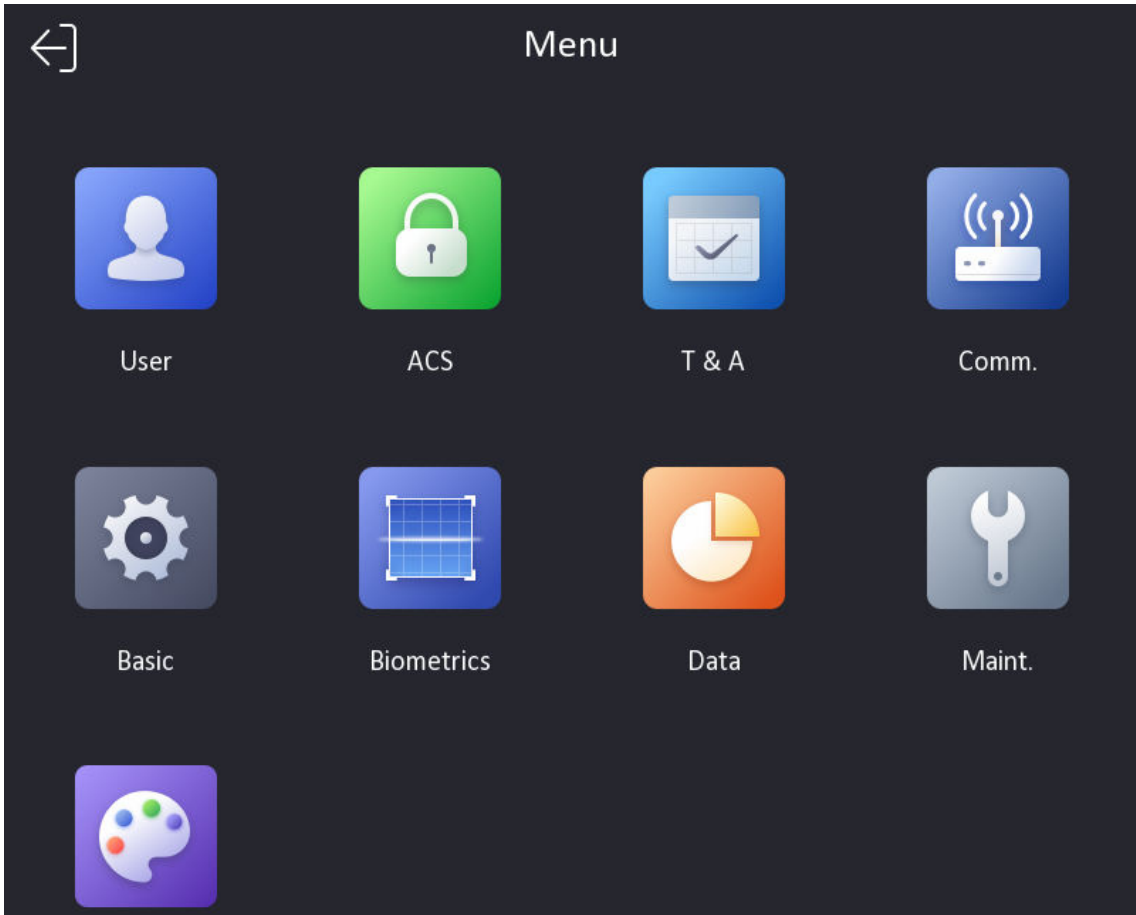



Figure 7-3 Home Page

7.1.3 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.

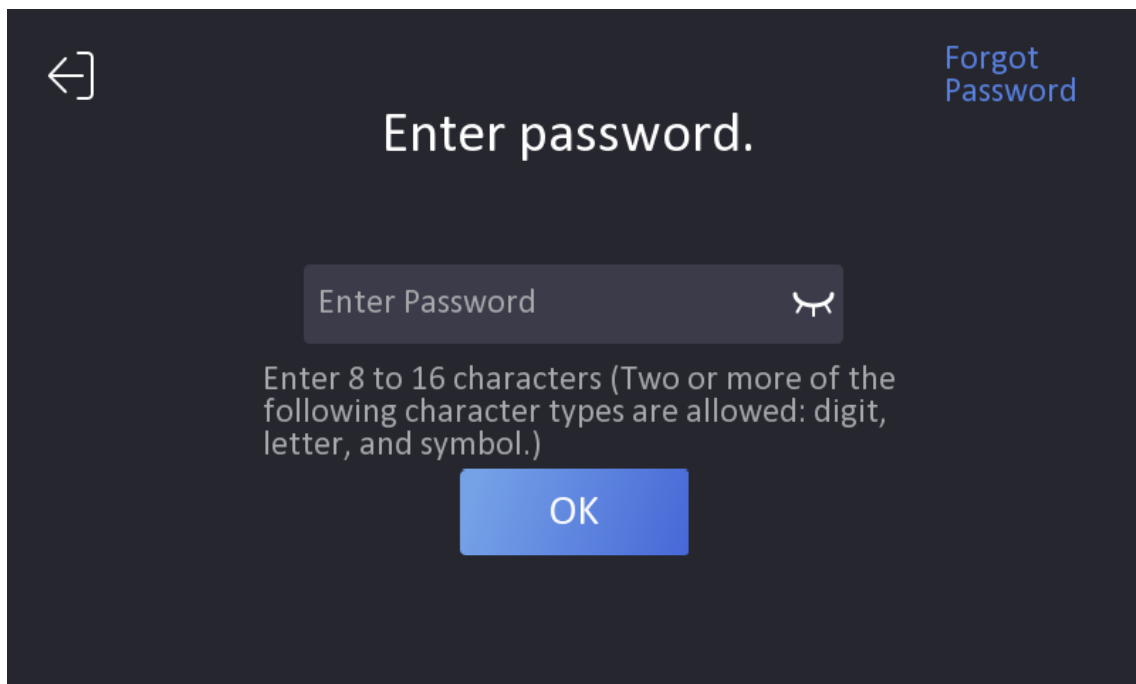


Figure 7-4 Password Authentication Page

3. Tap **Forgot Password**.
4. Select a password change type from the list.

 **Note**

If you have only set 1 password change type, you will go to the corresponded password change page for further settings.

5. Answer the security questions or change the password according to email address.
 - Security Questions: Answer the security questions that configured when activation.
 - Email Address

 **Note**

Make sure the device has added to the Hik-Connect account.

- a. Download Hik-Connect app.
- b. Go to **More** → **Reset Device Password** .
- c. Scan the QR code on the device and a verification code will be popped up.

 **Note**

Tap the QR code to get a larger picture.

- d. Enter the verification code on the device page.
6. Create a new password and confirm it.
 7. Tap **OK**.

7.2 Communication Settings

You can set the wired network, the Wi-Fi parameter, the RS-485 parameters, ISUP and access to Hik-Connect on the communication settings page.

7.2.1 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**.

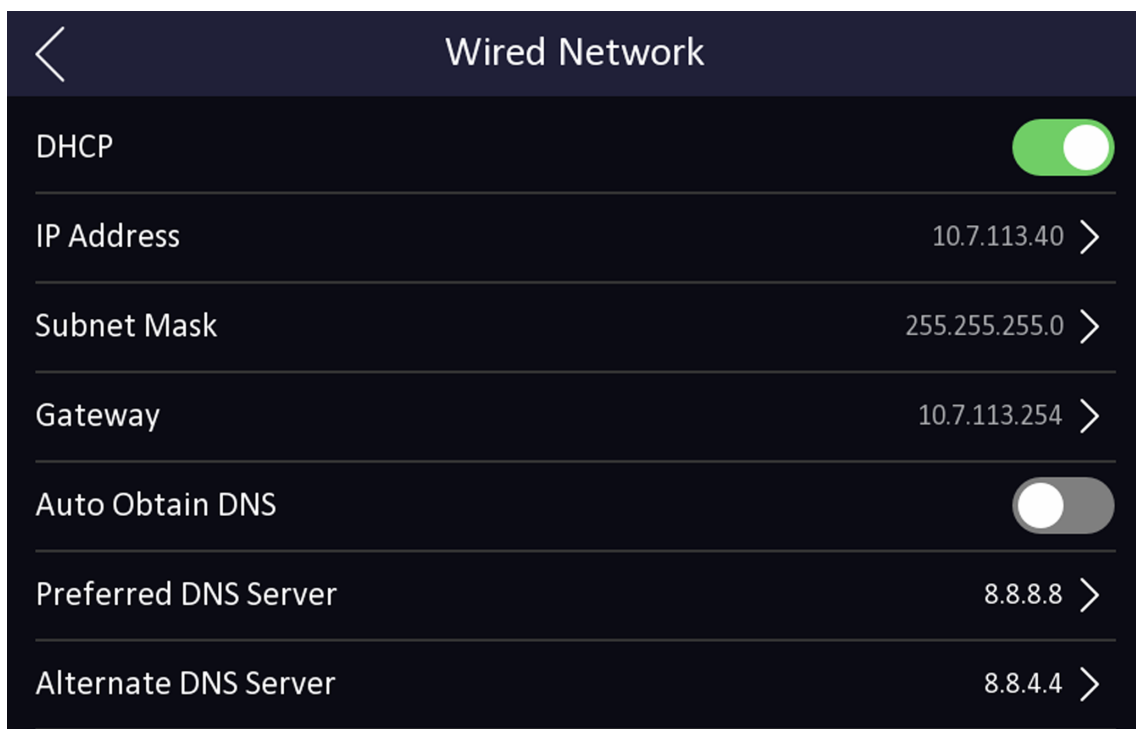


Figure 7-5 Wired Network Settings

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.

4. Set the DNS parameters. You can enable **Auto Obtain DNS**, set the preferred DNS server and the alternate DNS server.

7.2.2 Set Wi-Fi Parameters

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

Steps



The function should be supported by the device.

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

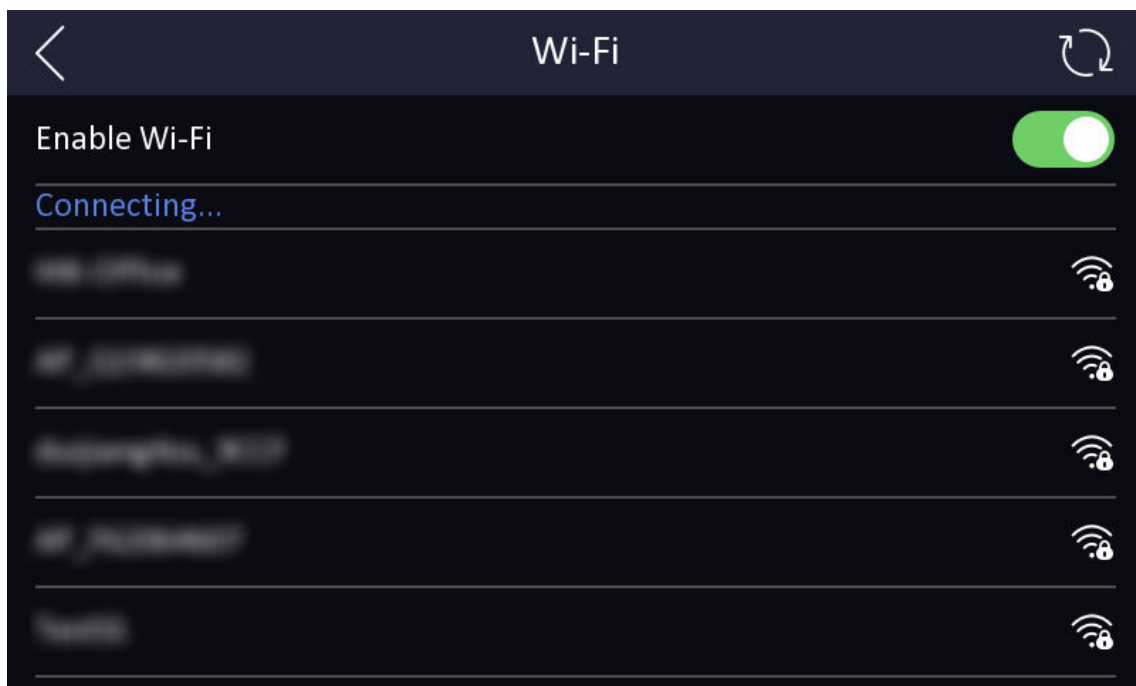


Figure 7-6 Wi-Fi Settings

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**.



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.

7.2.3 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.

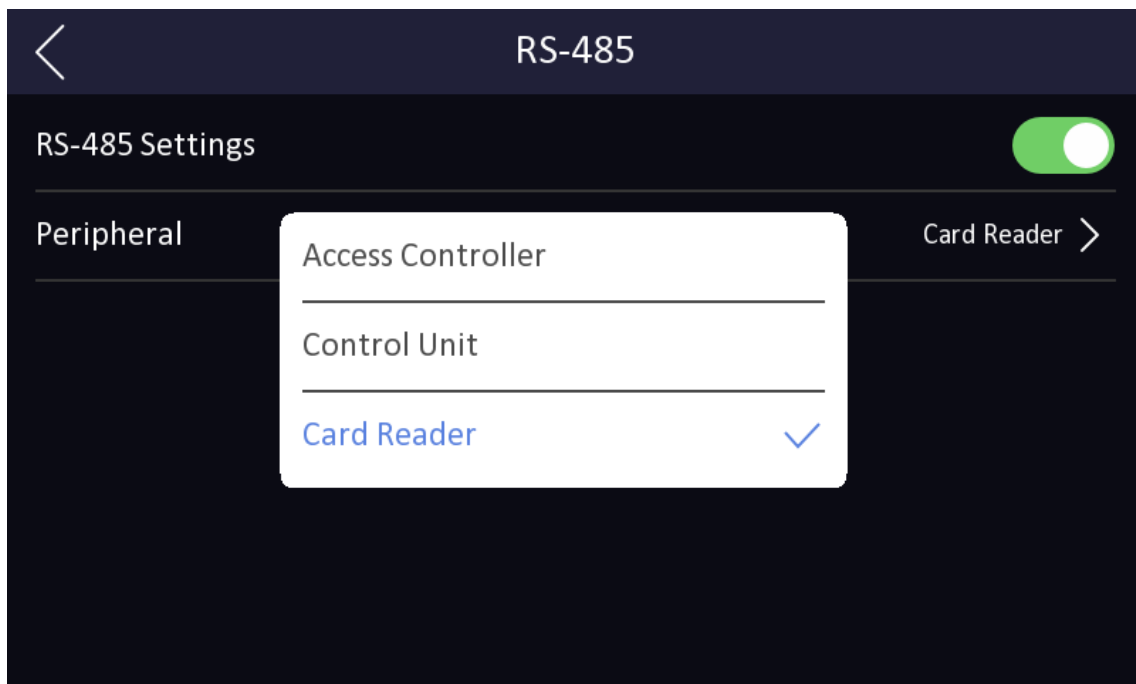


Figure 7-7 Set RS-485 Parameters

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.

7.2.4 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** .

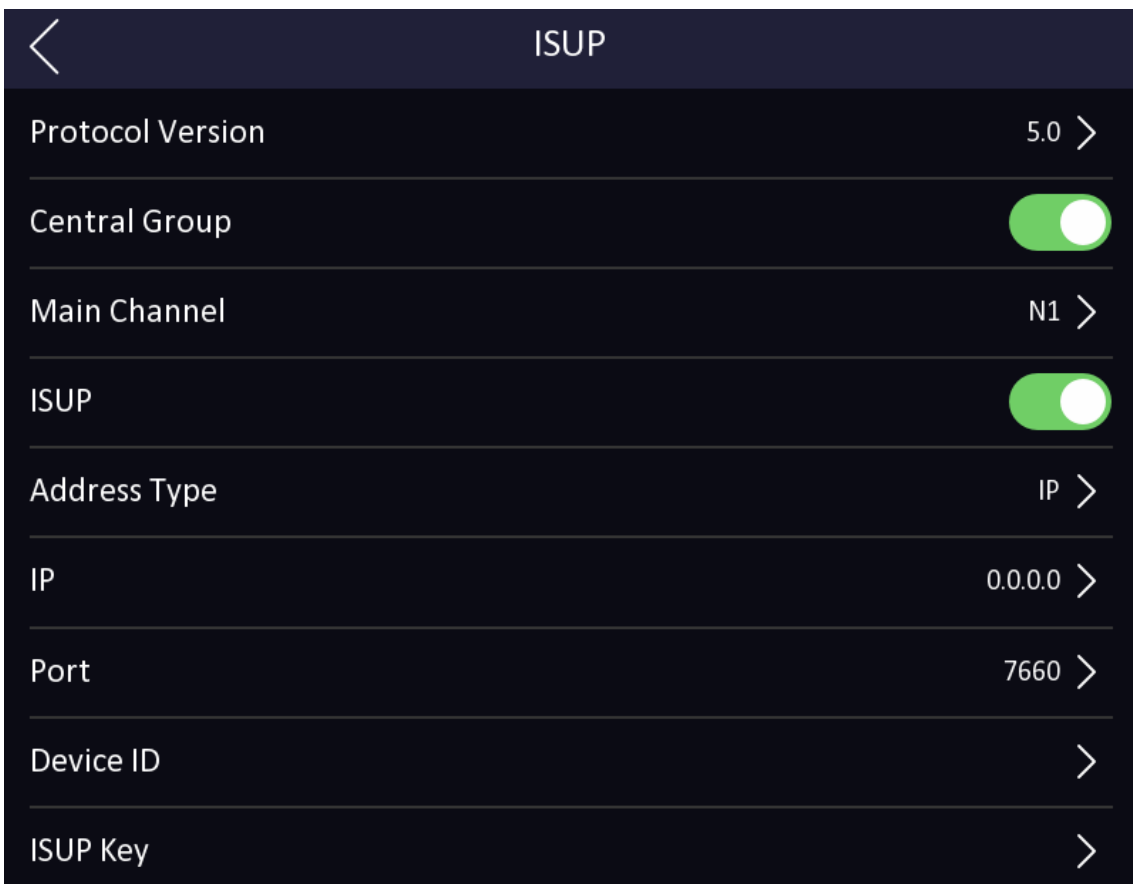


Figure 7-8 ISUP Settings

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.
-

7.2.5 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



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

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

7.3 User Management

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

7.3.1 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 **User** → **+** to enter the Add User page.

The screenshot shows a dark-themed 'Add User' screen. At the top left is a back arrow, and at the top right is a checkmark. The screen contains the following fields:

Field	Value
Employee No.	2
Name	Not Configured
Face	Not Configured
Card	0/5
PIN	Not Configured
Auth. Settings	Device Mode
User Role	Normal User

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 user name on the soft keyboard.

 **Note**

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

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


 **Note**

- For details about adding a face picture, see ***Add Face Picture*** .
- For details about adding a card, see ***Add Card*** .
- For details about adding a PIN, 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 user role as **Administrator**
8. Tap  to save the settings.

7.3.2 Add Face Picture

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

Steps

Note

Up to 1000 face pictures can be added.

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 **User** → **+** to enter the Add User 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 user name on the soft keyboard.
-

Note

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

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

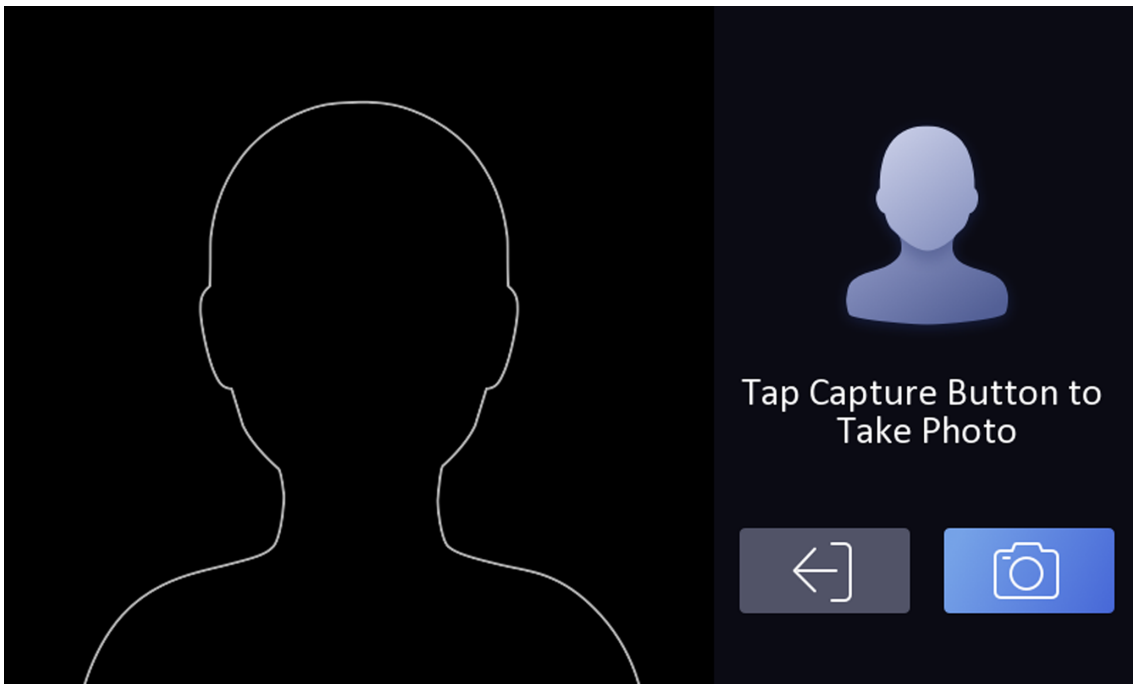


Figure 7-9 Add Face Picture

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 user role.

Administrator

The user is the administrator. Except for the normal attendance function, the user can also enter the Home page to operate after authenticating the permission.

Normal User

The User is the normal user. The user can only authenticate or take attendance on the initial page.

10. Tap  to save the settings.

7.3.3 Add Card

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

Steps

Note

Up to 1500 cards can be added.

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 **User** → **+** to enter the Add User page.
 3. Connect an external card reader according to the wiring diagram.
 4. 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.
-
5. Tap the Name field and input the user name on the soft keyboard.
-

Note

- Numbers, upper case letters, lower case letters, and special characters are allowed in the user name.
 - The suggested user name should be within 32 characters.
-
6. Tap the Card field and tap **+**.
 7. Configure the card No.
 - Enter the card No. manually.
 - Present the card over the card presenting 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.
-
8. Configure the card type.
 9. Set the user role.
-

Administrator

The user is the administrator. Except for the normal attendance function, the user can also enter the Home page to operate after authenticating the permission.

Normal User

The User is the normal user. The user can only authenticate or take attendance on the initial page.

10. Tap  to save the settings.

7.3.4 View PIN code

Add a PIN code for the user and the user 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 **User** → **+** to enter the Add User 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 user name on the soft keyboard.

Note

- Numbers, upper case letters, lower case letters, and special characters are allowed in the user name.
- The suggested user 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. Set the user role.

Administrator

The user is the administrator. Except for the normal attendance function, the user can also enter the Home page to operate after authenticating the permission.

Normal User

The User is the normal user. The user can only authenticate or take attendance on the initial page.

7. Tap  to save the settings.

7.3.5 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 **User → Add User/Edit User → 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.


7.3.6 Search and Edit User

After adding the user, you can search the user and edit it.

Search User

On the User Management page, Tap the search area to enter the Search User page. Tap **Card** on the left of the page and select a search type from the drop-down list. Enter the employee ID, card No., or the user name for search. Tap  to search.

Edit User

On the User Management page, select a user from the user list to enter the Edit User page. Follow the steps in *User Management* to edit the user parameters. Tap  to save the settings.



Note

The employee ID cannot be edited.

7.4 Data Management

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

7.4.1 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.

7.4.2 Import Data

Steps

1. Plug a USB flash drive in the device.
 2. On the Home page, tap **Data → Import Data** .
 3. Tap **User Data, Face Data** or **Access Control Parameters** .
-



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.
-



- 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 less than 2 M.
-

7.4.3 Export Data

Steps

1. Plug a USB flash drive in the device.
 2. On the Home page, tap **Data → Export Data** .
 3. Tap **Face Data, Event Data, User Data**, or **Access Control Parameters**.
-



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.
-

7.5 Authenticate via Face

If the authentication mode is Face, position the face looking at the camera to start face authentication.

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

7.6 Basic Settings

You can set the sound, time, sleeping, language, and supplement light.

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**.

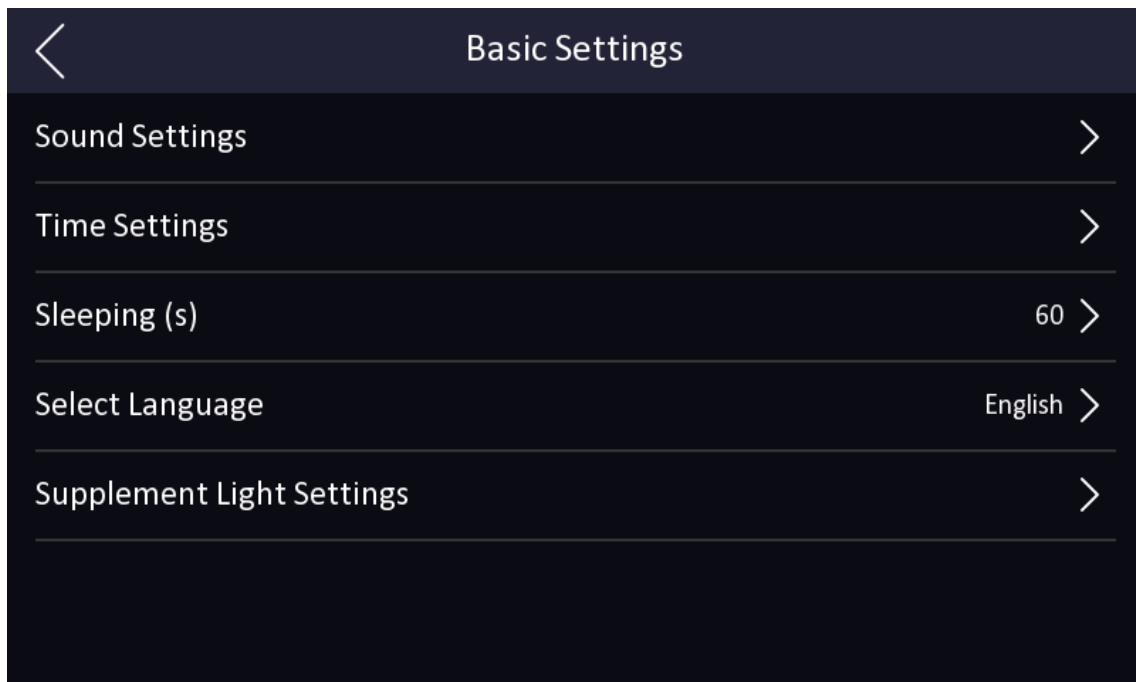


Figure 7-10 Basic Settings Page

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.

Time Settings

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

Sleeping (s)

Set the device sleeping waiting time. When you are on the initial page and if you set the sleeping time to 30 s, the device will sleep after 30 s without any operation.

Note

If you set the sleeping time to 0, the device will not enter sleeping mode.

Select Language

Select the language according to actual needs.

Supplement Light Settings

Tap **White Light** and you can set the supplement light mode. You can select to enable or disable the supplement light, or tap **Schedule** to customize the supplement light's brightness, start time, and end time.

7.7 Set Biometric Parameters


You can customize the face parameters to improve the face recognition performance. The configurable parameters includes face liveness level, recognition distance, face recognition interval, wide dynamic, face 1:N security level, ECO settings, face with mask detection.

Long tap on the initial page for 3 s and login the home page. Tap **Biometric**.



Figure 7-11 Biometric Parameters Page

Table 7-1 Face Picture Parameters

Parameter	Description
Face Liveness Level	After enabling face anti-spoofing function, you can set the matching security level when performing live face authentication.
Recognition Distance	Set the valid distance between the user and the camera when authenticating.
Face Recognition Interval	The time interval between two continuous face recognitions when authenticating.  Note You can input the number from 1 to 10.
Wide Dynamic	It is suggested to enable the WDR function if installing the device outdoors. When there are both very bright and very dark areas simultaneously in the view, you can enable the WDR function to balance the brightness of the whole image and provide clear images with details.

Parameter	Description
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.
ECO Settings	<p>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).</p> <p>ECO Mode Threshold</p> <p>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.</p> <p>ECO Mode (1:N)</p> <p>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</p> <p>Face with Mask&Face(1:N ECO)</p> <p>Set the matching value 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.</p>
Face with Mask Detection	<p>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.</p> <p>The strategy parameters are as follows:</p> <p>None</p> <p>No reminders will be pop up.</p> <p>Reminder of Wearing</p> <p>If the person do not wear a face mask when authenticating, the device prompts a notification and the door will open.</p> <p>Must Wear</p> <p>If the person do not wear a face mask when authenticating, the device prompts a notification and the door keeps closed.</p>

7.8 Set Access Control Parameters

You can set the access control permissions, including the functions of authentication mode, enable NFC card, enable M1 card, door contact, open duration (s) and authentication interval (s).

On the Home page, tap **ACS** (Access Control Settings) to enter the Access Control Settings page. Edit the access control parameters on this page.

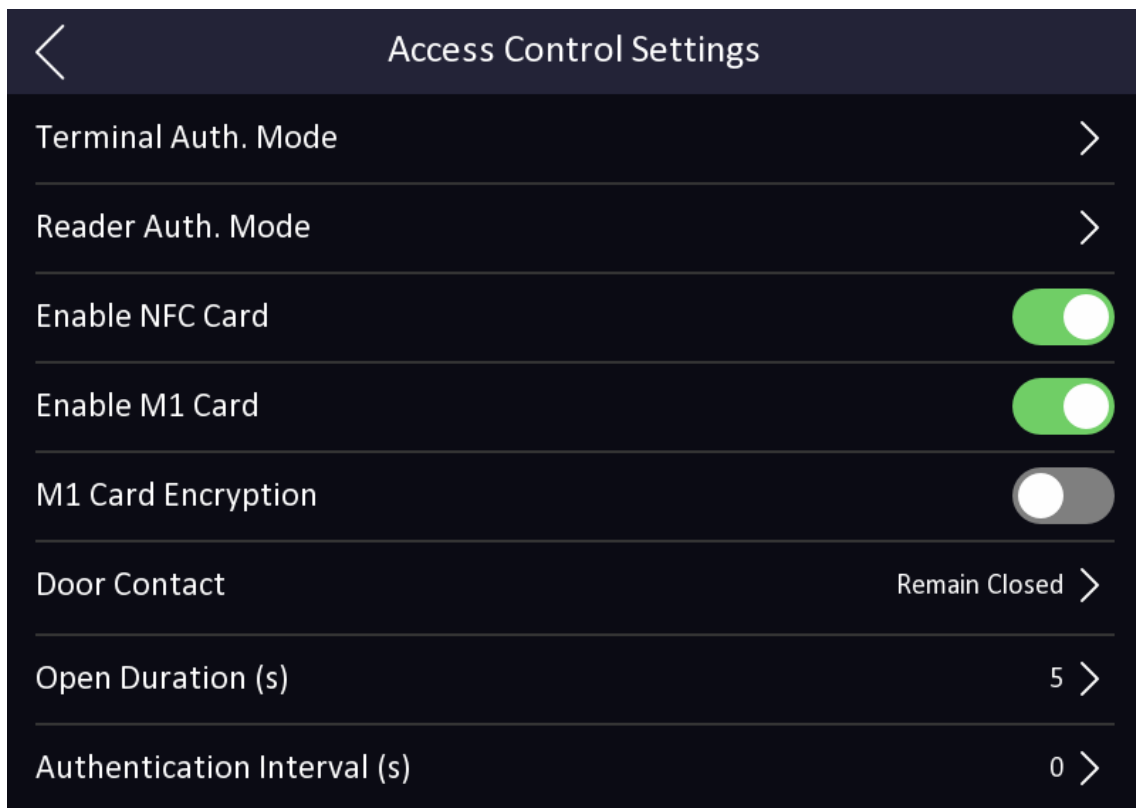


Figure 7-12 Access Control Parameters

The available parameters descriptions are as follows:

Table 7-2 Access Control Parameters Descriptions

Parameter	Description
Terminal Auth. Mode (Terminal Authentication Mode)	<p>Select the face recognition terminal's authentication mode. You can also customize the authentication mode.</p> <p>Note</p> <ul style="list-style-type: none"> 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.
Reader Auth. Mode (Card Reader Authentication Mode)	Select the card reader's authentication mode.
Enable NFC Card	Enable the function and you can present the NFC card to authenticate.

Parameter	Description
Enable M1 Card	Enable the function and you can present the M1 card to authenticate.
M1 Card Encryption	Enabling the M1 card encryption function can improve the card security level. The card will not be copied easily.
Door Contact	You can select "Open (Remain Open)" or "Close (Remian Closed)" according to your actual needs. By default, it is Close (Remian Closed).
Open Duration	Set the door unlocking duration. If the door is not opened for the set time, the door will be locked. Available door locked time range: 1 to 255s.
Authentication Interval	Set the device authenticating interval. Available authentication interval range: 0 to 65535.

7.9 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.

7.9.1 Disable Attendance Mode via Device

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

Tap **T&A Status** to enter the T&A Status page.

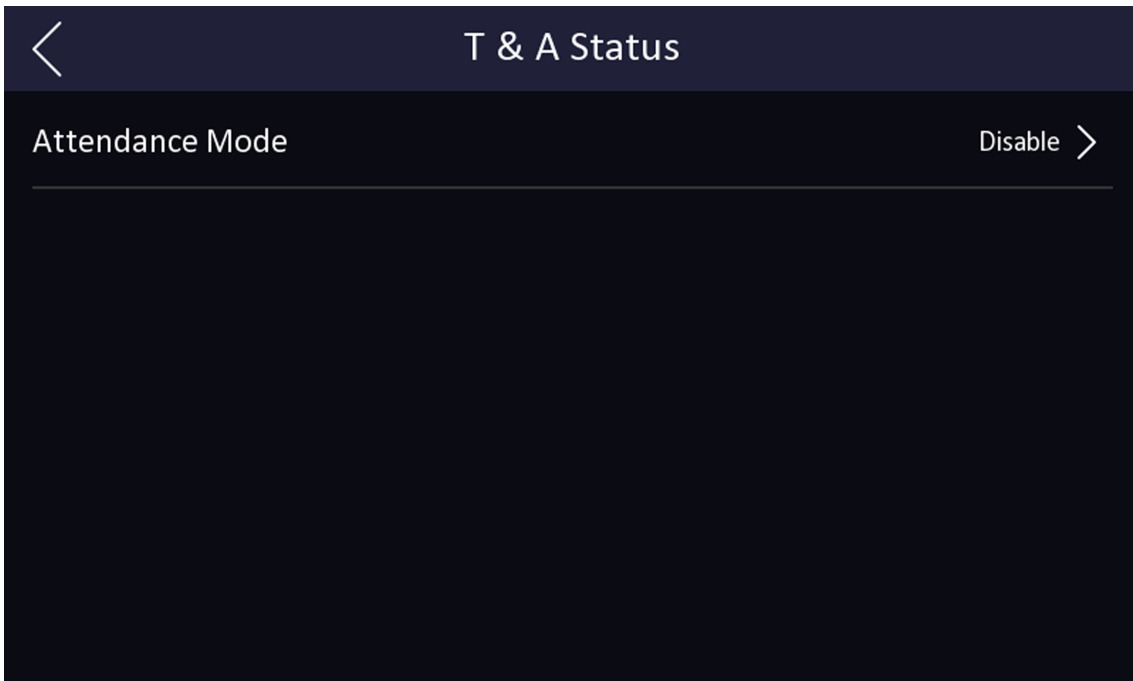


Figure 7-13 Disable Attendance Mode

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.

7.9.2 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 T&A Status** to enter the T&A Status page.
- 2. Set the Attendance Mode as Manual.**

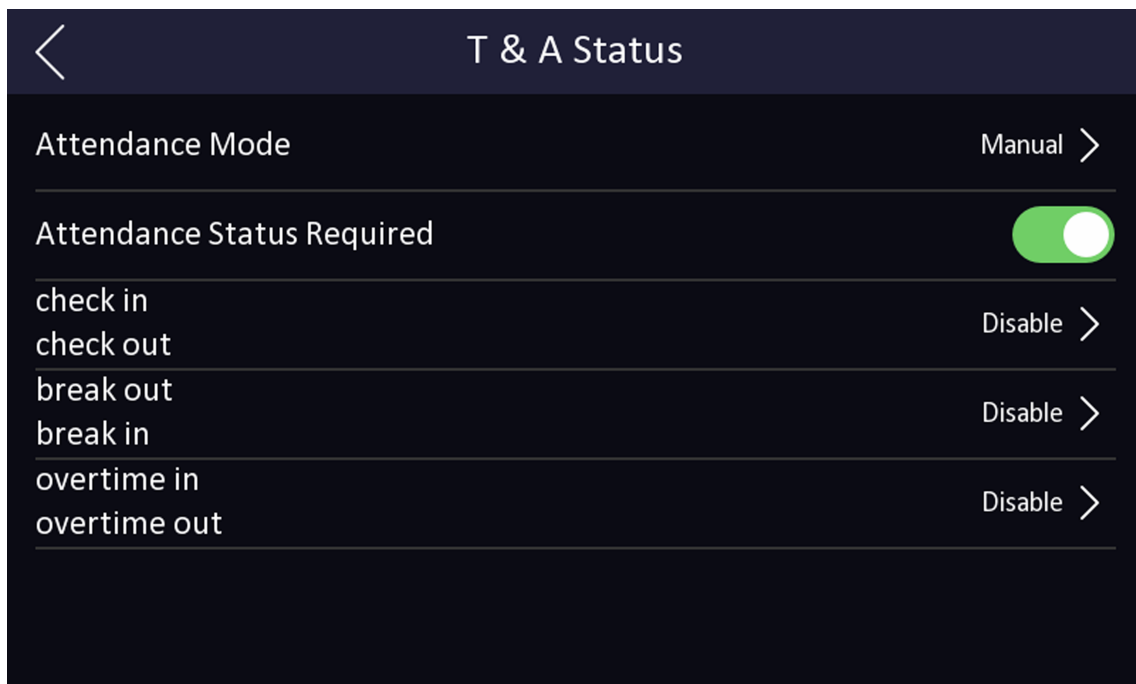


Figure 7-14 Manual Attendance Mode

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.

7.9.3 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 **T&A Status** to enter the T&A Status page.
2. Set the **Attendance Mode** as **Auto**.

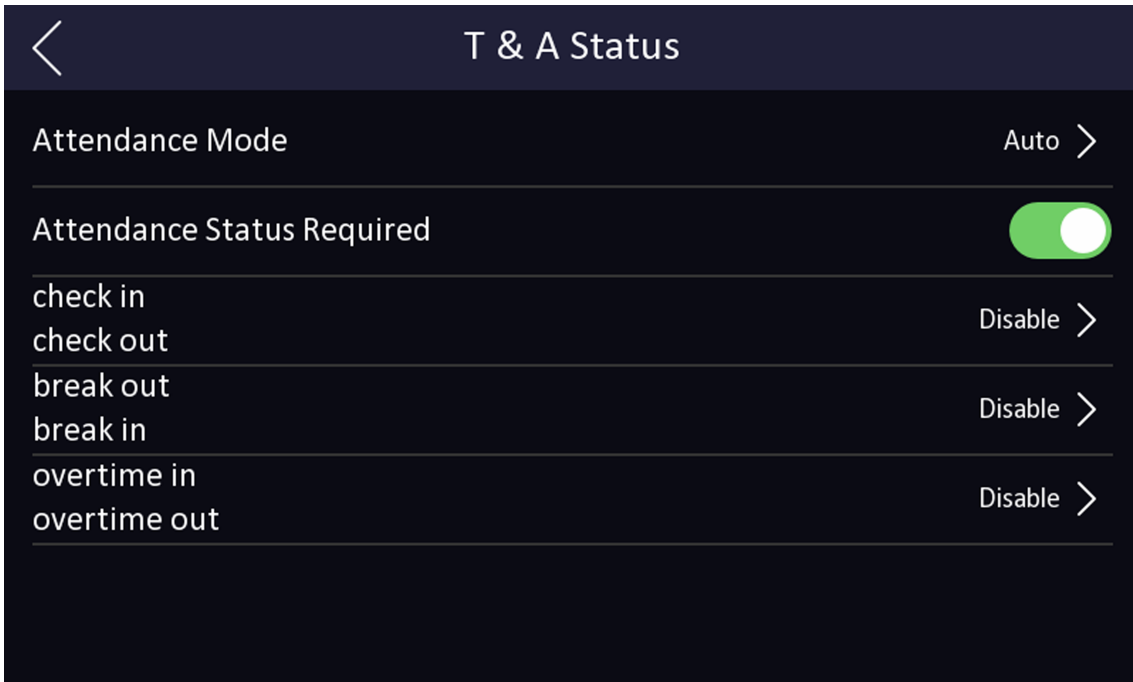


Figure 7-15 Auto Attendance Mode

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.

7.9.4 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 **T&A Status** to enter the T&A Status page.
2. Set the **Attendance Mode** as **Manual and Auto**.

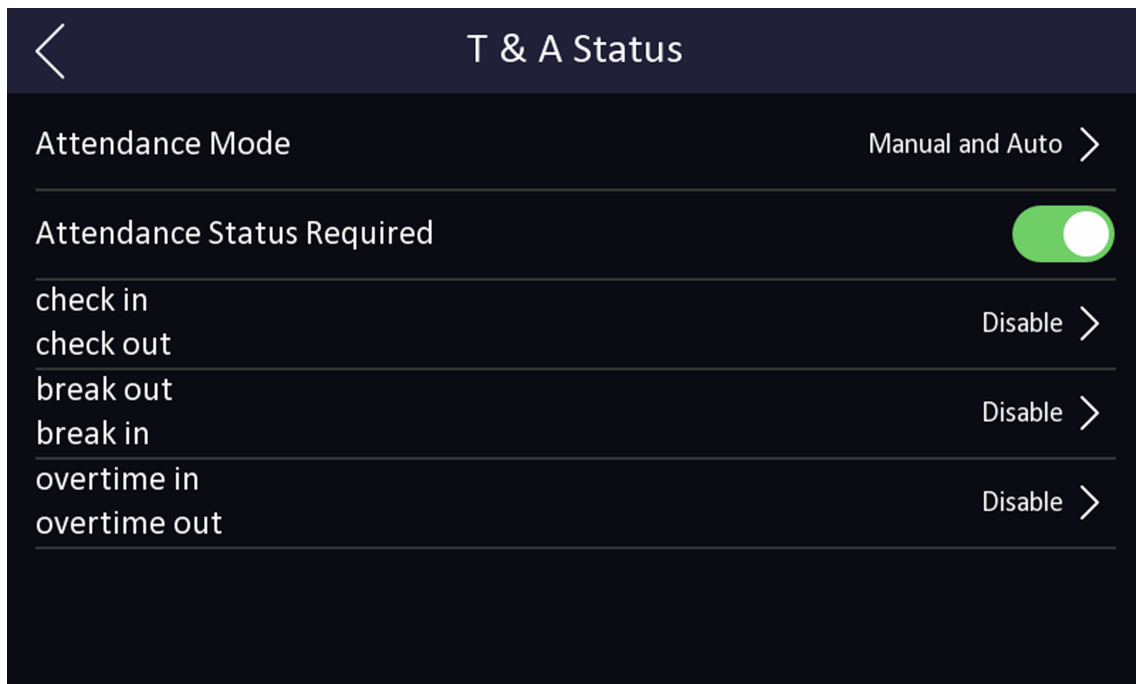


Figure 7-16 Manual and Auto Mode

3. Enable the **Attendance Status** function.
4. Enable a group of attendance status.



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.



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.

7.10 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, reboot the device, set face parameters and view version information.

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

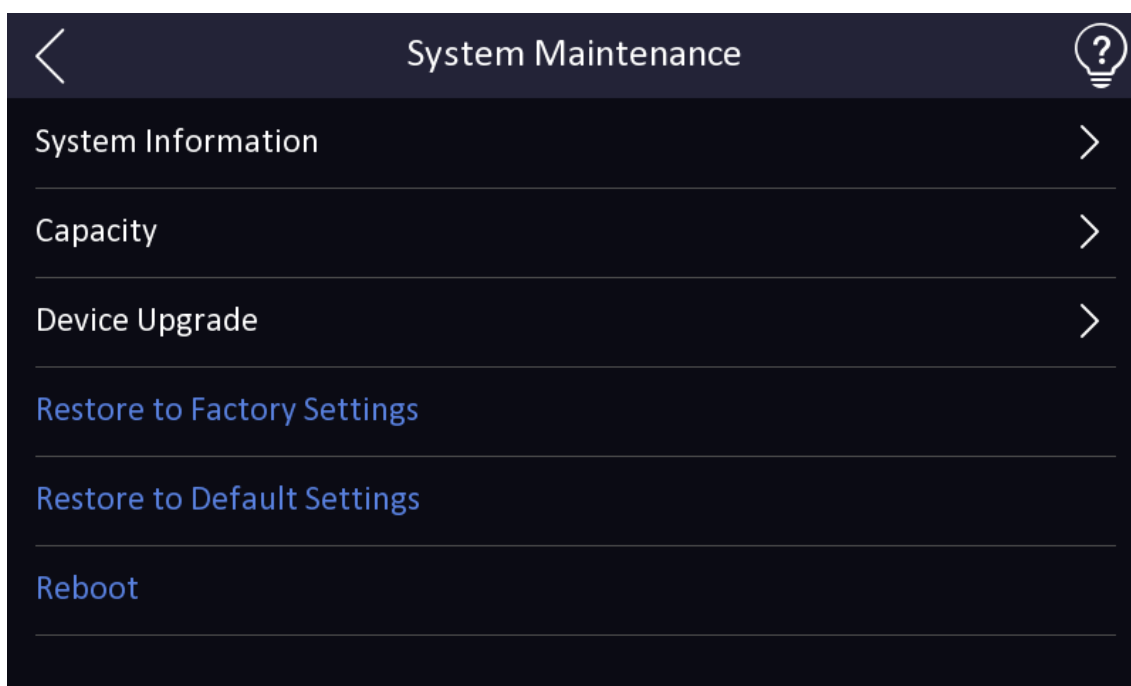


Figure 7-17 System Maintenance

System Information

You can view the device model, serial No., versions, MAC 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.

Capacity

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

Device 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.

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.

Reboot

Reboot the device.

Advanced Settings

Long Tap  on the right corner to enter the advanced settings page. Enter the password.

Face Parameter

Custom Anti-Spoofing Detection

Face Liveness Level

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

Anti-Spoofing Detection Threshold

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

Anti-Spoofing Detection Threshold of Face with Mask

The larger the value, the smaller the false accept rate and the larger the false rejection rate of the face with mask. The smaller the value, the larger the false accept rate and the smaller the false rejection rate of the face with mask.

Lock Face for Anti-Spoofing Protection

After enabling this function, the device will lock automatically when anti-spoofing detection failed.

Lock Duration

The lock duration after enabling **Lock Face for Anti-Spoofing Protection** when anti-spoofing detection failed.

Version Information

You can view the device information.

7.11 Preference Settings

You can configure preference settings parameters.

Steps

1. Tap **Preference** to enter the preference settings page.

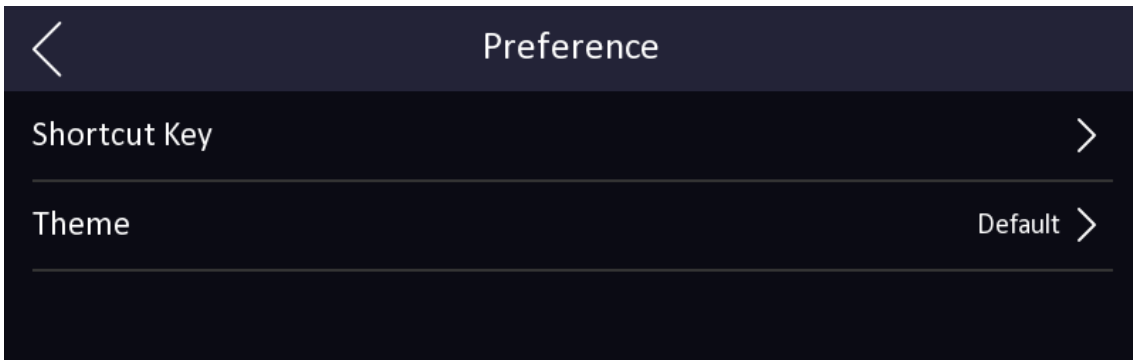


Figure 7-18 Preference Settings

Shortcut Key

Choose the shortcut key that displayed on the authentication page, including the password entering function.

Password

Enable this function and you can enter the password to authenticate via password.

Theme

You can set the theme of the prompt window on the authentication page. You can select **Theme** as **Default** or **Simple**.

Default

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


Simple

After selecting this mode, the live view of the authentication page will be disabled, and in the meanwhile, the person's name, employee ID, face pictures will all be hidden after authentication.

Chapter 8 Quick Operation via Web Browser

8.1 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.



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

Click **Next** to complete the settings.

8.2 Time Settings

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

Device Time

Display the device time in real time.

Time Zone

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

Time Synchronization Mode

NTP

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

Manual

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


DST

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

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

8.3 Privacy Settings

Set the picture uploading and storage parameters.

Click  in the top right of the web page to enter the wizard page. After setting device language and time, you can click **Next** to enter the **Privacy Settings** 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 parameters. Or click **Skip** to skip privacy settings.

8.4 Administrator Settings

Steps

1. Click  → **Administrator Settings** .
2. Enter the employee ID and name of the administrator.
3. Select a credential to add.

Note

You should select at least one credential.

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

Note

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

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

Note

Up to 5 cards can be supported.

Click **Next** to complete the settings.

Chapter 9 Operation via Web Browser

9.1 Login

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



Make sure the device is activated.

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



Make sure that the IP address starts with **Http:**.

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

9.2 Forgot Password

If you forget the device password, you can change the device password via security questions.

Steps



You can change the device password via PC web.

1. Click **Forgot Password** on the login page.
2. Select the verification method.
3. Answer the reserved security questions.



The answers are configured when you first activate the device.

4. Create a new password and confirm the password.
5. Click **Next** to save the settings.

9.3 Live View

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

Function Descriptions:

Door Status

Click  to view the device live view.



Set the volume when starting live view.



Note

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



You can capture image when starting live view.



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



Full screen view.



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

Controlled Status

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

Real-Time Event

You can view the event Employee ID, Name, Card No., Event Type, Time, and Operation. You can also click **View More** to enter the search conditions, including the event type, employee ID, the name, the card No., the time, the unit, the temperature and the temperature exception. Click **Search**. The results will be displayed on the right panel.

Person Information

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

Network Status

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

Basic Information

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

Device Capacity

You can view the Person, Face, Card and Event capacity.

View More

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

9.4 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, and person type.

If you select **Visitor** as the person type, you can set the visit times.

Click **Save** to save the settings.

Set Permission Time

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

Enable **Long-Term Effective User**, or set **Start Time** and **End Time** and the person can only has the permission within the configured time period according to your actual needs.

Click **Save** to save the settings.

Set Room No.

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

Click the textbox of **Floor No.** and **Room No.** and enter a numeric between 1 and 999 to set the floor No. and room No.

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.

9.5 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.

9.6 Configuration

9.6.1 View Device Information

View the device name, language, model, serial No., version, available cameras, IO input, IO output, Lock, Local RS-485, alarm input, alarm output, and device capacity, etc.

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

You can view device name, language, model, serial No., version, available cameras, IO input, IO output, Lock, Local RS-485, alarm input, alarm output, and device capacity, etc.

9.6.2 Set Time

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

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

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

Time Zone

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

Time 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.


9.6.3 Set DST

Steps

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

9.6.4 Change Administrator's Password

Steps

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



Caution

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

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

9.6.5 View Device Arming/Disarming Information

View device arming type and arming IP address.

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

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

9.6.6 Network Settings

Set TCP/IP, port, Wi-Fi parameters, ISUP, platform access and SDK server.

Note

Some device models do not support Wi-Fi or mobile data settings. Refer to the actual products when configuration.

Set Basic Network Parameters

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

You can view the mac address and MTU.

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 **Self-Adaptive**.

DHCP

If you disable DHCP, you should manually set the IPv4 address, IPv4 subnet mask, IPv4 default gateway, preferred DNS server, and alternate DNS server.

If you enable DHCP, the system will automatically allocate the IPv4 address, IPv4 subnet mask, the IPv4 default gateway preferred DNS server and alternate DNS server.

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 **Configuration** → **Network** → **Network Settings** → **Wi-Fi** .
2. Check **Wi-Fi**.
3. Add Wi-Fi.
 - Click **Manual Add**, and enter **SSID** and **Security Mode**.
4. Select a Wi-Fi
 - Click **Connect** of a Wi-Fi in the list and enter the Wi-Fi password.
 - Click **Manual Add**, and enter **SSID** and **Security Mode**. Click **OK**.
5. **Optional**: Set the WLAN parameters.
 - 1) Disable **DHCP** and 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.
 - 2) Disable **DHCP** and set the DNS server. Or enable **DHCP** and the system will allocate DNS server automatically.

6. Click **Save**.

Set Port Parameters

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

Click **Configuration** → **Network** → **Network Service** → **HTTP(S)** .

HTTP

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

HTTPS

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

HTTP Listening

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



Note

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

Click **Configuration** → **Network** → **Network Service** → **RTSP** .

RTSP

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

Click **Configuration** → **Network** → **Device Access** → **SDK Server** .

SDK Server

It refers to the port through which the client adds the device.

Platform Access

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

Steps



Note

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

1. Click **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. Check **Enable** to enable video encryption. Set the video encryption password and confirm password.
 6. Click **More** and check **WLAN** or **Wired Network** to adjust the network priority.
 7. Click **View** to view device QR code. Scan the QR code to bind the account.
-

Note

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

8. Click **Save** to enable the settings.
-

Set ISUP Parameters

Set the ISUP parameters for accessing device via ISUP protocol.

Steps

Note

The function should be supported by the device.

1. Click **Configuration** → **Network** → **Device Access** → **ISUP** .
 2. Check **Enable**.
 3. Select the ISUP version and Server IP Address, Port, Device ID, and you can view the Register status.
-

Note

If you select 5.0 as the version, you should set the Encryption Key and Network Connection Priority as well. You can click **More** and check **WLAN** or **Wired Network** to adjust the network priority.

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**.
-

9.6.7 Set Video and Audio Parameters

Set the image quality and resolution.

Set Video Parameters

Click **Configuration** → **Video/Audio** → **Video** .

Set the camera name, stream type, video type, resolution, bit rate type, Max. bit rate and I Frame Interval.

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



Note

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

Set Audio Parameters

Click **Configuration** → **Video/Audio** → **Audio** .

Set the audio output volume.

Check **Enable Voice Prompt** according to your needs.

9.6.8 Set Image Parameters

You can adjust the image parameters, video parameters, supplement light parameters, enable WDR.

Steps

1. Click **Configuration** → **Image** .
2. Configure the parameters to adjust the image.

Image Adjustment

Drag the block or enter the value to adjust the live video's brightness, contrast, saturation, and sharpness.

LED Light

Set the supplement light type and mode. You can also set the brightness.

Backlight

Enable or disable **WDR**.

When there are both very bright and very dark areas simultaneously in the view, WDR balances the brightness level of the whole image and provide clear images with details.

Video Adjustment (Video Standard)

Set the video frame rate when performing live view remotely. After changing the standard, you should reboot the device to take effect.

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.

Start All Recording

You can click  to record when starting live view.

Capture Interval

You can click  to capture image when starting live view.

Full Screen

You can click  for full screen view.

3. Click **Restore Default Settings** to restore the parameters to the default settings.

9.6.9 Access Control Settings

Set Authentication Parameters

Click **Configuration** → **Access Control** → **Authentication Settings** .



Note

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

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

If select **Terminal 1**:

Terminal/Terminal Type/Terminal Model

Select terminal and get the terminal description. They are read-only.

Enable Authentication Device

Enable the authentication function.

Authentication

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

Recognition Interval

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

Authentication Interval

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

Alarm of Max. Failed Attempts

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

Tampering Detection

Enable the anti-tamper detection for the card reader.

Card No. Reversing

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

If select **Terminal 2**:

Terminal/Terminal Type/Terminal Model

Select terminal and get the terminal description. They are read-only.

Enable Authentication Device

Enable the authentication function.

Authentication

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

Recognition Interval

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

Alarm of Max. Failed Attempts

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

Communication with Controller Every

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

Max. Interval When Entering Password

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

OK LED Polarity/Error LED Polarity

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

Tampering Detection

Enable the anti-tamper detection for the card reader.

Set Door Parameters

Click **Configuration** → **Access Control** → **Door Parameters** .

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

Door Name

You can create a name for the door.

Open Duration

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

Door Open Timeout Alarm

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

Door Magnetic Sensor Type

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

Exit Button Type

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

Door Lock Powering Off Status

You can set the door lock status when the door lock is powering off. By default, it is **Remain Closed**.

Extended Open Duration

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

Door Remain Open Duration with First Person

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

Duress Code

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

Super Password

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



Note

The duress code and the super code should be different.

Set RS-485 Parameters

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

Click **Configuration** → **Access Control** → **RS-485** .

You can view the default RS-485 protocol, baud rate, data bit, stop bit, parity, flow control and communication mode.

Check **Enable**, and set the parameters.

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

Peripheral Type

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

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.

Set Terminal Parameters

You can set terminal parameters for accessing.

Click **Configuration** → **Access Control** → **Terminal Parameters** .

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

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

9.6.10 Card Settings

Set Card Security

Click **Configuration** → **Card Settings** → **Card Type** to enter the settings page.

Set the parameters and click **Save**.

Enable NFC Card

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



Note

Disable NFC card cannot completely avoid presenting NFC card.

Enable M1 Card

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

M1 Card Encryption

Sector

M1 card encryption can improve the security level of authentication.

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

Enable EM Card

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

Enable DESFire Card

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

Enable FeliCa Card

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

Set Card No. Authentication Parameters

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

Go to **Configuration** → **Card Settings** → **Card No. Authentication Settings** .

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

Full Card No.

All card No. will be read.

Wiegand 26 (3 bytes)

The device will read card via Wiegand 26 protocol (read 3 bytes).

Wiegand 34 (4 bytes)

The device will read card via Wiegand 34 protocol (read 4 bytes).

9.6.11 Time and Attendance Status Settings

Set time and attendance status, for example, manual, auto, manual and auto.

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 **Configuration** → **T&A Status** 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.



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

Set Auto Attendance via Web

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

Before You Start

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

Steps

1. Click **Configuration** → **T&A Status** 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.



The Attendance Property will not be changed.

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

Set Manual and Auto Attendance via Web

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

Before You Start

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

Steps

1. Click **Configuration** → **T&A Status** 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.

9.6.12 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.

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.

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.

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.

9.6.13 Set Biometric Parameters

Set Basic Parameters

Click **Configuration** → **Smart** → **Smart** .



Note

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

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

Face Anti-spoofing

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



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

Anti-spoofing Detection Level

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

Recognition Distance

Select the distance between the authenticating user and the device camera.

Pitch Angle

The maximum pitch angle when starting face authentication.

Yaw Angle

The maximum yaw angle when starting face authentication.

Face Picture Quality Grade for Applying

Set the face picture's grade.

1:N Matching Threshold

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

Face Recognition Timeout Value

Set the timeout value when face recognizing. If the face recognition time is longer than the configured value, the system will pop up a prompt.

ECO Mode

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 Mode Threshold

The larger the value, the device enter the ECO Mode easier.

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

Face with Mask Detection

After enabling the face without mask detection, the system will recognize the captured face with mask picture or not. You can set face with mask 1:N matching threshold, it's ECO mode, and the strategy.

None

The function is disabled. The device will not detect whether a person is wearing a face mask or not.

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 1:N Match Threshold

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

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.

Set Recognition Area

Click **Configuration** → **Smart** → **Area Configuration** .

Drag the yellow frame in the live video to adjust the recognition area. Only the face within the area can be recognized by the system.

Or drag the block of each parameter to set the area.

Click **Save**.

Click  or  , or  to capture pictures, record videos, and view full screen live video.

9.6.14 Preference Settings

Set the theme, notice publication, prompt schedule, custom prompt, and authentication result text.

Set Preference

You can set the display theme and the sleep time for the device.

Set Theme

Click **Configuration** → **Preference** .

Sleep

Enable **Sleep** and the device will enter the sleep mode when no operation within the configured sleep time.

Display Mode

You can select display theme for device authentication. You can select **Display Mode** as **Authentication** or **Simple**. When you select **Simple**, the information of name, ID, face picture will be not displayed.

Notice Publication

You can set the notice publication for the device.

Click **Configuration** → **Preference** → **Notice Publication** .

Theme Management

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



Note

Only the format of JPG is supported. Each picture should be smaller than 1 MB with resolution up to 1920*1280. Up to 8 pictures are supported.

You can click **+**, and set **Name** and **Type** to create a theme. After creating the theme, click **+** in the **Theme Management** panel to select pictures in the media library. Click **OK** to add pictures to the theme.

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



Note

The slide show interval ranges from 1 s to 10 s.

Click **Edit Name** to change the them name. Click **Delete Program** to delete the theme.

Schedule Management

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 **Clear** or **Clear All** to delete the schedule.

Customize Audio Content


Customize the output audio content when authentication succeeded and failed.

Steps

1. Click **Configuration** → **Preference** → **Prompt Schedule** .
2. Enable the function.
3. Set the appellation.
4. Set the time period when authentication succeeded.
 - 1) Click **Add Time Duration**.
 - 2) Set the time duration and the language.


Note

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

-
- 3) Enter the audio content.
 - 4) **Optional:** Repeat substep 1 to 3.
 - 5) **Optional:** Click  to delete the configured time duration.
5. Set the time duration when authentication failed.
- 1) Click **Add Time Duration**.
 - 2) Set the time duration and the language.

Note



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

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

Customize Prompt Voice

You can customize prompt voices for the device.

Steps

1. Click **Configuration** → **Preference** → **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.

Configure Authentication Result Text

Steps

1. Go to **Configuration** → **Preference** → **Authentication Result Text** .
2. Enable **Customize Authentication Result Text**.
3. Enter custom texts.
4. Click **Save**.

9.6.15 Upgrade and Maintenance


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

Reboot Device

Click **Maintenance and Security** → **Maintenance** → **Restart** .
Click **Restart** to reboot the device.

Upgrade

Click **Maintenance and Security** → **Maintenance** → **Upgrade** .

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

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



Note

Do not power off during the upgrading.

Restore Parameters

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

Restore All

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

Restore

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

Import and Export Parameters

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

Export

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



Note

You can import the exported device parameters to another device.

Import

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

Click **Advanced Settings**, and enter the admin password.

Face Parameter

Custom Anti-Spoofing Detection

Face Liveness Level

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

Anti-Spoofing Detection Threshold

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

Anti-Spoofing Detection Threshold of Face with Mask

The larger the value, the smaller the false accept rate and the larger the false rejection rate when the detected face is with a mask. The smaller the value, the larger the false accept rate and the smaller the false rejection rate when the detected face is with a mask.

Lock Face for Anti-Spoofing Protection

After enabling this function, the device will lock automatically when anti-spoofing detection failed.

Lock Duration

The lock duration after enabling **Lock Face for Anti-Spoofing Protection** when anti-spoofing detection failed.

Unlock

You can click **Unlock** according to your needs.

Version Information

You can view the device information.

9.6.16 Device Debugging

You can set device debugging parameters.

Steps

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

Enable SSH

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

Print Log

You can click **Export** to export log.

Capture Network Packet

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

9.6.17 Log Query

You can search and view the device logs.

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

9.6.18 Security Mode Settings

Set the security mode for logging in the client software.

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

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

Security Mode

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

Compatible Mode

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

9.6.19 Certificate Management

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



Note

The function is only supported by certain device models.

Create and Import HTTPS Certificate

Steps

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

6. Import the signed certificate.

- 1) In the **Import Key** area, select a certificate from the local, and click **Import**.
- 2) In the **Import Communication Certificate** area, select a certificate from the local, and click **Import**.

Create and Import SYSLOG Certificate

Steps

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

Import CA Certificate

Before You Start

Prepare a CA certificate in advance.

Steps

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



Note

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

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

Chapter 10 Other Platforms to Configure

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

iVMS-4200 Client Software

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

<http://enpinfodata.hikvision.com/analysisQR/showQR/ca930247>

HikCentral Access Control (HCAC)

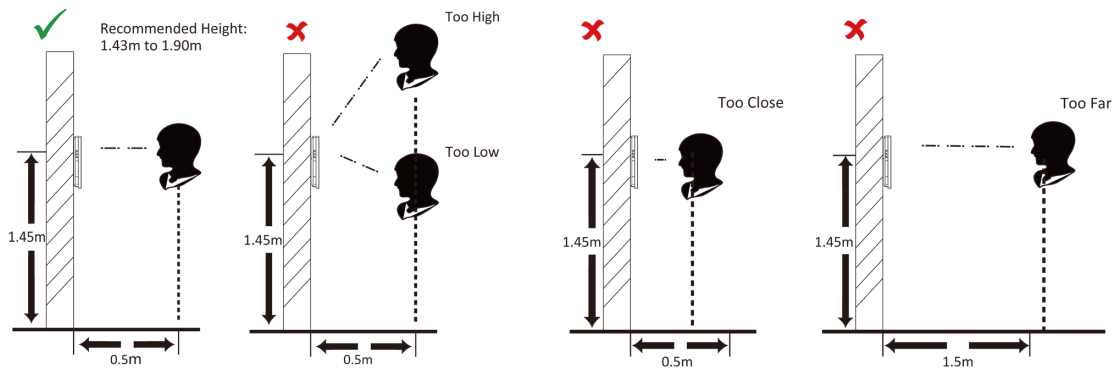
Click/tap the link to view the HCAC's user manual.

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

Appendix A. 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.

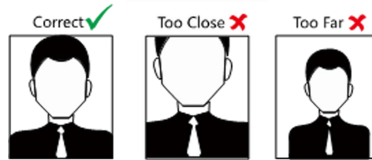
Posture

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 B. Tips for Installation Environment

1. Light Source Illumination Reference Value



Candle: 10Lux

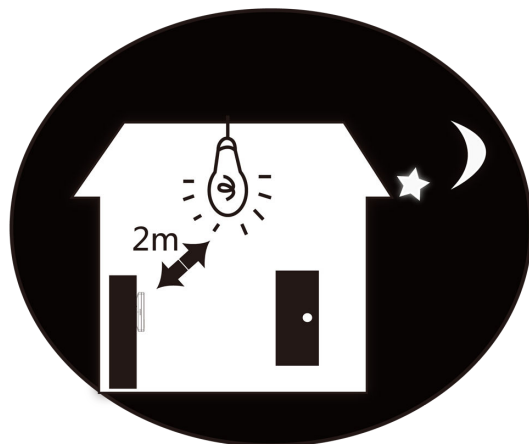
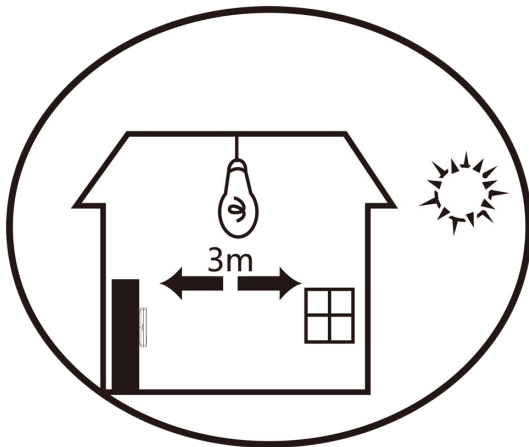


Bulb: 100~850Lux

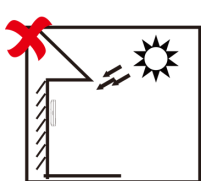


Sunlight: More than 1200Lux

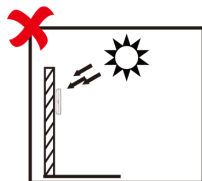
2. Install the device at least 2 meters away from the light, and at least 3 meters away from the window or door.



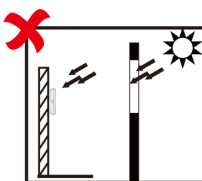
3. Avoid backlight, direct and indirect sunlight



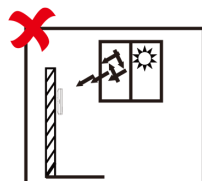
Backlight



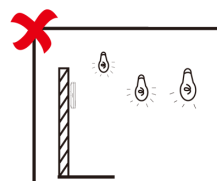
Direct Sunlight



Direct Sunlight
through Window

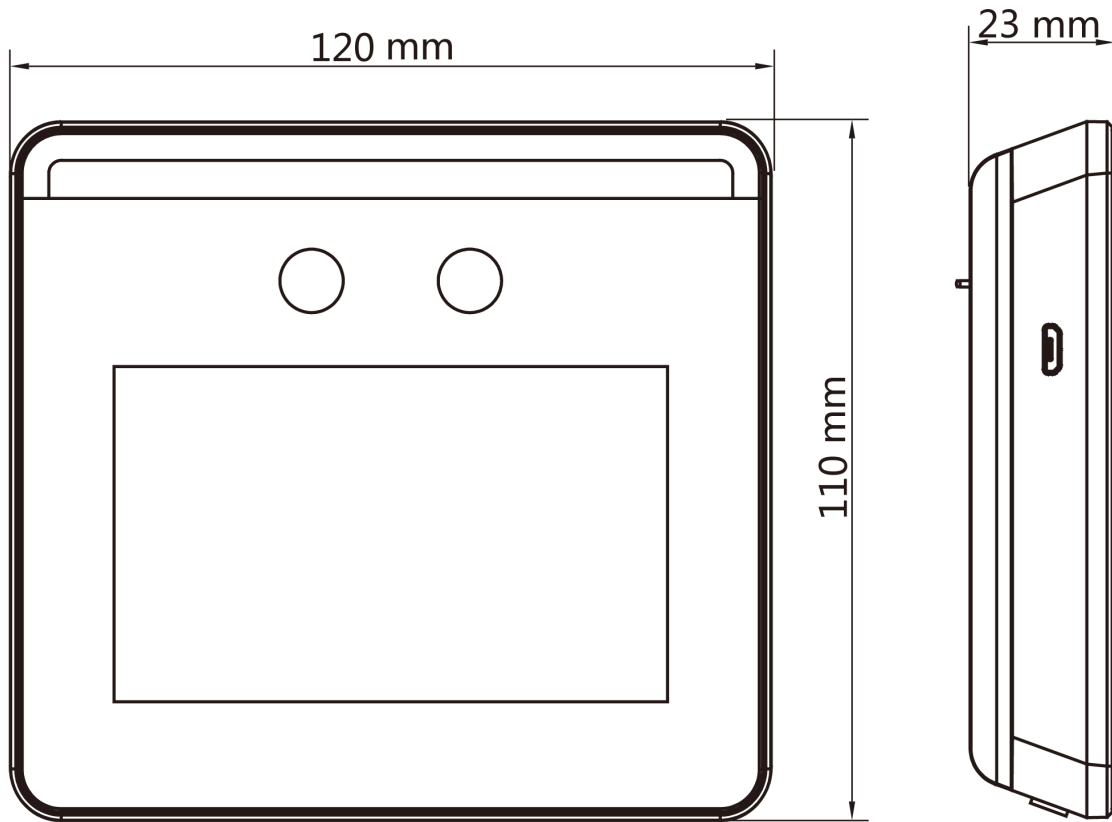


Indirect Light
through Window



Close to Light

Appendix C. Dimension



Appendix D. Communication Matrix and Device Command

Communication Matrix

Scan the following QR code to get the device communication matrix.

Note that the matrix contains all communication ports of Hikvision access control and video intercom devices.



Figure D-1 QR Code of Communication Matrix

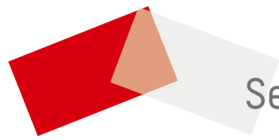
Device Command

Scan the following QR code to get the device common serial port commands.

Note that the command list contains all commonly used serial ports commands for all Hikvision access control and video intercom devices.



Figure D-2 Device Command



See Far, Go Further