



DS-K1A340 Series Face Recognition Terminal

User Manual

Legal Information

©2021 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 LATER 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:

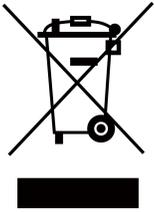
1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

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:

- In the use of the product, you must be in strict compliance with the electrical safety regulations of the nation and region.
- Do not connect several devices to one power adapter as adapter overload may cause over-heat or fire hazard.
- 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.
- The socket-outlet shall be installed near the equipment and shall be easily accessible.
- 1. Do not ingest battery. Chemical burn hazard!
 2. This product contains a coin/button cell battery. If the coin/button cell battery is swallowed, it can cause severe internal burns in just 2 hours and can lead to death.
 3. Keep new and used batteries away from children.
 4. If the battery compartment does not close securely, stop using the product and keep it away from children.
 5. If you think batteries might have been swallowed or placed inside any part of the body, seek immediate medical attention.
 6. CAUTION: Risk of explosion if the battery is replaced by an incorrect type.
 7. Improper replacement of the battery with an incorrect type may defeat a safeguard (for example, in the case of some lithium battery types).
 8. 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.
 9. 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.
 10. Do not subject the battery to extremely low air pressure, which may result in an explosion or the leakage of flammable liquid or gas.
 11. Dispose of used batteries according to the instructions.

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.
- Exposing the equipment to direct sun light, low ventilation or heat source such as heater or radiator is forbidden (ignorance can cause fire danger).
- 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).
- Please use a soft and dry cloth when clean inside and outside surfaces of the device cover, do not use alkaline detergents.
- Biometric recognition products are not 100% applicable to anti-spoofing environments. If you require a higher security level, use multiple authentication modes.
- The serial port of the equipment is used for debugging only.
- Install the equipment according to the instructions in this manual. To prevent injury, this equipment must be securely attached to the floor/wall in accordance with the installation instructions.
- 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.
- This bracket is intended for use only with equipped devices. Use with other equipment may result in instability causing injury.
- This equipment is for use only with equipped bracket. Use with other (carts, stands, or carriers) may result in instability causing injury.

Available Models

Product Name	Model
Face Time and Attendance Terminal	DS-K1A340X
	DS-K1A340FX
	DS-K1A340FWX
	DS-K1A340WX

Use only power supplies listed in the user instructions:

Model	Manufacturer	Standard
ADS-12FG-12N 12012EPG	Shenzhen Honor Electronic Co., Ltd	PG

Contents

Chapter 1 Overview	1
1.1 Overview	1
1.2 Features	1
Chapter 2 Appearance	2
Chapter 3 Installation	4
3.1 Installation Environment	4
3.2 Base Mounting	4
3.3 Install with Gang Box	5
Chapter 4 Device Wiring	8
Chapter 5 Activate via Device	9
Chapter 6 Quick Operation	10
6.1 Select Language	10
6.2 Set Application Mode	10
6.3 Privacy Settings	11
6.4 Set Administrator	11
Chapter 7 Basic Operation	14
7.1 Login	14
7.1.1 Login by Administrator	14
7.1.2 Login by Activation Password	15
7.1.3 Forget Password	16
7.2 Communication Settings	17
7.2.1 Set Wi-Fi Parameters	17
7.2.2 Platform Access	17
7.3 Local Time and Attendance	18
7.3.1 Attendance Process Description	18
7.3.2 Department Management	18

7.3.3 User Management	19
7.3.4 Shift Management	24
7.3.5 Manage Holiday (Add/Edit/Delete)	28
7.3.6 Shift Schedule	29
7.4 Time and Attendance Status Settings	31
7.4.1 Disable Attendance Mode via Device	31
7.4.2 Set Manual Attendance via Device	32
7.4.3 Set Auto Attendance via Device	33
7.4.4 Set Manual and Auto Attendance via Device	34
7.5 Data Management	35
7.5.1 Export Attendance Template	35
7.5.2 Export Attendance Summary Table/Abnormal Attendance Table	35
7.5.3 Import Face Picture	36
7.5.4 Export User Data/Access Control Parameters	37
7.6 Identity Authentication	37
7.6.1 Authenticate via Single Credential	38
7.6.2 Authenticate via Multiple Credential	38
7.7 Basic Settings	39
7.8 Set Biometric Parameters	40
7.9 System Maintenance	41
Chapter 8 Configure the Device via the Mobile Browser	44
8.1 Login	44
8.2 Search Event	44
8.3 Configuration	44
8.3.1 View Device Information	44
8.3.2 Time Settings	45
8.3.3 Set DST	46
8.3.4 View Open Source Software License	47

8.3.5 Network Settings	47
8.3.6 Set Time and Attendance via Mobile Web Browser	50
8.3.7 General Settings	57
8.3.8 Face Parameters Settings	59
Chapter 9 Operation via Web Browser	62
9.1 Login	62
9.2 Person Management	62
9.3 Search Event	63
9.4 Configuration	63
9.4.1 Set Local Parameters	63
9.4.2 View Device Information	64
9.4.3 Set Time	64
9.4.4 Set DST	64
9.4.5 View Open Source Software License	65
9.4.6 Upgrade and Maintenance	65
9.4.7 Security Mode Settings	66
9.4.8 Certificate Management	66
9.4.9 Change Administrator's Password	67
9.4.10 Online Users	68
9.4.11 View Device Arming/Disarming Information	68
9.4.12 Network Settings	68
9.4.13 Set Video and Audio Parameters	71
9.4.14 Customize Audio Content	71
9.4.15 Time and Attendance Settings	73
9.4.16 General Settings	75
9.4.17 Title: Local Time and Attendance Settings	77
9.4.18 Set Biometric Parameters	82
9.4.19 Set Theme	85

Chapter 10 Client Software Configuration	86
10.1 Configuration Flow of Client Software	86
10.2 Device Management	86
10.2.1 Add Device	87
10.2.2 Reset Device Password	89
10.2.3 Manage Added Devices	90
10.3 Group Management	90
10.3.1 Add Group	91
10.3.2 Import Resources to Group	91
10.4 Person Management	92
10.4.1 Add Organization	92
10.4.2 Import and Export Person Identify Information	92
10.4.3 Get Person Information from Access Control Device	95
10.4.4 Issue Cards to Persons in Batch	96
10.4.5 Report Card Loss	96
10.4.6 Set Card Issuing Parameters	96
10.5 Configure Schedule and Template	97
10.5.1 Add Holiday	98
10.5.2 Add Template	99
10.6 Set Access Group to Assign Access Authorization to Persons	100
10.7 Configure Advanced Functions	102
10.7.1 Configure Device Parameters	102
10.7.2 Configure Device Parameters	107
10.8 Door Control	110
10.8.1 Control Door Status	110
10.8.2 Check Real-Time Access Records	111
Appendix A. Tips for Installation Environment	115
Appendix B. Tips for Scanning Fingerprint	116

Appendix C. Tips When Collecting/Comparing Face Picture	118
Appendix D. Attendance Capacity	120
Appendix E. Attendance Report Table	121
Chapter 11 Dimensions	114
Appendix F. Communication Matrix and Device Command	125

Chapter 1 Overview

1.1 Overview

Face time and attendance terminal is a kind of access control device for face attendance. Face, fingerprint and other identity verification and are supported. It is mainly applied in security access control systems, such as buildings, enterprises, office buildings, financial outlets and key area protection.

1.2 Features

- Supports local time attendance and remote time attendance.
- 4.3-inch touch screen
- 2 MP wide-angle dual-lens
- Face anti-spoofing
- Face recognition distance: 0.3 m to 2 m
- Face recognition duration < 0.2 s/User; face recognition accuracy rate ≥ 99%
- Deep learning algorithm
- 1,500 face capacity
- Support 3000 fingerprints (supported by some models) and store 300,000 attendance records
- Support face, fingerprint, face or fingerprint or pin code, face + fingerprint, face + pin code, fingerprint + pin code, face + fingerprint + pin code authentication methods

 **Note**

Some devices support fingerprint authentication. Refers to the actual device for details.

-
- Export pictures, events, from the device to the USB flash drive
 - Manage, search and set device data after logging in the device locally
 - Support fill-in light function. The interface of the device is automatically brightened at night

Chapter 2 Appearance

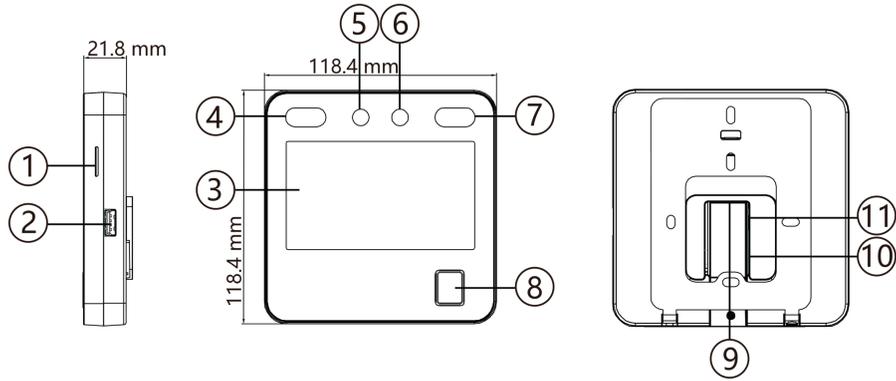


Figure 2-1 Appearance (With Fingerprint)

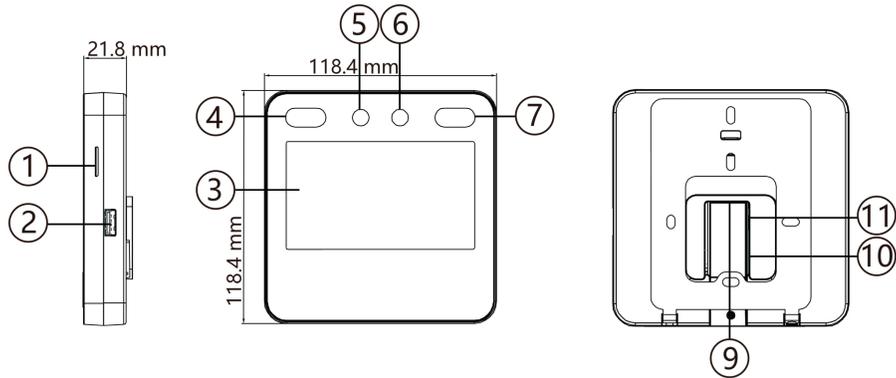


Figure 2-2 Appearance (Without Fingerprint)

Table 2-1 Appearance Description

No.	Name
1	Loudspeaker
2	USB Interface
3	Touch Screen
4	IR Light
5	Camera
6	Camera
7	IR Light
8	Fingerprint Module

No.	Name
	 Note Only devices that support the fingerprint function contain a fingerprint module.
9	Power Interface
10	Debugging Port 2
11	Debugging Port 1

 **Note**

The device requires special hardware to connect to the network.

Chapter 3 Installation

3.1 Installation Environment

- Install the device at least 2 meters away from the light, and at least 3 meters away from the window or the door.
- Make sure the environment illumination is more than 100 Lux.

 **Note**

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

3.2 Base Mounting

Steps

1. Route the cables through the cable hole of the bracket, and connect the terminals with peripherals cables. Place the bracket close to the back side of the device.

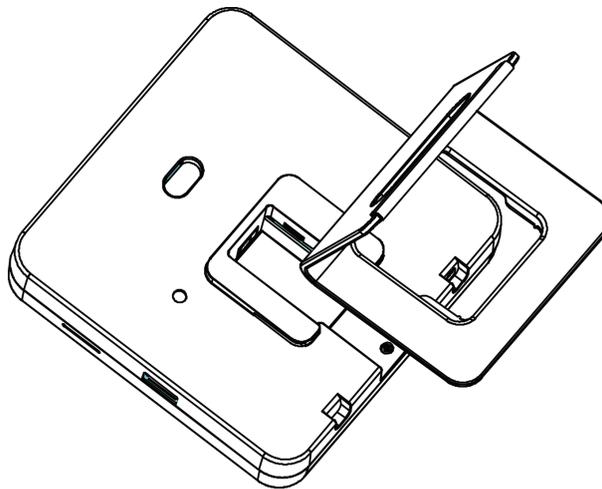


Figure 3-1 Place Bracket Close to Device Back Side

2. Press the bracket with both hands, and make sure that the buckle of the bracket fits with the back side of the device. Fasten the bracket in the direction of the arrow.

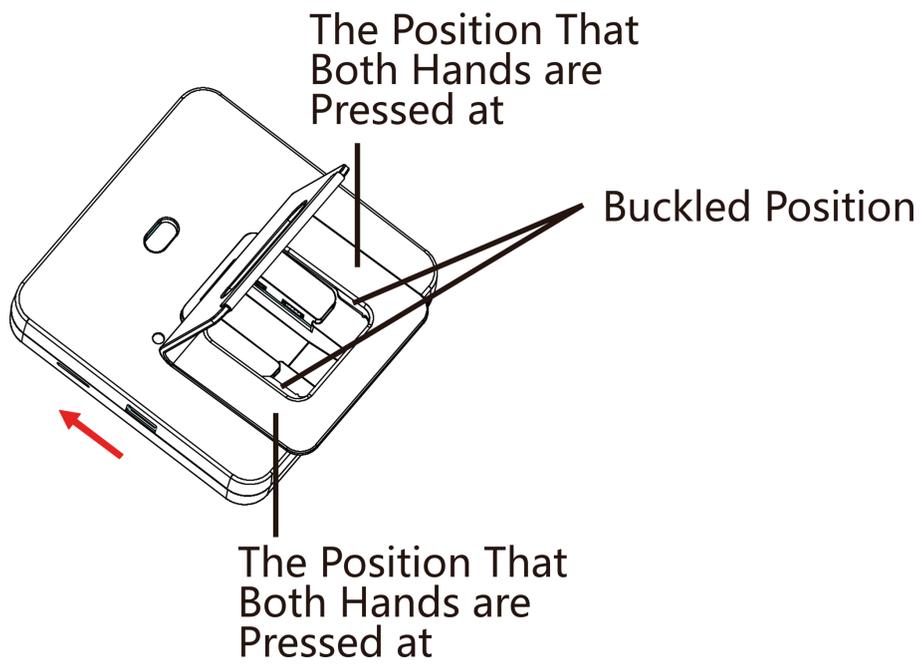


Figure 3-2 Fasten Bracket

3. Buckle into the bracket to the end to complete the installation.

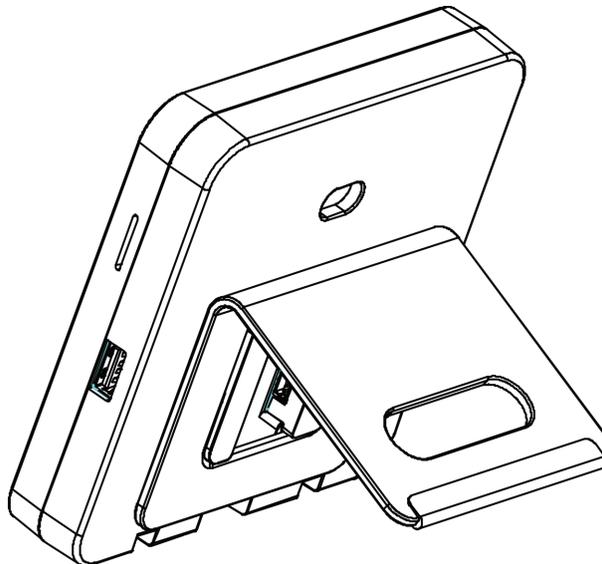


Figure 3-3 Complete Installation

3.3 Install with Gang Box

Steps

1. Make sure the gang box is installed on the wall.

 **Note**

You should purchase the gang box separately.

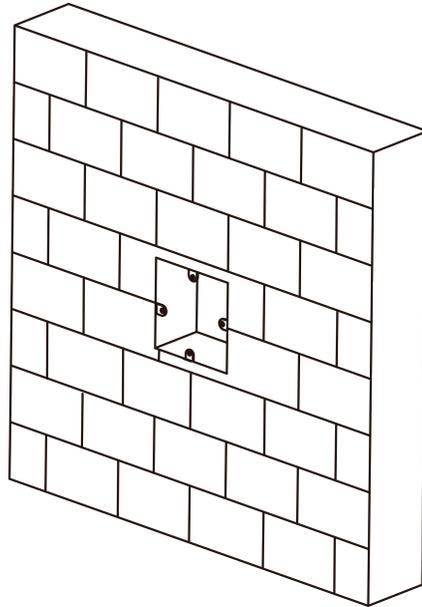


Figure 3-4 Install Gang Box

2. Use 4 supplied screws (M4) to secure the mounting plate on the gang box.

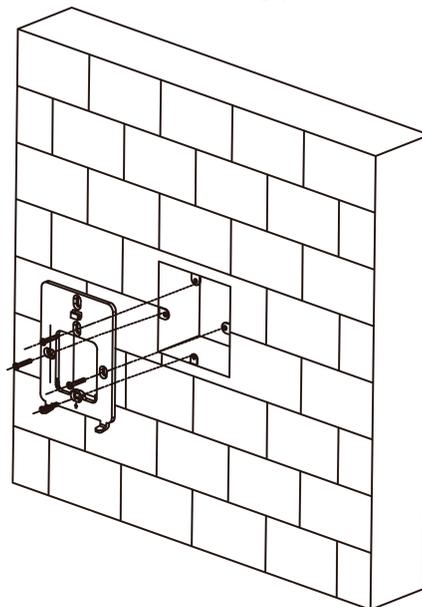


Figure 3-5 Install Mounting Plate

3. Route the cables through the cable hole of the mounting plate, and connect to the corresponding peripherals cables.
4. Buckle into the mounting plate after aligning the device with the mounting plate. Use 1 supplied screw (M3) to secure the device on the mounting plate.

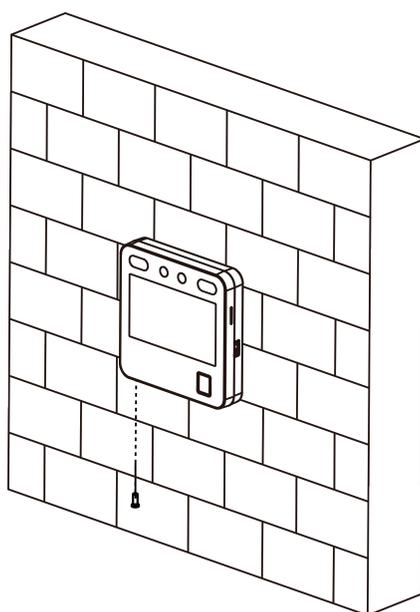


Figure 3-6 Secure Device

Chapter 4 Device Wiring

Connect the device to the power supply with the supplied power cable.

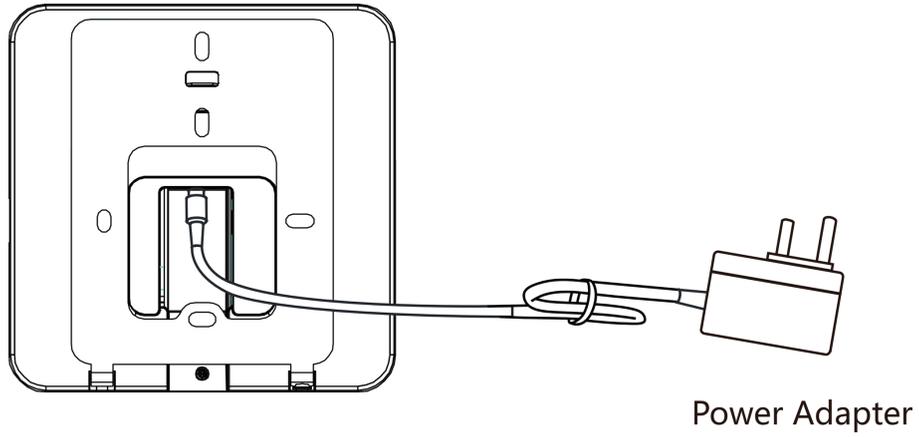


Figure 4-1 Device Wiring

Chapter 5 Activate via Device

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

After powering on, you will enter the QR code scanning page. Tap **Local**. On the Activate Device page, create a password and confirm the password. Tap **Activate** and the device will be activated.

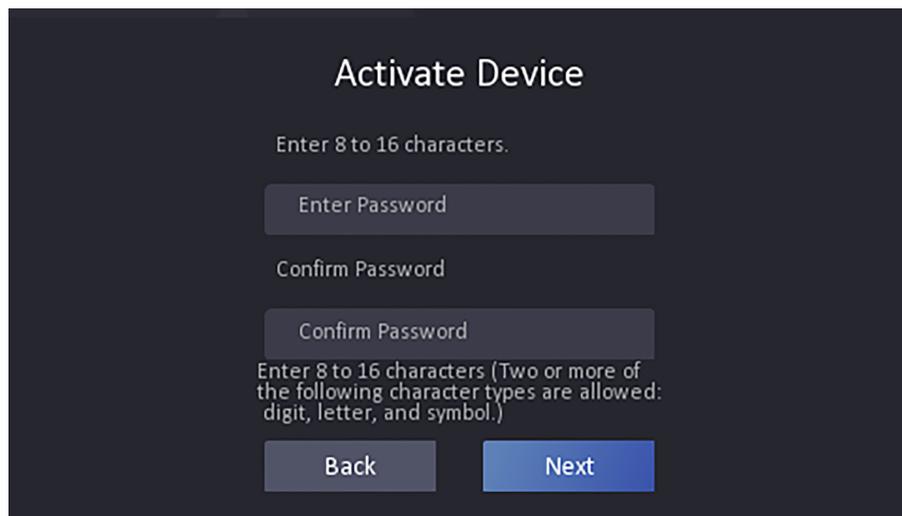


Figure 5-1 Activation Page

 **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.

-
- After activation, you should select a language according to your actual needs, see **Select Language** .
 - After activation, you should select an application mode. For details, see **Set Application Mode** .
 - After activation, if you need to set privacy, you should check the item. For details, see **Privacy Settings** .
 - After activation, if you need to add administrator to manage the device parameters, you should set administrator. For details, see **Add Administrator** .

Chapter 6 Quick Operation

6.1 Select Language

You can select a language for the device system.

After the device activation, you can select a language for the device system.

By default, the system language is English.

6.2 Set Application Mode

After activating the device, you should select an application mode for better device application.

Steps

1. On the Welcome page, select **Indoor** or **Others** from the drop-down list.

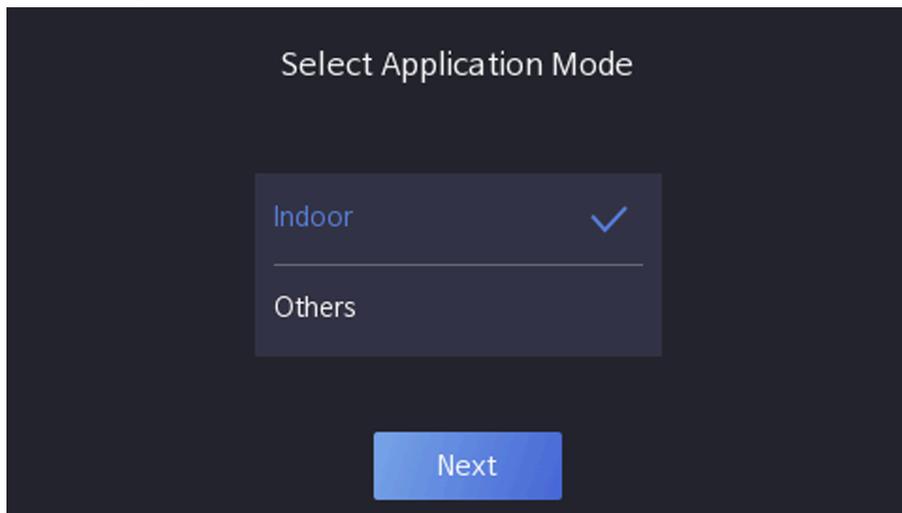


Figure 6-1 Welcome Page

2. Tap **OK** to save.

Note

- You can also change the settings in *System Settings*.
 - If you install the device indoors near the window or the face recognition function is not working well, select **Others**.
 - If you do not configure the application mode and tap **Next**, the system will select **Indoor** by default.
 - If you activate the device via other tools remotely, the system will select **Indoor** as the application mode by default.
-

6.3 Privacy Settings

After activation, selecting application mode, and selecting network, you should set the privacy parameters, including the picture uploading and storage.

Select parameters according to your actual needs.

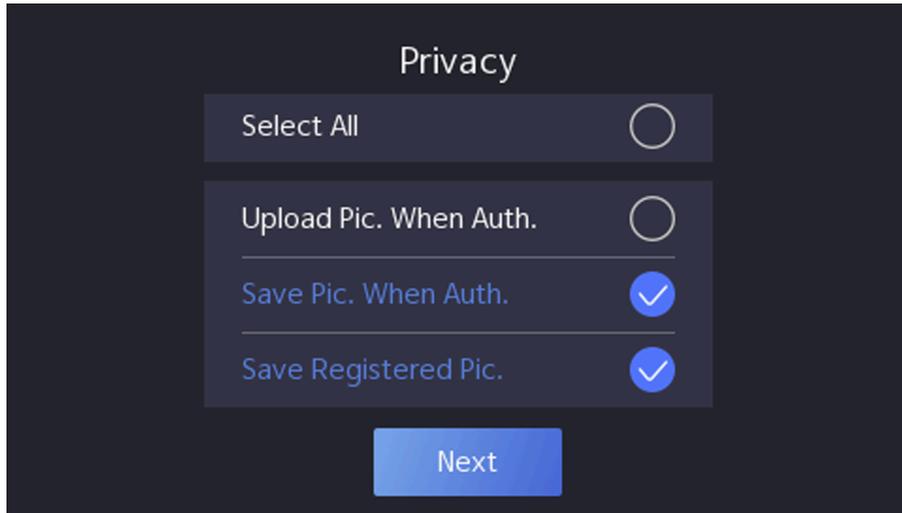


Figure 6-2 Privacy

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

Upload the pictures captured when authenticating to the platform automatically.

Save Captured 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.

6.4 Set Administrator

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

Steps

- 1. Optional:** Tap **Skip** to skip adding administrator if not required.
- 2.** Enter the administrator's name (optional) and tap **Next**.

 **Note**

Up to 5 administrators can be added.

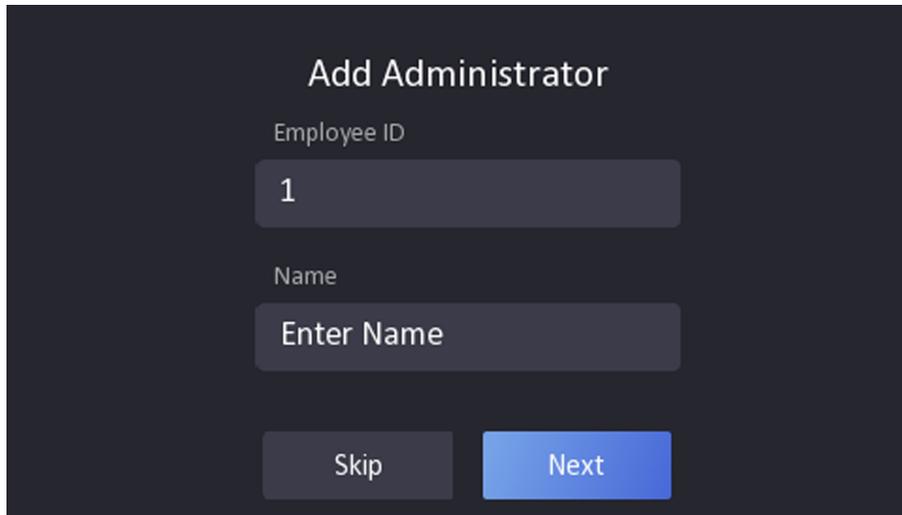


Figure 6-3 Add Administrator Page

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. Tap  to capture and tap  to confirm.
-  : Press your finger according to the instructions on the device screen. Tap  to confirm.

4. Tap 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 [**Basic Settings**](#).



Enter pin code 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, fingerprint to enter the home page.

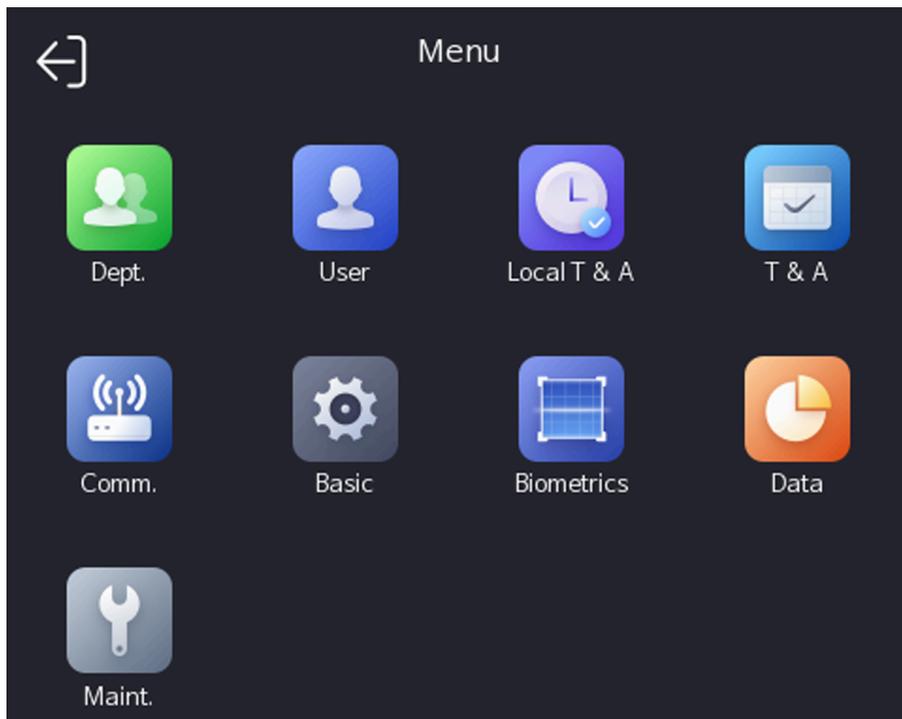


Figure 7-2 Home Page

 **Note**

The device will be locked for 30 minutes after 5 failed face, or fingerprint 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. Tap the Password field and enter the device activation password.
3. Tap **OK** to enter the home page.

 **Note**

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

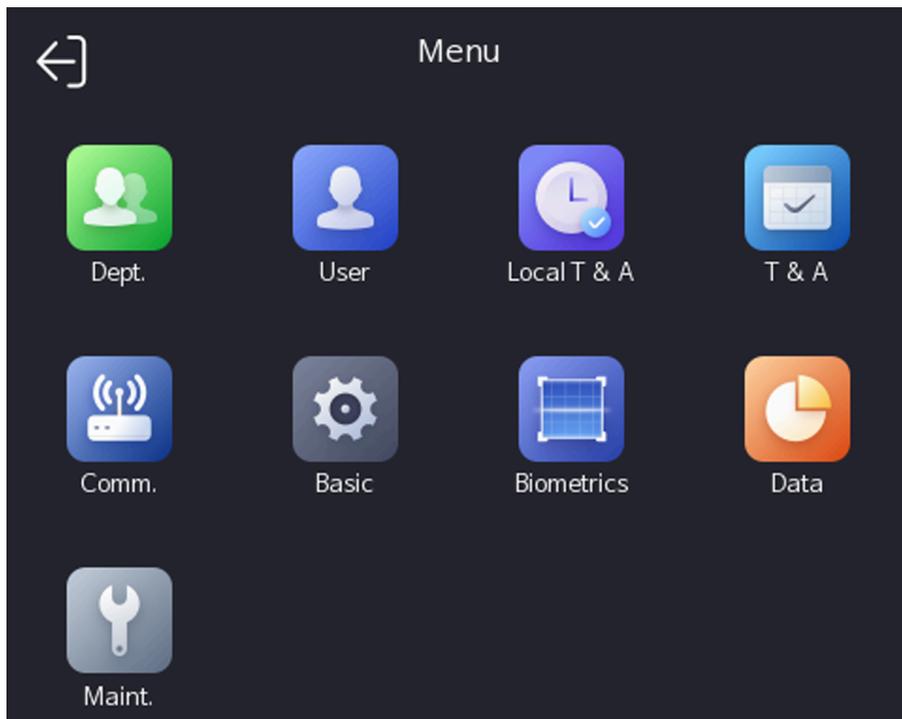


Figure 7-3 Home Page

7.1.3 Forget Password

If you forget the password during authentication, you can reset the password by importing the key.

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 page.
2. Tap  in the pop-up admin authentication page.
3. Tap **Forget Password** in the upper right corner of the page.
4. Plug USB flash drive into the USB interface.

Note

- The supported USB flash drive formats are FAT32 and exfat.
- The device supports 1 G to 32 G (including 1 G and 32 G) USB flash drive. Make sure that the free space of the USB flash drive is more than 512 M.

-
5. Tap **Export File**, and contact the technician to get the key, and enter the key in the export file.
 6. Tap **Import File** to import the file with the key to the device.
 7. Follow the prompts to reset the password.

7.2 Communication Settings

Support Wi-Fi, ISUP and remote configuraion via mobile browser.

7.2.1 Set Wi-Fi Parameters

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

Steps



Note

The function should be supported by the device.

1. Tap **Comm.** (Communication Settings) on the Home page to enter the Communication Settings page.
 2. On the Communication Settings page, tap **Wi-Fi**.
 3. Enable the Wi-Fi function.
 4. Configure the Wi-Fi parameters.
 - Select a Wi-Fi from the list, and enter the Wi-Fi's password. Tap **OK**.
 - If the target Wi-Fi is not in the list, tap **Add Wi-Fi**. Enter the Wi-Fi's name and password. And tap **OK**.
-



Note

- If the mobile phone remote configuration is enabled, the Wi-Fi function will be disabled.
 - 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.
-

7.2.2 Platform Access

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

Before You Start

Make sure your device has connected to a network.

Steps

1. Tap **Comm.** (Communication Settings) on the Home page to enter the Communication Settings page.

2. On the Communication Settings page, tap **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 Local Time and Attendance

Manage department, shift, holiday, schedule, and report.

You can add, edit, delete department/shift/holiday/schedule. You can also export the attendance report.

7.3.1 Attendance Process Description

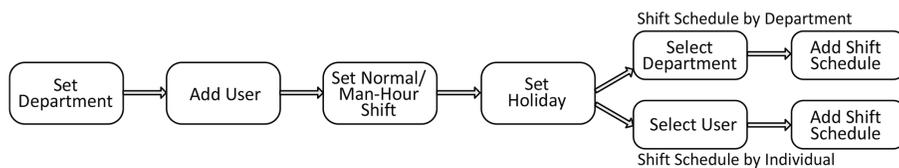


Figure 7-4 Attendance Process Description

7.3.2 Department Management

You can add, edit and delete the department.

Tap **Dept.** on the Home page to enter the settings page.

Add Department

Tap **+**, enter the department name, and tap **OK**.

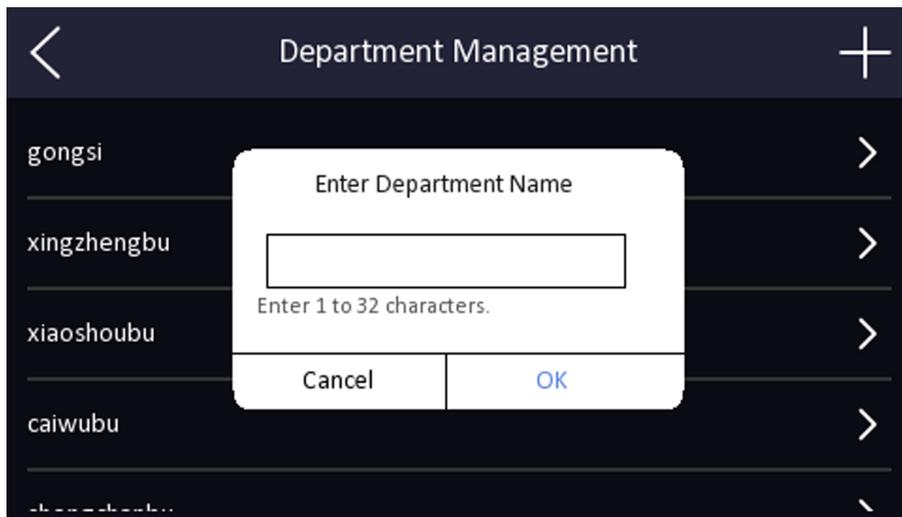


Figure 7-5 Add Department

 **Note**

- The department name supports uppercase English, lowercase English, numbers and symbols.
 - Up to 32 characters can be entered in department name.
 - There are 7 departments in the department management by default.
-

Edit Department

Tap the department that needs to be edited, to edit the settings.

You can edit the department name, and view employee information according to your actual needs.

Delete Department

Tap the department that needs to be deleted.

Tap , and tap **OK** to delete the department.

7.3.3 User Management

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

Add Administrator

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

Steps

1. Long tap on the initial page 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 enter the user name.

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. Select the department.

Note

For details about adding a department, see [*Manage Department via Mobile Web Browser*](#) .

6. **Optional:** Add a face picture, or fingerprints for the administrator.

Note

- For details about adding a face picture, see [*Add Face Picture*](#) .

-  Note

For details about adding a fingerprint, see [*Add Fingerprint*](#) .

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

Note

For details about setting the authentication type, see [*Set Authentication Mode*](#) .

8. Select the **User Role**.

9. Tap  to save the settings.

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.

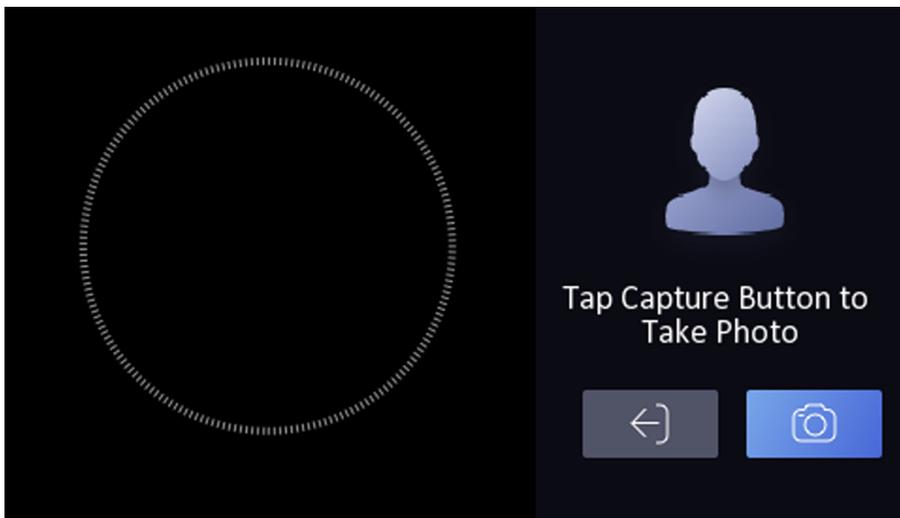


Figure 7-6 Add Face Picture

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.

Add Fingerprint

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

Steps

Note

- The function should be supported by the device.
 - Up to 3000 fingerprints can be added.
-

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.
 3. Tap the Employee ID. field and edit the employee ID.
-

Note

- The employee ID should be less than 32 characters. And it can be a combination of lower letters, upper letters, and numbers.
 - The employee ID should not start with 0 and should not be duplicated.
-
4. Tap the Name field and input the 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 Fingerprint field to enter the Add Fingerprint page.
 6. Follow the instructions to add a fingerprint.
-

Note

- The same fingerprint cannot be repeatedly added.
 - Up to 10 fingerprints can be added for one user.
 - You can also use the client software or the fingerprint recorder to record fingerprints.
For details about the instructions of scanning fingerprints, see ***Tips for Scanning Fingerprint*** .
-
7. 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.

8. Tap  to save the settings.

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.

Set Authentication Mode

After adding the user's face picture, PIN code, 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 the authentication mode.

Custom

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

4. Tap to save the settings.

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. Enter the employee ID, or the user name for searching. 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.



The employee ID cannot be edited.

7.3.4 Shift Management

The normal shift and the man-hour shift are available to be configured.

- Normal Shift: It is applicable to the normal attendance situation. You can set the attendance rule and the attendance checking times in the normal shift.
- Man-Hour Shift: It is applicable to the situation with flexible working hours.



Up to 256 shifts can be added.

Set Attendance Rule for Normal Shift

Set attendance rule before setting normal shift.

Tap **Local T&A** → **Shift Management** → **Normal Shift Management** → **Attendance Rule** to enter the page.



Figure 7-7 Attendance Rule

Set the attendance rule, including Advanced Check In Time, Latest Check In Time, Absence Time (Late), Earliest Check Out Time, Latest Check Out Time and Absence Time (Early Leave). After entering the duration, tap **OK** to save the settings.

Take the following picture as an example to describe the rules.

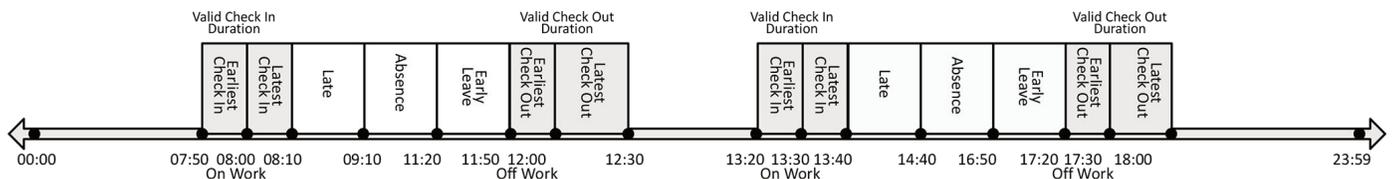


Figure 7-8 Attendance Rule Example

Advanced Check In Time

Set the earliest check in time. For example, if set the on work time as 8:00, and set the parameter as 10 min, the earliest check in time will be 7:50. Checking in at and earlier than 7:49 will be marked as invalid.

 **Note**

By default, if set as 0 min, the valid check in time starts from 00:00.

Latest Check In Time

Set the latest check in time. For example, if set the on work time as 8:00, and set the parameter as 10 min, the latest check in time will be 8:10. Checking in at and later than 8:11 will be marked as late or absence.

Late Time

The late time is N min after the latest check in time. For example, if set the latest check in time as 8:10, and set the parameter as 60 min, checking in at and later than 9:11 will be marked as absence. 8:10 to 9:10 will be marked as late.

Earliest Check Out Time

Set the earliest check out time. For example, set the off work time as 17:30 and set the parameter as 10 min, the earliest check out time will be 17:20. Checking out at or earlier than 17:19 will be marked as invalid.

Latest Check Out Time

Set the latest check out time. For example, set the off work time as 17:30 and set the parameter as 30 min, the latest check out time will be 18:00. Checking out at or later than 18:01 will be marked as invalid.



Note

By default, if set as 0 min, the valid check out time ends at 23:59:59.

Absence Time (Early Leave)

The early leave time is N min earlier than the check out time. For example, if set the earliest check out time as 17:20, and set the parameter as 30 min, checking out between 16:50 and 17:20 will be marked as early leave.



Note

- The unit is min.
 - The available time is from 0 to 1440 min.
-

Set Normal Shift

Edit or add the normal shift attendance information, including the shift name, the shift period, and the overtime shift period. You can also reset the normal shift after editing.

Before You Start

Set the attendance rule. For details, see [***Set Attendance Rule for Normal Shift***](#) .

Steps

1. Tap **Local T&A** → **Shift Management** → **Normal Shift Management** to enter the page.

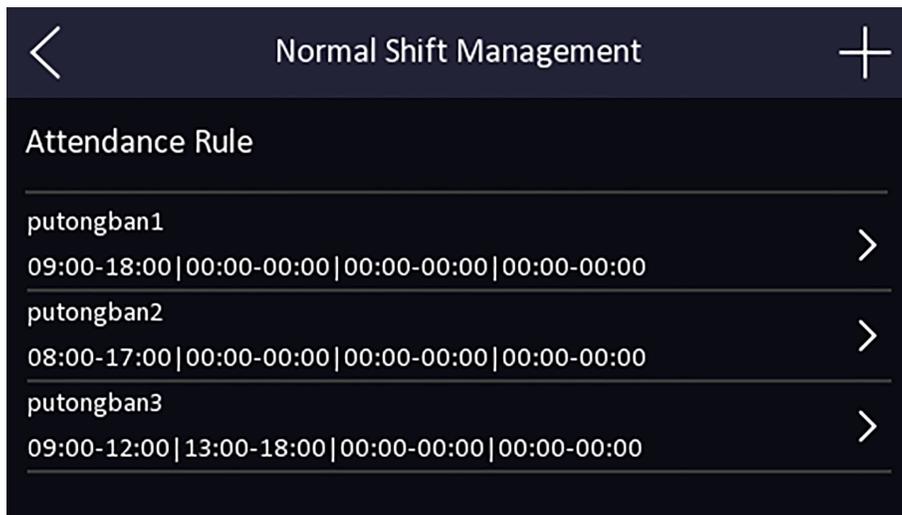


Figure 7-9 Normal Shift Management

2. Select a shift from the list to enter the Shift Details page.

 **Note**

By default, there are 3 configured normal shifts in the system.

3. Set the shift name and period in order and set the overtime shift period according to your needs.

 **Note**

- If the attendance rules conflict with the normal shift period, the device will prompt "Incorrect Time Duration". Delete all configured time durations and reset after exiting.
- The shift name supports numbers, uppercase letters, lowercase letters, Chinese characters and symbols.
- Up to 32 characters are allowed in the shift name.

4. Tap **OK** to save the settings.

5. **Optional:** Add shift.

- 1) Tap **+** in the upper right of the Normal Shift Management page to add shift.
- 2) Set shift name, start time and end time in order.
- 3) Tap  in the upper right of the add shift page to save the settings.

Set Man-Hour Shift

Set the man-hour shift parameters, including the shift name, the work duration, the latest on-work time, and the break time. You can also reset the man-hour shift after editing.

Steps

1. Tap **Local T&A** → **Shift Management** → **Man-Hour Shift Management** to enter the page.

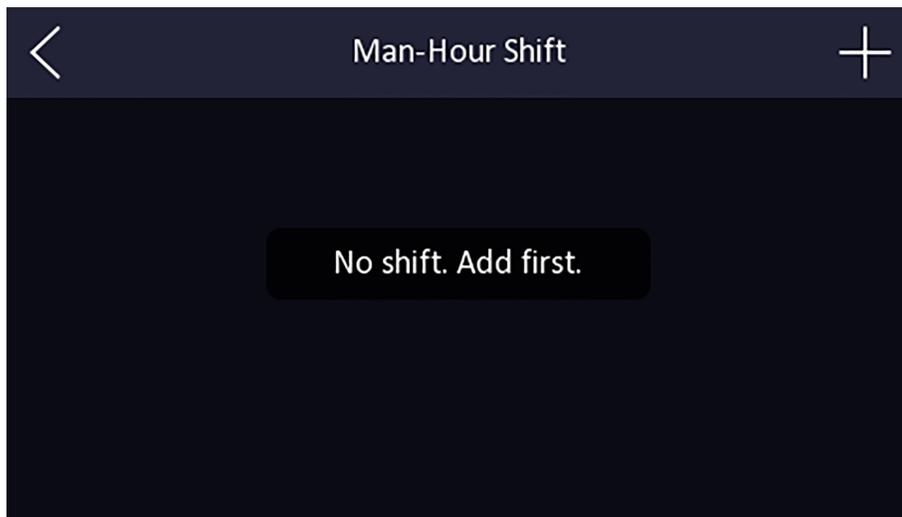


Figure 7-10 Man-Hour Shift

2. Tap + in the upper right of the Man-Hour Shift page to add the shift.
3. Set shift name, work duration, latest on-work time and add break time.

 **Note**

- Break time is not recorded as working duration.
- If the latest on-work time is set as 0, this feature is disabled by default.

-
4. Tap  in the upper right of the add shift page to save the settings.

7.3.5 Manage Holiday (Add/Edit/Delete)

Set the attendance holiday. The attendance will not be recorded during the holiday.

Add Holiday

Tap **Local T&A** → **Holiday Management** , and tap + in the upper right of the Holiday page to enter the Add Holiday page. Enter Holiday Name and set Holiday Duration, and tap  in the upper right of the Add Holiday page to save the settings.

Edit Holiday

Tap **Local T&A** → **Holiday Management** to enter the Holiday page. Select a holiday to enter the Holiday Details page to edit the holiday.

Delete Holiday

Tap **Local T&A** → **Holiday Management** to enter the Holiday page. Select a holiday to enter the Holiday Details page and tap  in the upper right of the Holiday Details page to delete the holiday.

7.3.6 Shift Schedule

Combine shift and holiday according to your actual needs. Scheduling shift by department and scheduling shift by individual are supported.

Schedule Shift by Department: All persons in the department use the same shift schedule to take attendance.

Schedule Shift by Individual: Take attendance according to individual's conditions.

Shift Schedule by Department

All persons in the department use the same shift schedule to take attendance.

Before You Start

- Edit department. For details, see [Department Management](#) .
- Set normal shift or man-hour shift. For details, see [Set Normal Shift](#) and [Set Man-Hour Shift](#) .
- Set the attendance holiday. For details, see [Manage Holiday \(Add/Edit/Delete\)](#) .

Steps

1. Tap **Local T&A → Shift Schedule by Department** to enter the Shift Schedule by Department page.
2. Select a department from the list to enter the Shift Schedule Details page.
3. Edit parameters.

Department Name

The department name should be edited in Dept. management page. For details, see [Department Management](#) .

Employee

You can see employees in the department.

Add Shift Schedule

You can add shift schedules and set shift schedule of each shift schedule and shift type of shift on Monday to Sunday.



Note

Up to 8 shift schedules can be added and each shift schedule time can not be overlapped with other shift schedule time.

Holiday Settings

Tap holiday settings and tap in the upper right of the Holiday Settings page. After saving the settings, the attendance will not be recorded during the holiday.

4. Tap to save the settings.

Shift Schedule by Individual (Add/Edit/Delete)

Take attendance according to individual's conditions.

Before You Start

- Add user before setting shift schedule by individual. For details, see [User Management](#) .
- Set normal shift or man-hour shift. For details, see [Set Normal Shift](#) 和 [Set Man-Hour Shift](#) .
- Set the attendance holiday. For details, see [Manage Holiday \(Add/Edit/Delete\)](#) .

Steps

Note

The shift schedule by individual has higher priority than shift schedule by department. If a user has configured both shift schedule by department and by individual, the system will take attendance according to shift schedule by individual first.

1. Tap **Local T&A** → **Shift Schedule by Individual** to enter the Shift Schedule by Individual page.

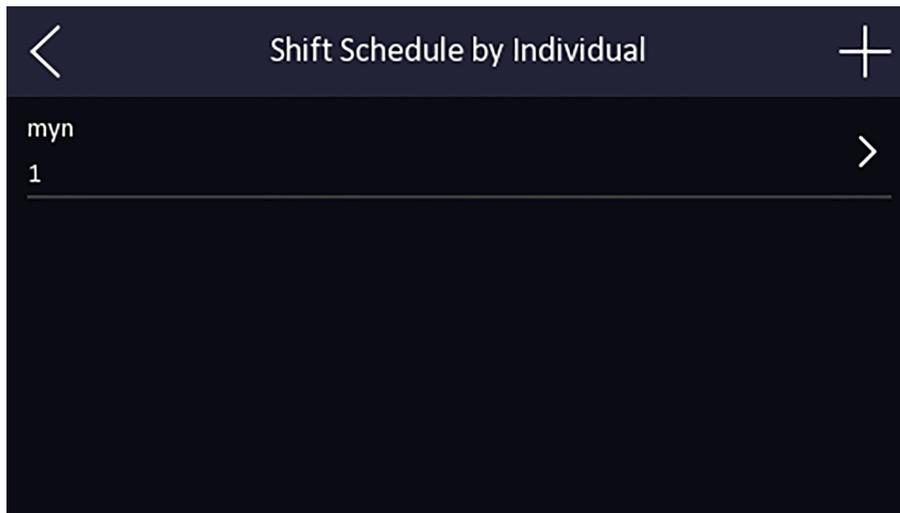


Figure 7-11 Shift Schedule by Individual

2. Tap + in the upper right of the Shift Schedule by Individual page to add Shift Schedule by Individual.
3. Select a person from the list to enter the Shift Schedule Details page.
4. Edit parameters.

Add Shift Schedule

You can add shift schedules and set shift schedule of each shift schedule and shift type of shift on Monday to Sunday.

Note

Up to 8 shift schedules can be added and each shift schedule time can not be overlapped with other shift schedule time.

Holiday Settings

Tap **Holiday Settings** in the Holiday Settings page. After saving the settings, the attendance will not be recorded during the holiday.

5. Tap to save the settings.
6. **Optional:** Select an individual in the Shift Schedule by Individual page and edit the shift schedule.
7. **Optional:** Select an individual you want to delete in the Shift Schedule by Individual page, and tap  in the upper right of the Shift Schedule by Individual page to delete the shift schedule.

7.4 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.

7.4.1 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.

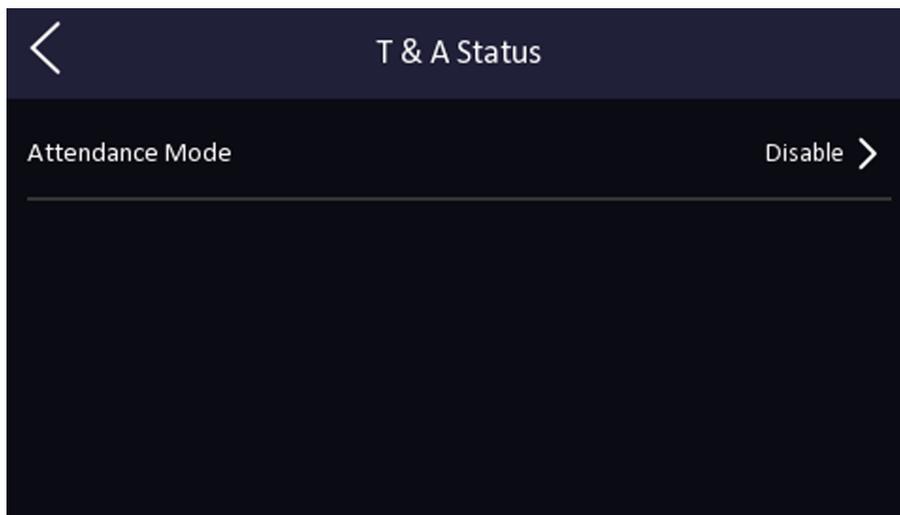


Figure 7-12 Disable Attendance Mode

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.

7.4.2 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**.

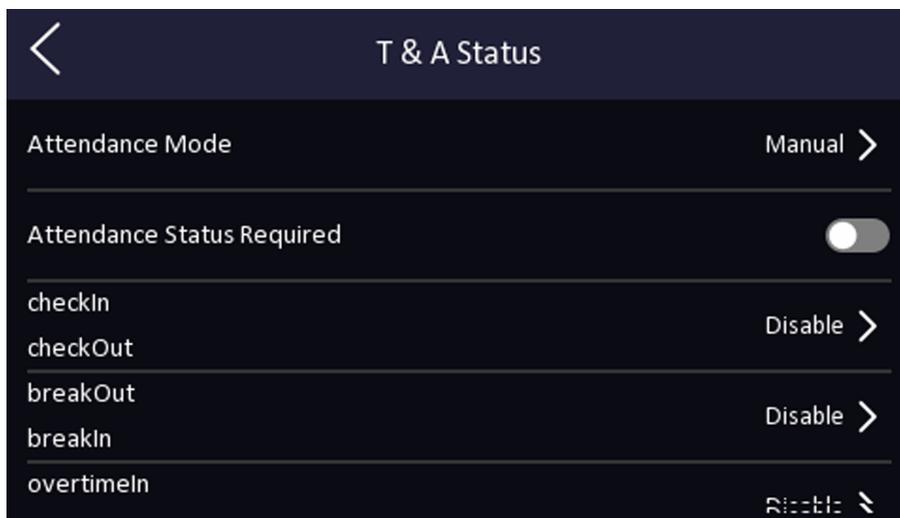


Figure 7-13 Manual Attendance Mode

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.

7.4.3 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**.

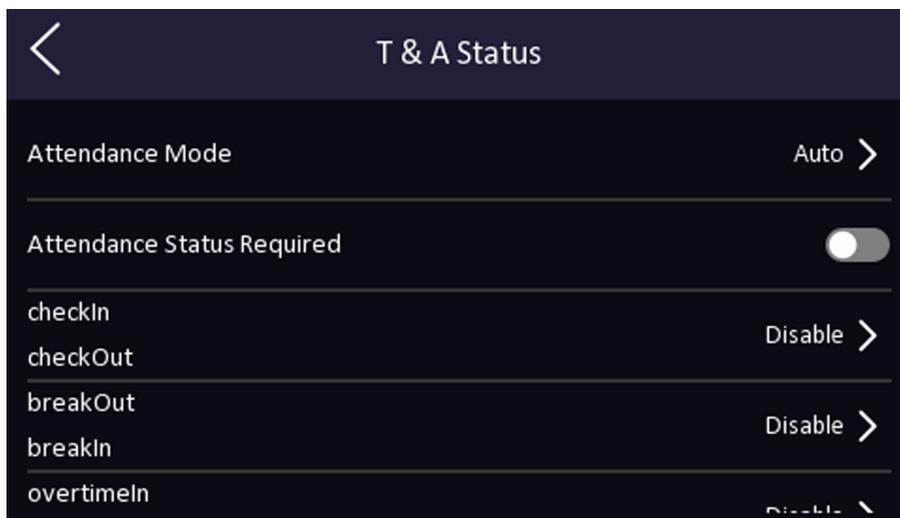


Figure 7-14 Auto Attendance Mode

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.

7.4.4 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**.

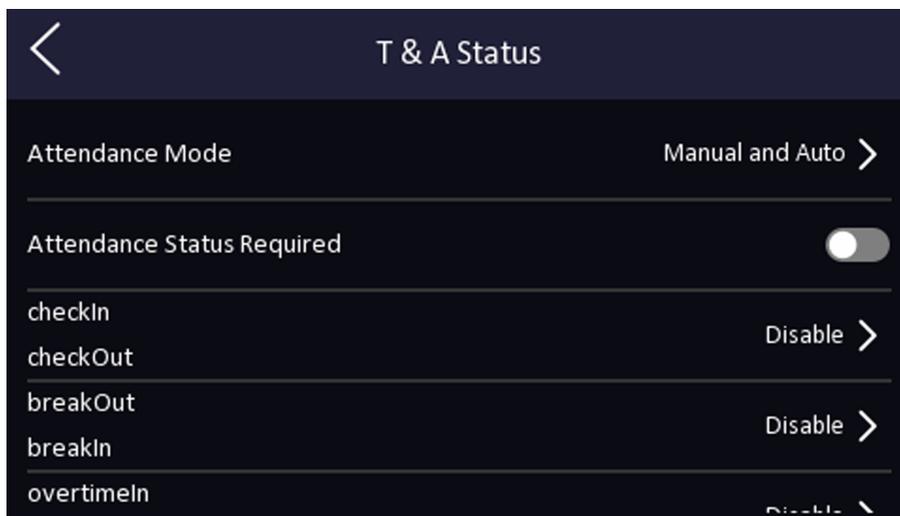


Figure 7-15 Manual and Auto Mode

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

Note

The Attendance Property will not be changed.

5. **Optional:** Select an status and change its name if required.

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

6. Set the status' schedule.

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



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.

7.5 Data Management

You can import user data, face data, access control parameters, and export attendance summary table, abnormal attendance table, attendance template, user data, face data, and access control parameters.

7.5.1 Export Attendance Template

Steps

1. Plug a USB flash drive in the device.



- The supported USB flash drive format is FAT32 and exfat.
- The system supports the USB flash drive with the storage of 1 G to 32 G. Make sure the free space of the USB flash drive is more than 512 M.

-
2. Tap **Data** → **Import Data** → **Attendance Template** .
 3. Set the start date and end date.
 4. Tap **OK** to export the attendance template.

7.5.2 Export Attendance Summary Table/Abnormal Attendance Table

You can export attendance summary table and abnormal attendance table.

Steps

1. Plug a USB flash drive in the device.

Note

- The supported USB flash drive format is FAT32 and exfat.
- The system supports the USB flash drive with the storage of 1 G to 32 G. Make sure the free space of the USB flash drive is more than 512 M.

2. Tap **Data** → **Export Data** → **Attendance Summary Table/Abnormal Attendance Table** .

3. Tap the table that needs to be exported.

Note

- You need to enter the start date and end date when exporting attendance summary table/ abnormal attendance table.
- For exported table content details, see ***Attendance Report Table*** .

Result

The exported content will be stored in the USB flash drive in Excel format.

7.5.3 Import Face Picture

Face pictures can be imported into the device through a USB flash drive. You can also export the pictures from one device and import them into other devices.

Steps

1. Import the external face pictures through a USB flash drive directly.

- 1) Plug a USB flash drive in the device.

Note

- The supported USB flash drive format is FAT32 and exfat.
- The system supports the USB flash drive with the storage of 1 G to 32 G. Make sure the free space of the USB flash drive is more than 512 M.

- 2) Tap **Data** → **Import Data** → **Face Data** .

- 3) Enter the password when importing the face data, and tap **OK**.

Note

The pictures are stored in the enroll_pic folder in the root directory of the USB flash drive.

2. Export the pictures from one device and import them into other devices.

- 1) Tap **Data** → **Export Data** → **Face Data** .

- 2) Enter the password when exporting face data.

Note

The pictures are stored in the enroll_pic folder in the root directory of the USB flash drive.

- 3) Store the exported pictures in the export_pic folder in the root directory of the USB flash drive.
- 4) Tap **Data** → **Import Data** → **Face Data** .
- 5) Enter the password when importing the face data, and tap **OK**.

Note

- The picture size cannot be larger than 200 KB, and the picture format supports .jpg, 24 bit .bmp, or .png formats. The format of the picture imported by the user is: Employee ID_Name_Department_Gender.jpg, where gender can be represented by 0 or 1, and male is 0 and female is 1.
 - Non-encrypted or encrypted importing/exporting are supported.
-

7.5.4 Export User Data/Access Control Parameters

You can export user data and access control parameters.

Steps

1. Plug a USB flash drive in the device.

Note

- The supported USB flash drive format is FAT32 and exfat.
 - The system supports the USB flash drive with the storage of 1 G to 32 G. Make sure the free space of the USB flash drive is more than 512 M.
-
2. Tap **Data** → **Export Data** → **User Data/Access Control Parameters** .
 3. Tap **User Data** or **Access Control Parameters**.
 4. Enter the password when importing the user data/access control parameters, and tap **OK**.

Note

- You can export the imported data to iVMS-4200.
 - Non-encrypted or encrypted importing/exporting are supported.
 - Please refer to for exported table content.
-

Result

The exported content will be stored in the USB flash drive in Excel format.

7.6 Identity Authentication

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

7.6.1 Authenticate via Single Credential

Set the user authentication type before authentication. For details, see [Set Authentication Mode](#) .
Authenticate face, fingerprint, card or QR code.

Face

Face forward at the camera and start authentication via face.

Fingerprint

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

PIN Code

Enter the PIN code to authenticate via PIN code.



Note

PIN code should be configured in the platform.

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

7.6.2 Authenticate via Multiple Credential

Before You Start

Set the user authentication type before authentication. For details, see [Set Authentication Mode](#) .

Steps

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



Note

- Some devices support fingerprint authentication. Refers to the actual device for details.
- Support, face + fingerprint, face + pin, fingerprint + pin, face + fingerprint + pin authentication methods.

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



Note

- For detailed information about scanning fingerprint, see *Tips for Scanning Fingerprint*.
 - For detailed information about authenticating face, see *Tips When Collecting/Comparing Face Picture*.
-

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

7.7 Basic Settings

You can set the shortcut key, theme, voice, time, sleeping (s), wait to Logout (s), language.

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**.

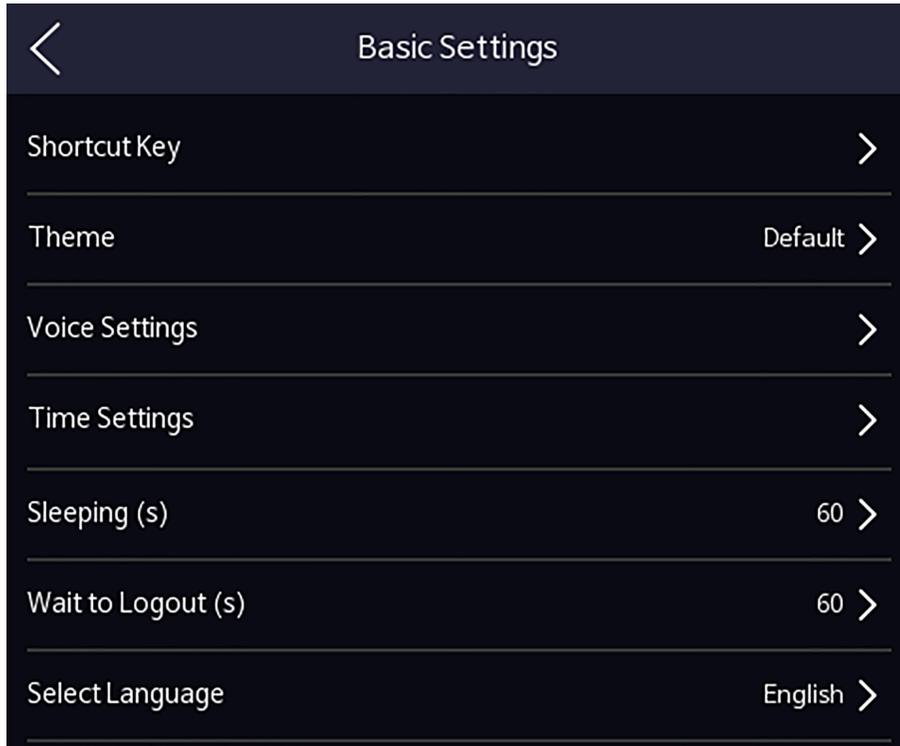


Figure 7-16 Basic Settings Page

Shortcut Key

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

Theme

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

Voice 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 (minute). When you are on the initial page and if you set the sleeping time to 30 min, the device will sleep after 30 min without any operation.

 **Note**

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

Wait to Logout (s)

If there is no operation within the configured time, the system will logout.

Language

Select the language according to actual needs.

 **Note**

After changing the language, the device will reboot.

7.8 Set Biometric Parameters

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

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

Table 7-1 Face Picture Parameters

Parameter	Description
Application Mode	Select either others or indoor according to actual environment.
Face Liveness Level	After enabling face anti-spoofing function, you can set the matching security level when performing live face authentication.
Face 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.

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.
Face 1:1 Security Level	Set the matching threshold when authenticating via 1:1 matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate.
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 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 (1:1)</p> <p>Set the matching threshold when authenticating via ECO mode 1:1 matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate.</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>
Multiple Faces Authentication	After multiple faces authentication is enabled, multiple faces authentication is supported.

7.9 System Maintenance

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

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

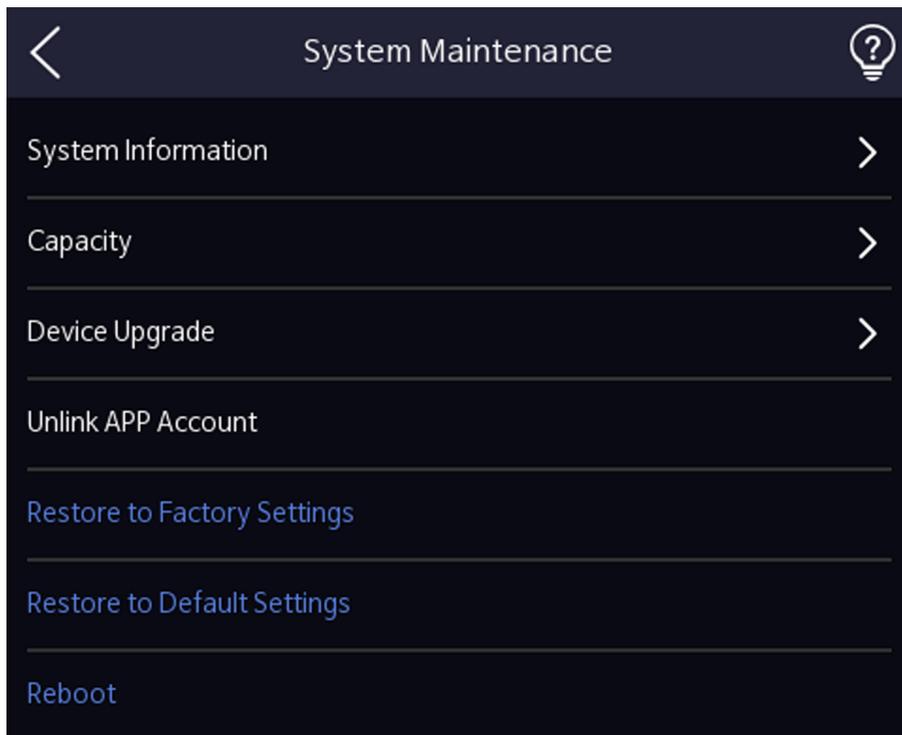


Figure 7-18 Maintenance Page

System Information

You can view the device information including serial No., firmware version, MCU version, MAC address, production data, device QR code, 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 administrator, user, face picture, card, and event.

Note

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

Device Upgrade

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

Unlink APP Account

Unlink the Hik-Connect account from the platform.

Restore to Factory Settings

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

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.

Reboot

The device will reboot after the confirmation.



Long tap , and enter admin password to view device version information.

Chapter 8 Configure the Device via the Mobile Browser

8.1 Login

You can login via mobile browser.



- Parts of the model supports Wi-Fi settings.
- Make sure the device is activated.

Obtain the IP address from the device after Wi-Fi is enabled. Make sure the IP segment of the device and the computer is the same. For details, refers to ***Set Wi-Fi Parameters*** .

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

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

8.2 Search Event

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

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



Support searching for names within 32 digits.

The results will be displayed in the list.

8.3 Configuration

8.3.1 View Device Information

You can view the device name, device No., language, model, serial No., version, device capacity, etc.

Tap **Configuration** → **System** → **System Settings** → **Basic Information** , to enter the settings page.

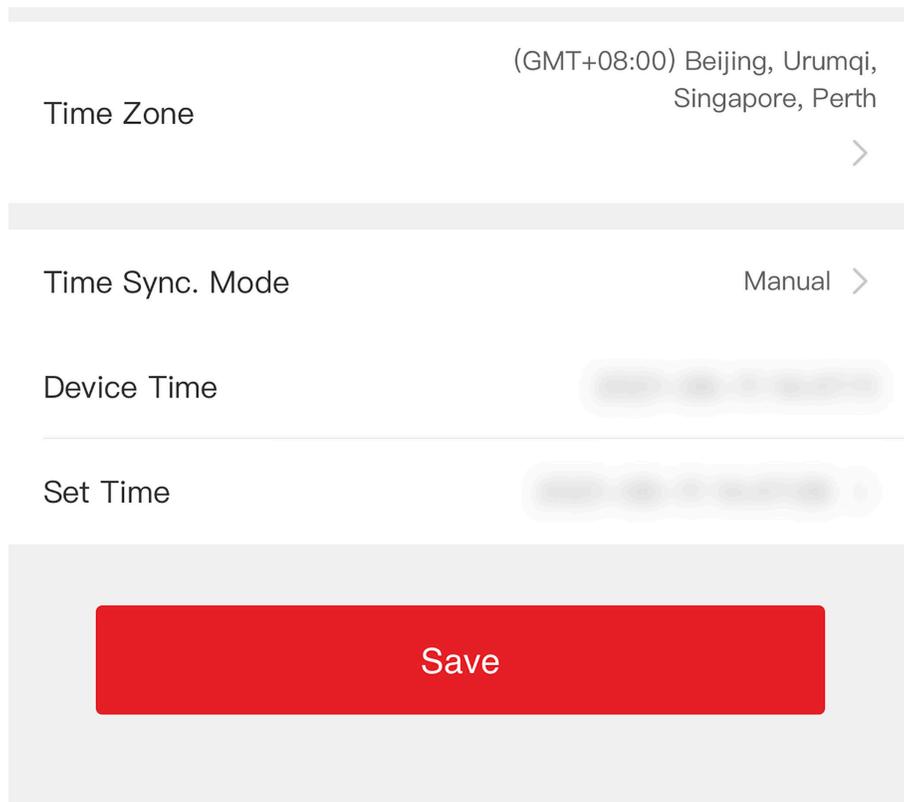


Figure 8-2 Time Settings

Tap **Save** to save the settings.

Time Zone

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

Time Sync. Mode

Manual

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

NTP

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

8.3.3 Set DST

Steps

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

Enable DST

Start Time Apr First Sunday 02h

Month Apr >

Week First >

Weekday Sunday >

Time 02 >

End Time Oct Last Sunday 02h

Month Oct >

Week Last >

Weekday Sunday >

DST Bias 30minute(s) >

Save

Figure 8-3 DST

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

8.3.4 View Open Source Software License

Tap **Configuration** → **System** → **System Settings** → **About** , and tap **View Licenses** to view the device license.

8.3.5 Network Settings

You can set the port and Wi-Fi parameters.

Set Port Parameters

You can set the HTTP, RTSP, HTTPS, and Server according to actual needs when accessing the device via network.

Tap **Configuration** → **Network** → **Basic Settings** → **Port** , to enter the settings page.

HTTP

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

RTSP

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

HTTPS

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

Server

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

Set Wi-Fi Parameters

Set the Wi-Fi parameters for device wireless connection.

Steps



Note

The function should be supported by the device.

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



Note

If Wi-Fi is enabled, the AP will be disabled automatically.

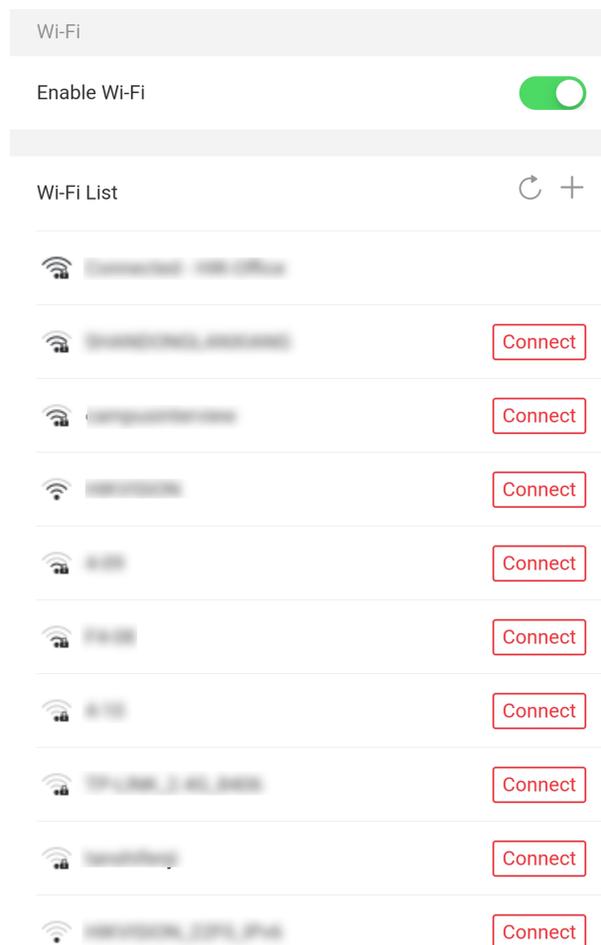


Figure 8-4 Wi-Fi

3. Add Wi-Fi.

1) Tap +.

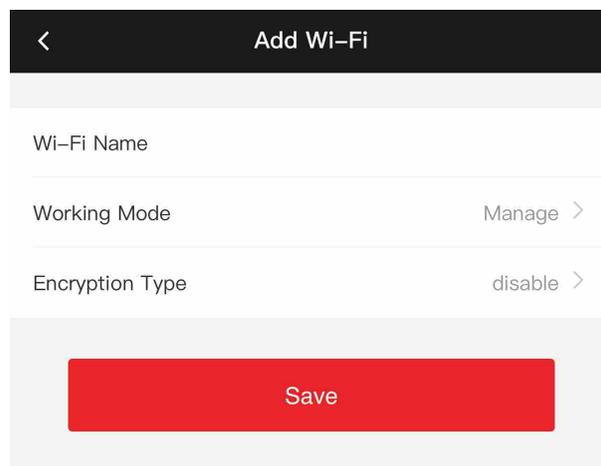


Figure 8-5 Add Wi-Fi

2) Enter **Wi-Fi Name** and **Wi-Fi Password**, and select **Working Mode** and **Encryption Type**.

- 3) Tap **Save**.
4. Select the Wi-Fi name, and tap **Connect**.
5. Enter the password and tap **Save**.
6. Set WLAN parameters.
 - 1) Set the IP address, subnet mask, and gateway. Or enable DHCP and the system will allocate the IP address, subnet mask, and gateway automatically.
 - 2) Tap **Save**.

8.3.6 Set Time and Attendance via Mobile Web Browser

You can set time and attendance by managing department, user, shift, holiday, and shift schedule. You can add, edit, and delete attendance department, user, shift, holiday, and shift schedule.

Manage Department via Mobile Web Browser

You can add, edit and delete the department.

Steps

1. Tap **Configuration** → **Time and Attendance** → **Department Management** to enter the settings page.
2. Add the department.
 - 1) Tap **+**.

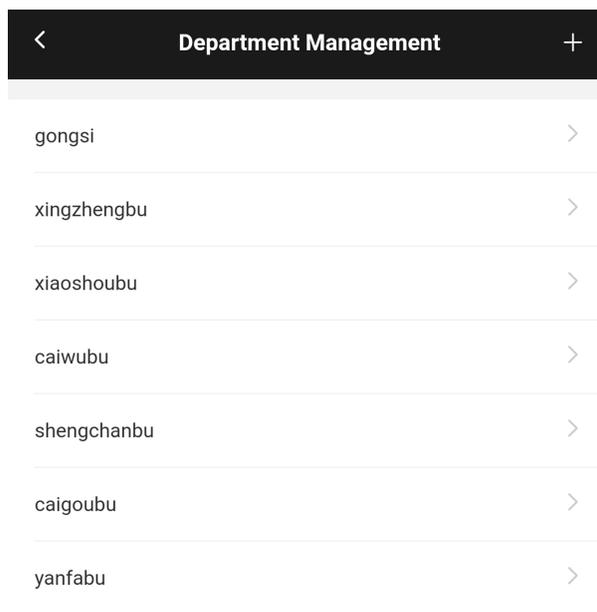


Figure 8-6 Add Department

- 2) Enter the department name, and tap **OK**.



Note

- The department name supports uppercase English, lowercase English, numbers and symbols.
- Up to 32 characters can be entered in department name.
- There are 7 departments in the department management by default.

3. Optional: You can view employee according to your actual needs.

4. Delete the department.

- 1) Tap the department that needs to be deleted.
- 2) Tap , and tap **OK** to delete the department.

User Management

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

Steps

- 1.** Tap **User** to enter the settings page.
- 2.** Add user.
 - 1) Tap+.

The screenshot shows a mobile application interface for editing a person's profile. The title bar is black with a back arrow on the left, 'Edit Person' in the center, and a trash icon on the right. The form fields are as follows:

*Employee ID	1
Name	
Gender	none >
User Role	Normal User >
Floor No.	0
Room No.	0
Face	0 >
Fingerprint	1 >
Start Date	2000-01-01 >
End Date	2037-12-31 >
Administrator	<input checked="" type="checkbox"/>
Authentication Settings	
Authentication Type	The Same Device >

A large red button labeled 'Save' is positioned at the bottom of the form.

Figure 8-7 Add User

2) Set the following parameters.

Employee ID

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

Name

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

Gender

Select the gender.

User Role

Select your user role.

Floor No./Room No.

Enter the floor No./room No.

Face

Add Face picture. Tap **Face**, then tap **Import**, and select the mode to import the face.

Fingerprint

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

Start Date/End Date

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

Administrator

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

Authentication Type

Set the authentication type.

3) Tap **Save**.

3. Tap the user that needs to be edited in the user list to edit the information.

4. Tap the user that needs to be deleted in the user list, and tap  to delete the user.

5. You can search the user by entering the employee ID or name in the search bar.

Manage Shift via Mobile Web Browser

You can set the normal shift and man-hour shift. Normal shift can be applied in attendance scenarios of regular attendance, and you can set the attendance rules and the attendance number. Man-hour shift can be applied in the attendance scenarios of flexible working system.

Manage Normal Shift via Mobile Web Browser

You can edit and add normal shift attendance information, including shift name and attendance duration.

Steps

1. Set attendance rules.

1) Tap **Configuration** → **Time and Attendance** → **Shift Management** → **Normal Shift Management**.

2) Tap **Attendance Rule**.

3) Set advanced check in time, latest check in time, absence time(late), earliest check out time, latest check out time, and absence time(early leave).



Note

- The time unit is minute.
- The configurable time range is from 0 to 1440 minutes (including 0 and 1440).

4) Tap **Save**.

2. Set normal shift.

1) Tap **Configuration** → **Time and Attendance** → **Shift Management** → **Normal Shift Management** .

2) Tap a normal shift to enter the settings page.

 **Note**

3 normal shifts has been configured by default.

3) Set the shift name, the start time and end time of the attendance duration.

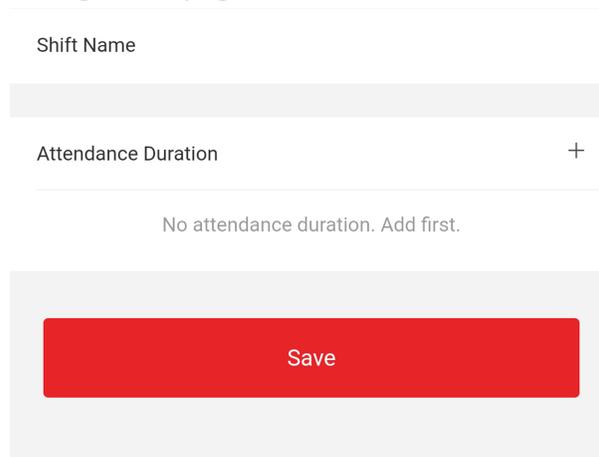
 **Note**

- If the attendance rules conflict with the normal shift durations, the device will prompt "Duration error". Please delete all durations and reconfigure the settings after exiting.
- The shift name supports Chinese, uppercase English, lowercase English, numbers and symbols.
- Up to 32 characters can be entered in shift name.

4) Tap **Save**.

3. Optional: Add the shift.

1) Tap **+** in normal shift management page.



Shift Name

Attendance Duration +

No attendance duration. Add first.

Save

Figure 8-8 Add Shift

2) Set the shift name, the start time and end time of the attendance duration.

3) Tap **Save**.

Manage Man-Hour Shift via Mobile Web Browser

You can edit the shift name, work duration, latest on-work time, and break time.

Steps

1. Tap **Configuration** → **Time Attendance** → **Shift Management** → **Man-Hour Shift Management** .

2. Tap **+**.

3. Edit the shift name, work duration, latest on-work time, and break time.

Note

- Break time is not recorded in working time.
 - If the latest work time is set to 0, this function is not enabled by default.
-

4. Tap **Save**.

Manage Holiday via Mobile Web Browser

There is no attendance during the holidays.

Steps

1. Add the holidays.
 - 1) Tap **Configuration** → **Time and Attendance** → **Holiday Management** , to enter the settings page.
 - 2) Tap **+** to enter the settings page. Enter **Holiday Name**, **Start Date** and **End Date**, and tap **Save**.
2. Edit the holidays. Tap **Configuration** → **Time and Attendance** → **Holiday Management** to enter the settings page. Tap the holiday to edit the settings.
3. Delete the holidays. Tap **Configuration** → **Time and Attendance** → **Holiday Management** , tap the holiday to enter the settings page, and tap  to delete the holiday.

Manage Shift Schedule via Mobile Web Browser

You can combine the shift and holiday according to your actual needs. Shift schedule by department and shift schedule by individual are supported.

Manage Shift Schedule by Department via Mobile Web Browser

You can set the shift schedule by department, and the employees in the same department will use the same shift schedule.

Before You Start

- Edit the department. You can refer to [***Manage Department via Mobile Web Browser***](#) for details.
- Set the normal shift and man-hour shift. You can refer to [***Manage Normal Shift via Mobile Web Browser***](#) and [***Manage Man-Hour Shift via Mobile Web Browser***](#) for details.
- Set the holiday attendance. You can refer to [***Manage Holiday via Mobile Web Browser***](#) for details.

Steps

1. Tap **Configuration** → **Time and Attendance** → **Shift Schedule Management** → **Shift Schedule by Department** to enter the settings page.
2. Tap the shift schedule to edit the shift schedule by department.
3. Edit the shift schedule by department parameters.

Department Name

You should set the department name in department management. You can refer to [**Manage Department via Mobile Web Browser**](#) for details.

Add Shift Schedule

Tap **+**, and set the shift schedule name, shift schedule time and daily shift schedule information.



Up to 8 shift schedules can be added, and the dates of each shift schedule cannot overlap.

Holiday Settings

Tap **Holiday Settings**, select the holiday and tap **OK**. After setting, the attendance will not be checked during holidays.

4. Tap **Save**.
5. **Optional:** Tap the shift schedule that needs to be deleted, and tap  to delete the shift schedule.

Manage Shift Schedule by Individual via Mobile Web Browser

You can set the shift schedule by individual.

Before You Start

- Edit the department. You can refer to [**Manage Department via Mobile Web Browser**](#) for details.
- Set the normal shift and man-hour shift. You can refer to [**Manage Normal Shift via Mobile Web Browser**](#) and [**Manage Man-Hour Shift via Mobile Web Browser**](#) for details.
- Set the holiday attendance. You can refer to [**Manage Holiday via Mobile Web Browser**](#) for details.

Steps



The priority of shift schedule by individual is higher than that of shift schedule by department. If a person is configured with shift schedule by individual and department at the same time, shift schedule by individual will be used first during attendance.

1. Tap **Configuration** → **Time and Attendance** → **Shift Schedule Management** → **Shift Schedule by Individual** to enter the settings page.
2. Tap **+** to add the shift schedule by individual.
3. Select the employee.
4. Edit the shift schedule parameters.

Add Shift Schedule

Tap **+**, and set the shift schedule name, shift schedule time and daily shift schedule information.

Note

Up to 8 shift schedules can be added, and the dates of each shift schedule cannot overlap.

Holiday Settings

Tap **Holiday Settings**, select the holiday and tap **OK**. After setting, the attendance will not be checked during holidays.

5. Tap **Save**.
6. **Optional:** Tap the shift schedule that needs to be edited, to edit the settings.
7. **Optional:** Tap the shift schedule that needs to be deleted, and tap  to delete the shift schedule.

8.3.7 General Settings

Set Authentication Parameters

Set Authentication Parameters.

Steps

1. Tap **Configuration** → **General Settings** → **Authentication Settings** .
2. Tap **Save**.

Device Type

Main Card Reader

You can configure the device card reader's parameters. If you select main card reader, you need to configure the following parameters: **Card Reader Type**, **Card Reader Description**, **Enable Card Reader**, **Authentication**, **Recognition Interval (s)**, **Max.Authentication Failed Attempts Alarm/Alarm of Max. Failed Attempts**.

Card Reader Type

Get card reader type.

Card Reader Description

Get card reader description. It is read-only.

Enable Card Reader

Enable the card reader's function.

Authentication

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

Recognition Interval

If the interval between card presenting of the same card is less than the configured value, the card presenting is invalid. The interval time range is from 0 to 255 seconds (When set to 0, it means that recognition interval is not enabled, and the same authentication can be used for unlimited times).

Multiple People Authentication

After multiple faces authentication is enabled, multiple faces authentication is supported.

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

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

Set Privacy Parameters

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

Tap **Configuration** → **General Settings** → **Privacy** .

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

Check Face Picture, Name, or Employee ID. When authentication is completed, the system will display the selected contents in the result.

Picture Uploading and Storage

You can upload and store pictures.

Upload Captured Picture When Authenticating

Upload the pictures captured when authenticating to the platform automatically.

Save Captured Picture When Authenticating

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

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.

Clear All Pictures in Device

You can clear registered face pictures and captured pictures in device.

Clear Registered Face Pictures

All registered pictures in the device will be deleted.

Clear Authentication/Captured Pictures

All authentication/captured pictures in the device will be deleted.

8.3.8 Face Parameters Settings

Set face parameters.

Face Parameters Settings

Tap **Configuration** → **Smart** → **Intelligent Parameter** to enter the page.



Note

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

Set Face Parameters.

Face Anti-spoofing

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

Live Face Detection Security Level

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

Recognition Distance

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

Application Mode

Select **Indoor** or **Others** according to actual environment. In the outdoor scene, indoor scene near the window, or bad environment, you can choose **Others**.



Note

If the device is not activated by other tools, the device uses indoor as the environment mode by default.

Face Recognition Mode

Normal Mode

The device uses a camera to perform face recognition.

Deep Mode

It is applicable for for more complex environments, and the range of people recognized is wider.



Note

- The two modes cannot be compatible with each other. Do not change the mode once it is selected. If you change the mode, all face pictures of the previous mode will be cleared.
 - In the deep mode, you can add the face pictures only via the user adding function of the device or the enrollment station. It is not supported to add face pictures via pictures importing.
-

The device uses a camera to perform face recognition.

Continuous Face Recognition Interval

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



Note

Value Range: 1 to 10.

1:1 Matching Threshold

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

1:N Matching Threshold

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

Face Recognition Timeout Value

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

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

Set the matching threshold when authenticating via ECO mode 1:1 matching mode and ECO mode 1:N matching mode.

ECO Mode (1:1)

Set the matching threshold when authenticating via ECO mode 1:1 matching mode.

ECO Mode (1:N)

Set the matching threshold when authenticating via ECO mode 1: N matching mode.

Set Recognition Area

Tap **Configuration** → **Smart** → **Area Configuration** to enter the page.

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

Drag the slider to configure the effective area of face recognition.

Tap **Save** to save the settings.

Chapter 9 Operation via Web Browser

9.1 Login

You can login via the web browser.

 **Note**

- Parts of the model supports Wi-Fi settings.
- Make sure the device is activated.

Obtain the IP address from the device after Wi-Fi is enabled. Make sure the IP segment of the device and the computer is the same. For details, refers to ***Set Wi-Fi Parameters*** .

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

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

 **Note**

Make sure that the IP address starts with "Https:".

9.2 Person Management

Click and add the person's information, including the basic information, card, authentication mode, and the picture.

Click **OK** to save the person.

Add Basic Information

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

Add the person's basic information, including the employee ID, the person's name, the gender, user level, floor No., and room No.

Click **OK** to save the settings.

Add Card

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

Click **Add Card** and enter a card number.

Click **OK** to save the settings.

Add Face Picture

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

Click + on the right to upload a face picture from the local PC.

Note

The picture format should be JPG, JPEG or PNG. The size should be less than 200K.

Click **OK** to save the settings.

Set Permission Time

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

Set **Start Time** and **End Time**.

Click **OK** to save the settings.

Set Access Control

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

After check **Administrator** in **Access Control**, the added person can log in by authenticating face.

Click **OK** to save the settings.

Add Authentication Mode

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

Set the authentication type.

Click **OK** to save the settings.

9.3 Search Event

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

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

The results will be displayed in the list.

9.4 Configuration

9.4.1 Set Local Parameters

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

Set Live View Parameters

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

Set Record File Saving Path

Click **Configuration** → **Local** to enter the Local page. Select a record file size and select a saving path from your local computer and click **Save**.

You can also click **Open** to open the file folder to view details.

Set Captured Pictures Saving Path

Click **Configuration** → **Local** to enter the Local page. Select a saving path from your local computer and click **Save**.

You can also click **Open** to open the file folder to view details.

9.4.2 View Device Information

View the device name, language, model, serial No., QR code, version, device capacity, etc.

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

You can view the device name, language, model, serial No., QR code, version, device capacity, etc.

9.4.3 Set Time

Set the device's time zone, synchronization mode, and the device time.

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.

9.4.4 Set DST

Steps

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

9.4.5 View Open Source Software License

Go to **Configuration** → **System** → **System Settings** → **About** , and click **View Licenses** to view the device license.

9.4.6 Upgrade and Maintenance

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

Reboot Device

Click **Configuration** → **System** → **Maintenance** → **Upgrade & Maintenance** .
Click **Reboot** to start reboot the device.

Restore Parameters

Click **Configuration** → **System** → **Maintenance** → **Upgrade & Maintenance** .

Restore All

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

Default

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

Unlink APP Account

Unlink the Hik-Connect account from the platform.

Import and Export Parameters

Click **Configuration** → **System** → **Maintenance** → **Upgrade & Maintenance** .

Export

Click **Export** to export the logs or 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.

Upgrade

Click **Configuration** → **System** → **Maintenance** → **Upgrade & Maintenance** .

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



Do not power off during the upgrading.

9.4.7 Security Mode Settings

Set the security mode for logging in.

On the Device for Management page, click **Configuration → System → Security → Security Service** .

Enable SSH

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

Enable HTTPS

In order to increase the network security level when visiting websites, you can enable HTTPS to acquire a more secure and encrypted network communication environment. The communication should be authenticated by identity and encryption password after enabling HTTPS, which is safe.

Enable Illegal Login Lock

In order to increase the network security level when visiting websites, you can enable Illegal Login Lock to secure legal login. The auto-lock feature will block devices that are attempting to connect for 30 minutes if the login is entered incorrectly after several attempts.

9.4.8 Certificate Management

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



The function is only supported by certain device models.

Create and Install Self-signed Certificate

Steps

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

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

The certificate will be saved automatically.

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

Install Other Authorized Certificate

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

Steps

1. Go to **Configuration → System → Security → Certificate Management** .
2. In the **Import Passwords** and **Import Communication Certificate** areas, select certificate type and upload certificate.
3. Click **Install**.

Install CA Certificate

Before You Start

Prepare a CA certificate in advance.

Steps

1. Go to **Configuration → System → Security → Certificate Management** .
2. Create an ID in the **Import CA Certificate** area.



Note

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

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

9.4.9 Change Administrator's Password

Steps

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



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.

9.4.10 Online Users

The information of users logging into the device is shown.

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

9.4.11 View Device Arming/Disarming Information

View device arming type and arming IP address.

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

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

9.4.12 Network Settings

Set TCP/IP, port, Wi-Fi parameters, report strategy, platform access, HTTP listening, and network service.



Note

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

Set Basic Network Parameters

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

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

DHCP

If uncheck the function, you should set the IPv4 address, IPv4 subnet mask, IPv4 default gateway, MTU, and the device port.

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

NIC Type

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

DNS Server

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

Set Port Parameters

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

Click **Configuration** → **Network** → **Basic Settings** → **Port** .

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.

RTSP

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

HTTPS

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

Server

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

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** → **Basic Settings** → **Wi-Fi** .
2. Check **Wi-Fi**.
3. Select a Wi-Fi
 - Click  of a Wi-Fi in the list and enter the Wi-Fi password.
 - Click **Add** and enter a Wi-Fi's name, password, and encryption type. Click **Connect**. When the Wi-Fi is connected, click **OK**.
4. **Optional**: Set the WLAN parameters.
 - 1) Click **TCP/IP Settings**.
 - 2) Set the IP address, subnet mask, and default gateway. Or check **Enable DHCP** and the system will allocate the IP address, subnet mask, and default gateway automatically.

5. Click **Save**.

Report Strategy Settings

You can set the center group for uploading the log via the ISUP protocol.

Go to **Configuration → Network → Basic Settings → Report Strategy** .

You can set the center group and the system will transfer logs via ISUP protocol. Click **Save** to save the settings.

Center Group

Select a center group from the drop-down list.

Main Channel

The device will communicate with the center via the main channel.



Note

N1 refers to wired network.

Platform Access

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

Steps

1. Click **Configuration → Network → Advanced → Platform Access** to enter the settings page.
2. Check the checkbox of **Enable** to enable the function.
3. Select the **Platform Access Mode**.



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.

4. Create a **Stream Encryption/Encryption Key** for the device.
-



Note

6 to 12 letters (a to z, A to Z) or numbers (0 to 9), case sensitive. You are recommended to use a combination of no less than 8 letters or numbers.

5. 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** → **Advanced Settings** → **Platform** .
 2. Select **ISUP** from the platform access mode drop-down list.
 3. Check **Enable**.
 4. Set the ISUP version, server address, device ID, and the ISUP status.
-

Note

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

5. Click **Save**.
-

Enable SDK Service

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

Click **Configuration** → **Network** → **Advanced** → **Network Service** to enter the settings page.

Check the checkbox of **Enable** to enable the function.

Click **Save** to enable the settings.

9.4.13 Set Video and Audio Parameters

Set the output volume and voice prompt.

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

Drag the block to adjust the output volume.

Enable **Voice Prompt**, and the device will make voice prompts.

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

Note

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

9.4.14 Customize Audio Content

Customize the output audio content when authentication succeeded and failed.

Steps

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

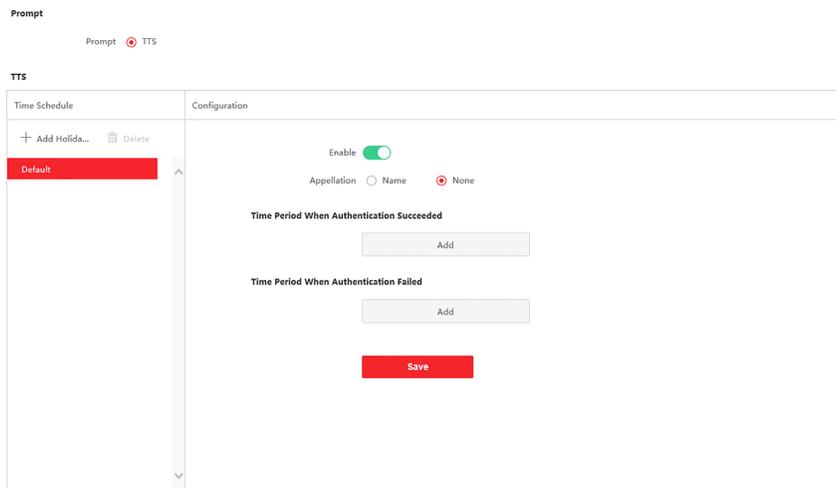


Figure 9-1 Customize Audio Content

2. Select time schedule.
3. Enable the function.
4. Set the appellation.
5. Set the time period when authentication succeeded.
 - 1) Click **Add**.
 - 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.
6. Set the time duration when authentication failed.
 - 1) Click **Add**.
 - 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.
7. **Optional:** Add holiday schedule.
 - 1) Click **Add** to add holiday schedule.
 - 2) Repeat step 3 to 6.
8. Click **Save** to save the settings.

9.4.15 Time and Attendance Settings

If you want to track and monitor when the persons start/stop work and monitor their working hours and late arrivals, early departures, time taken on breaks, and absenteeism, you can add the person to the shift group and assign a shift schedule (a rule for the attendance defining how the schedule repeats, the shift type, break settings, and the card swiping rule.) to the shift group to define the attendance parameters for the persons in the shift group.

Disable Attendance Mode via Web

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

Steps

1. Click **Configuration** → **Attendance** to enter the settings page.
2. Set the **Attendance Mode** as **Disable**.

Result

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

Time Settings

Steps

1. Click **Configuration** → **Time Settings** to enter the settings page.
2. Select **Status Type**.
3. **Optional**: Edit **Schedule Name** according to the actual needs.
4. Drag mouse to set the schedule.



Note

Set the schedule from Monday to Sunday according to the actual needs.

-
5. **Optional**: Select a timeline and click **Delete**. Or click **Delete All** to clear the settings.
 6. Click **Save**.

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** → **Attendance** to enter the settings page.
 2. Set the **Attendance Mode** as **Manual**.
 3. Enable the **Attendance Status Required** and set the attendance status lasts duration.
 4. Enable a group of attendance status.
-

Note

The Attendance Property will not be changed.

5. **Optional:** Select an status and change its name if required.

Result

You should select an attendance status manually after authentication.

Note

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

Set Auto Attendance via Web

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

Before You Start

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

Steps

1. Click **Configuration** → **Attendance** to enter the settings page.
 2. Set the **Attendance Mode** as **Auto**.
 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.
6. Set the status' schedule. Refers to ***Time Settings*** 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** → **Attendance** to enter the settings page.
2. Set the **Attendance Mode** as **Manual and Auto**.
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.
6. Set the status' schedule. Refers to ***Time Settings*** 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.

9.4.16 General Settings

Set Authentication Parameters

Click **Configuration** → **General** → **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.

Card Reader

You can configure the device card reader's parameters.

Card Reader Type/Card Reader Description

Get card reader type and description. They are read-only.

Enable Card Reader

Enable the card reader's function.

Authentication

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

Multiple People Authentication

Multiple people can be authenticated at the same time.

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.

Max. Authentication Failed Attempts

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

Set Privacy Parameters

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

Go to **Configuration** → **General** → **Privacy** .

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**, **Employee ID** and **Temperature**, to display the authentication result.

Picture Uploading and Storage

Upload Captured Picture When Authenticating

Upload the pictures captured when authenticating to the platform automatically.

Save Captured Picture When Authenticating

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

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.

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.

Set Face Recognition Parameters

You can set face recognition parameters for accessing.

Click **Configuration** → **General** → **Face Recognition 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.

Enable **Blocklist Authentication**.

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

9.4.17 Title: Local Time and Attendance Settings

You can set the department management, normal shift management, man-hour shift management, holiday management and shift settings for the device.

Manage Department via Web

You can add, edit and delete department information via Web.

Steps

1. Click **Configuration** → **Time and Attendance** → **Department Management** .

Department Information

+ Add

No.	Name	Employee Number	Operation
01	Company	1	
02	Admin. Dept.	0	
03	Sales Dept.	0	
04	Financial Dept.	0	
05	Production Dept.	0	
06	Purchasing Dept.	0	
07	R&D Dept.	0	

Total 7 Items Items per Page 20 Items Prev Page 1 Next Page Go to Page Go to

Figure 9-2 Department Management

2. Click **Add** to add department.
 - 1) Enter **Department Name**.
 - 2) Click **OK** to save the settings.
3. **Optional:** Manage department information.

Edit Department Information Click to edit department information.

Delete Department Information Click to delete department information.

Manage Normal Shift via Web

You can add, edit and delete normal shift information via Web.

Steps

1. Click **Configuration** → **Time and Attendance** → **Normal Shift Management** .
2. Set check in and check out information.

Check In Settings

Advanced Check In Time minute

Latest Check In Time minute

Absence Time (Late) minute

Check Out Settings

Earliest Check Out Time minute

Latest Check Out Time minute

Absence Time (Early Leave) minute

Figure 9-3 Check In and Out Settings

- 1) Enter **Advanced Check In Time**, **Latest Check In Time** and **Absence Time (Late)**.
- 2) Enter **Earliest Check Out Time**, **Latest Check Out Time** and **Absence Time (Early Leave)**.
3. Click **Add** to add shift.

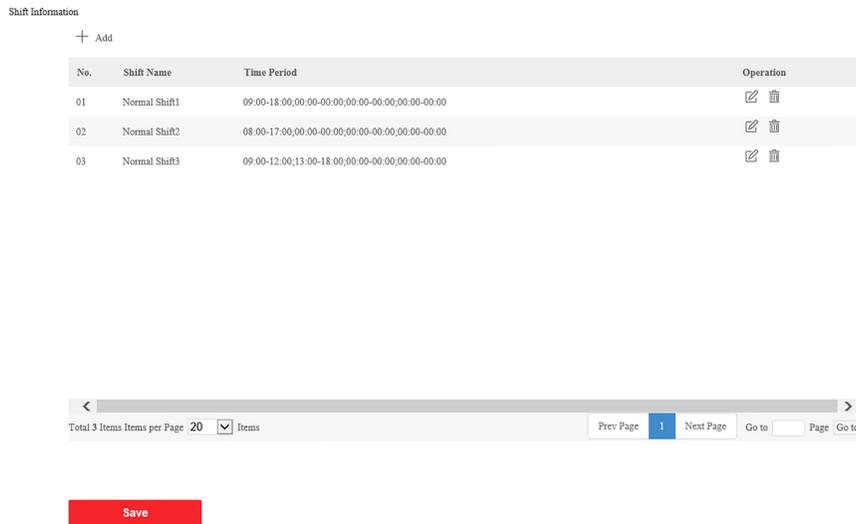


Figure 9-4 Shift Information

- 1) Enter **Shift Name**.
 - 2) Click **Add**.
 - 3) Set **Time Period**.
 - 4) Click **OK** to save the settings.
4. **Optional**: Manage shift information.

Edit Shift Information Click to edit shift information.

Delete Shift Information Click to delete shift information.

Manage Man-Hour Shift via Web

You can add, edit and delete man-hour shift information via Web.

Steps

1. Click **Configuration** → **Time and Attendance** → **Man-Hour Shift Management** .

Shift Information

+ Add

No.	Shift Name	Work Duration(units: min)	Latest On-Work Time	Break Duration	Operation
04	Celine	480	23:59:00	00:00:00;00:00:00;00:00:00;00:00:00	 

Total 1 Items Items per Page 20 Items

Prev Page 1 Next Page Go to Page Go to

Figure 9-5 Man-Hour Shift Management

2. Click **Add** to add shift.
 - 1) Enter **Shift Name**.
 - 2) Set **Work Duration** and **Latest On-Work Time**.
 - 3) Click **Add Duration**.
 - 4) Set **Time Period**.
 - 5) Click **OK** to save the settings.
3. **Optional:** Manage shift information.

Edit Shift Information Click  to edit shift information.

Delete Shift Information Click  to delete shift information.

Manage Holiday via Web

You can add, edit and delete holiday information via Web.

Steps

1. Click **Configuration** → **Time and Attendance** → **Holiday Management** .

Holiday Information

+ Add

No.	Holiday Name	Holiday Start Time	Holiday End Time	Operation
01	D	2000-01-01	1902-11-24	

Total 1 Items Items per Page 20 Items

Prev Page 1 Next Page Go to Page Go to

Figure 9-6 Holiday Management

2. Click **Add** to add holiday.
 - 1) Enter **Holiday Name**.
 - 2) Set **Holiday Start Time** and **Holiday End Time**.
 - 3) Click **OK** to save the settings.
3. **Optional:** Manage holiday information.

Edit Holiday Information Click to edit holiday information.

Delete Holiday Information Click to delete holiday information.

Manage Shift Schedule by Department

You can add, edit and delete shift schedule by department information via Web.

Steps

1. Click **Configuration → Time and Attendance → Shift Settings** .

Shift Schedule by Department

No.	Department Name	Week Schedule Details	Holiday Group Settings	Operation
1	Company	Weekly Schedule1	Holiday Group0	
2	Admin. Dept.	Weekly Schedule2	Holiday Group0	
3	Sales Dept.	Weekly Schedule3	Holiday Group0	
4	Financial Dept.	Weekly Schedule4	Holiday Group0	
5	Production Dept.	Weekly Schedule5	Holiday Group0	
6	Purchasing Dept.	Weekly Schedule6	Holiday Group0	
7	R&D Dept.	Weekly Schedule7	Holiday Group0	

Total 7 Items Items per Page 20 Items

Prev Page 1 Next Page Go to Page Go to

Figure 9-7 Shift Schedule by Department

2. **Optional:** Manage shift schedule by department information.

Edit Shift Schedule by Department Information

Click  to edit shift schedule by department information.

Delete Shift Schedule by Department Information

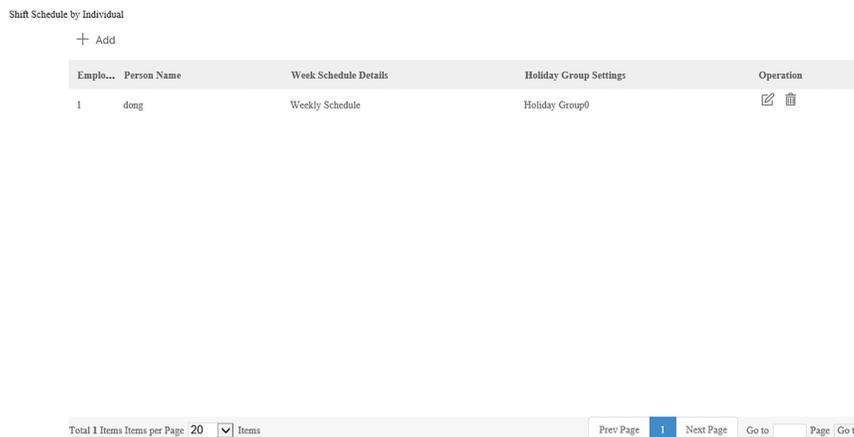
Click  to delete shift schedule by department information.

Manage Shift Schedule by Individual

You can add, edit and delete shift schedule by individual information via Web.

Steps

1. Click **Configuration** → **Time and Attendance** → **Shift Settings** .



Emple...	Person Name	Week Schedule Details	Holiday Group Settings	Operation
1	dong	Weekly Schedule	Holiday Group0	 

Figure 9-8 Shift Schedule by Individual

2. Click **Add** to add shift schedule by individual.
 - 1) Enter **Person Name**.
 - 2) Set **Holiday**.
 - 3) Click **Add Week Schedule**.
 - 4) Enter **Week Schedule Name**, and set **Start Time** and **End Time**.
 - 5) Select duration and shift.
 - 6) Click **OK** to save the settings.
3. **Optional:** Manage shift schedule by individual information.

Edit Shift Schedule by Individual Information

Click  to edit shift schedule by individual information.

Delete Shift Schedule by Individual Information

Click  to delete shift schedule by individual information.

9.4.18 Set Biometric Parameters

Set Basic Parameters

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



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

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

Face Recognition Mode

Normal Mode

Recognize face via the camera normally.

Deep Mode

In the deep mode, you can add the face pictures only via the user adding function of the device or the enrollment station. It is not supported to add face pictures via pictures importing.

Enable Multiple Faces Authentication

After enabling, multiple people can authenticate at the same time.

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 100% applicable to anti-spoofing environments. If you require a higher security level, use multiple authentication modes.

Live Face Detection Security Level

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

Recognition Distance

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

Application Mode

Select either others or indoor according to actual environment.

Continuous Face Recognition Interval

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

Pitch Angle

The maximum pitch angle when starting face authentication.

Yaw Angle

The maximum yaw angle when starting face authentication.

Min. Detection Area (Width)

Set the minimum width of the detection area.

Min. Detection Area (Height)

Set the minimum height of the detection area.

Face Grading

Set the face grading according to your needs.

1:1 Matching Threshold

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

1:N Matching Threshold

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

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 (1:1)

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

ECO Mode (1:N)

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

Fingerprint Security Level

Select the fingerprint security level.

The higher is the security level, the lower is the false acceptance rate (FAR).

The higher is the security level, the higher is the false rejection rate (FRR).

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.

Set **Area Configuration**, **Margin (Left)**, **Margin (Right)**, **Margin (Top)** and **Margin (Bottom)** as desired.

Click **Save** to save the settings.

Click  or  to record videos or capture pictures.

9.4.19 Set Theme

You can set the theme for the device.

Click **Configuration** → **Theme** → **Media Database** to enter the page.

Click **Add** to add media database file.

Click **Upload**.

Click **Configuration** → **Theme** → **Theme** to enter the page.

Click **Add Media File**.

Note

Only 1 media file can be added.

Click **+** to select media file and click **OK**.

Click  to edit media file name.

Set play schedule. Select a theme to play. Drag the time bar in the timeline to set the time for the image to play. Select the time period, you can edit the start and end time of the time period, click **Save** or **Delete** to save or delete the time period. You can also click **Delete** or **Delete All** to delete the selected time period or to delete all time periods.

Chapter 10 Client Software Configuration

10.1 Configuration Flow of Client Software

Follow the flow diagram below to configure on the client software.

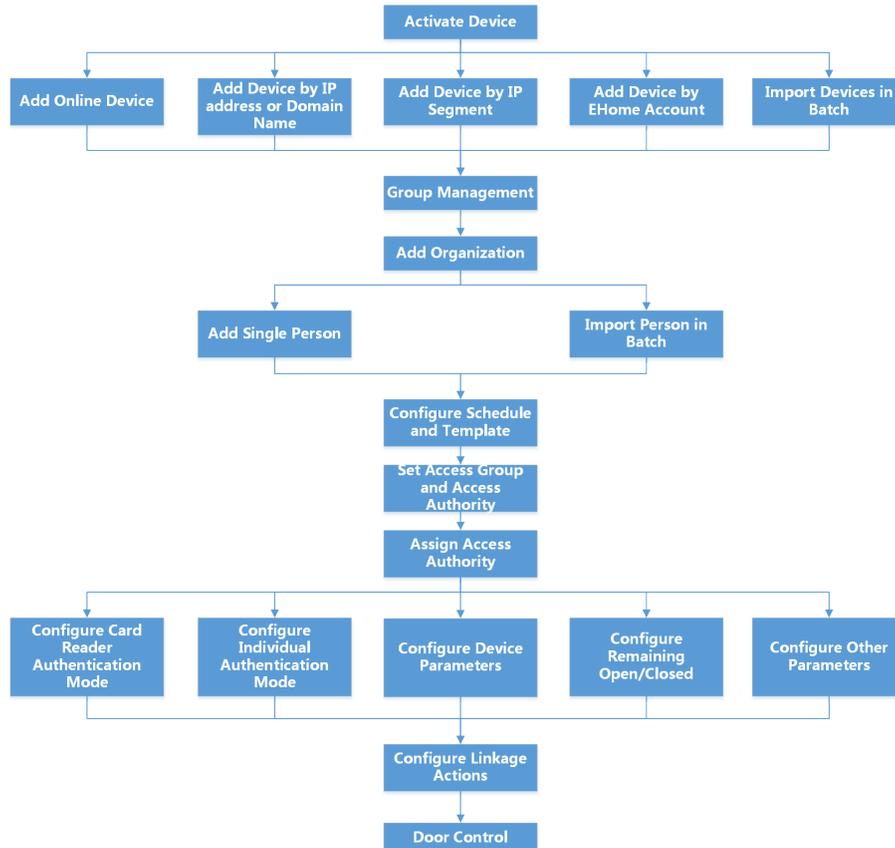


Figure 10-1 Flow Diagram of Configuration on Client Software

10.2 Device Management

The client supports managing access control devices and video intercom devices.

Example

You can control entrance & exit and manage attendance after adding access control devices to the client; you can perform video intercom with the indoor stations and door stations.

10.2.1 Add Device

The client provides three device adding modes including by IP/domain, IP segment, and ISUP protocol. The client also supports importing multiple devices in a batch when there are large amount of devices to be added.

Add Device by IP Address or Domain Name

If you know the IP address or domain name of the device to add, you can add devices to the client by specifying the IP address (or domain name), user name, password, etc.

Steps

1. Enter Device Management module.
2. Click **Device** tab on the top of the right panel.
The added devices are displayed on the right panel.
3. Click **Add** to open the Add window, and then select **IP/Domain** as the adding mode.
4. Enter the required information.

Name

Create a descriptive name for the device. For example, you can use a nickname that can show the location or feature of the device.

Address

The IP address or domain name of the device.

Port

The devices to add share the same port number. The default value is **8000**.

User Name

Enter the device user name. By default, the user name is **admin**.

Password

Enter the device 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.

-
5. **Optional:** Check **Transmission Encryption (TLS)** to enable transmission encryption using TLS (Transport Layer Security) protocol for security purpose.

Note

- This function should be supported by the device.
- If you have enabled Certificate Verification, you should click **Open Certificate Directory** to open the default folder, and copy the certificate file exported from the device to this default directory to strengthen the security. See for details about enabling certificate verification.
- You can log into the device to get the certificate file by web browser.

-
6. Check **Synchronize Time** to synchronize the device time with the PC running the client after adding the device to the client.
 7. **Optional:** Check **Import to Group** to create a group by the device name, and import all the channels of the device to this group.

Example

For access control device, its access points, alarm inputs/outputs, and encoding channels (if exist) will be imported to this group.

8. Finish adding the device.
 - Click **Add** to add the device and back to the device list page.
 - Click **Add and New** to save the settings and continue to add other device.

Import Devices in a Batch

You can add multiple devices to the client in a batch by entering the device parameters in a pre-defined CSV file.

Steps

1. Enter the Device Management module.
2. Click **Device** tab on the top of the right panel.
3. Click **Add** to open the Add window, and then select **Batch Import** as the adding mode.
4. Click **Export Template** and then save the pre-defined template (CSV file) on your PC.
5. Open the exported template file and enter the required information of the devices to be added on the corresponding column.

Note

For detailed description of the required fields, refer to the introductions in the template.

Adding Mode

Enter **0** or **1** or **2**.

Address

Edit the address of the device.

Port

Enter the device port number. The default port number is **8000**.

User Name

Enter the device user name. By default, the user name is **admin**.

Password

Enter the device 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.

Import to Group

Enter **1** to create a group by the device name. All the channels of the device will be imported to the corresponding group by default. Enter **0** to disable this function.

6. Click  and select the template file.

7. Click **Add** to import the devices.

10.2.2 Reset Device Password

If you forgot the password of the detected online devices, you can reset the device password via the client.

Steps

1. Enter Device Management page.

2. Click **Online Device** to show the online device area.

All the online devices sharing the same subnet will be displayed in the list.

3. Select the device from the list and click  on the Operation column.

4. Reset the device password.

- Click **Generate** to pop up the QR Code window and click **Download** to save the QR code to your PC. You can also take a photo of the QR code to save it to your phone. Send the picture to our technical support.



Note

For the following operations for resetting the password, contact our technical support.



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.

10.2.3 Manage Added Devices

After adding devices to device list, you can manage the added devices including editing device parameters, remote configuration, viewing device status, etc.

Table 10-1 Manage Added Devices

Edit Device	Click  to edit device information including device name, address, user name, password, etc.
Delete Device	Check one or more devices, and click Delete to delete the selected devices.
Remote Configuration	Click  to set remote configuration of the corresponding device. For details, refer to the user manual of device.
View Device Status	Click  to view device status, including door No., door status, etc.  Note For different devices, you will view different information about device status.
View Online User	Click  to view the details of online user who access the device, including user name, user type, IP address and login time.
Refresh Device Information	Click  to refresh and get the latest device information.
Upgrade Device	View device status on Firmware Upgrade column, check one or more upgradable devices, and click Upgrade Device Firmware to upgrade the selected devices. For details, refer to .
Get Events from Device	Check one device, and click Get Events from Device to synchronize events. For details, refer to .

10.3 Group Management

The client provides groups to manage the added resources in different groups. You can group the resources into different groups according to the resources' locations.

Example

For example, on the 1st floor, there mounted 16 doors, 64 alarm inputs, and 16 alarm outputs. You can organize these resources into one group (named 1st Floor) for convenient management. You can control door status, and do some other operations of the devices after managing the resources by groups.

10.3.1 Add Group

You can add group to organize the added device for convenient management.

Steps

1. Enter the Device Management module.
2. Click **Device Management** → **Group** to enter the group management page.
3. Create a group.
 - Click **Add Group** and enter a group name as you want.
 - Click **Create Group by Device Name** and select an added device to create a new group by the name of the selected device.



The resources (such as alarm inputs/outputs, access points, etc.) of this device will be imported to the group by default.

10.3.2 Import Resources to Group

You can import the device resources (such as alarm inputs/outputs, access points, etc.) to the added group in a batch.

Before You Start

Add a group for managing devices. Refer to [Add Group](#).

Steps

1. Enter the Device Management module.
2. Click **Device Management** → **Group** to enter the group management page.
3. Select a group from the group list and select the resource type as **Access Point**, **Alarm Input**, **Alarm Output**, etc.
4. Click **Import**.
5. Select the thumbnails/names of the resources in the thumbnail/list view.



You can click  or  to switch the resource display mode to thumbnail view or to list view.

6. Click **Import** to import the selected resources to the group.
-

10.4 Person Management

You can add person information to the system for further operations such as access control, video intercom, time and attendance, etc. You can manage the added persons such as issuing cards to them in a batch, importing and exporting person information in a batch, etc.

10.4.1 Add Organization

You can add an organization and import person information to the organization for effective management of the persons. You can also add a subordinate organization for the added one.

Steps

1. Enter **Person** module.
2. Select a parent organization in the left column and click **Add** in the upper-left corner to add an organization.
3. Create a name for the added organization.



Up to 10 levels of organizations can be added.

4. **Optional:** Perform the following operation(s).

Edit Organization Hover the mouse on an added organization and click  to edit its name.

Delete Organization Hover the mouse on an added organization and click  to delete it.



- The lower-level organizations will be deleted as well if you delete an organization.
 - Make sure there is no person added under the organization, or the organization cannot be deleted.
-

Show Persons in Sub Organization Check **Show Persons in Sub Organization** and select an organization to show persons in its sub organizations.

10.4.2 Import and Export Person Identify Information

You can import the information and pictures of multiple persons to the client software in a batch. Meanwhile, you can also export the person information and pictures and save them in your PC.

Import Person Information

You can enter the information of multiple persons in a predefined template (CSV/Excel file) to import the information to the client in a batch.

Steps

1. Enter the Person module.
2. Select an added organization in the list, or click **Add** in the upper-left corner to add an organization and then select it.
3. Click **Import** to open the Import panel.
4. Select **Person Information** as the importing mode.
5. Click **Download Template for Importing Person** to download the template.
6. Enter the person information in the downloaded template.



Note

- If the person has multiple cards, separate the card No. with semicolon.
- Items with asterisk are required.
- By default, the Hire Date is the current date.

-
7. Click  to select the CSV/Excel file with person information from local PC.
 8. Click **Import** to start importing.



Note

- If a person No. already exists in the client's database, delete the existing information before importing.
 - You can import information of no more than 2,000 persons.
-

Import Person Pictures

After importing face pictures for the added persons to the client, the persons in the pictures can be identified by an added face recognition terminal. You can either import person pictures one by one, or import multiple pictures at a time according to your need.

Before You Start

Be sure to have imported person information to the client beforehand.

Steps

1. Enter the Person module.
2. Select an added organization in the list, or click **Add** in the upper-left corner to add an organization and then select it.
3. Click **Import** to open the Import panel and check **Face**.
4. **Optional:** Enable **Verify by Device** to check whether face recognition device managed in the client can recognize the face in the photo.
5. Click  to select a face picture file.

Note

- The (folder of) face pictures should be in ZIP format.
- Each picture file should be in JPG format and should be no larger than 200 KB.
- Each picture file should be named as "Person ID_Name". The Person ID should be the same with that of the imported person information.

6. Click **Import** to start importing.

The importing progress and result will be displayed.

Export Person Information

You can export the added persons' information to local PC as a CSV/Excel file.

Before You Start

Make sure you have added persons to an organization.

Steps

1. Enter the Person module.
2. **Optional:** Select an organization in the list.

Note

All persons' information will be exported if you do not select any organization.

-
3. Click **Export** to open the Export panel.
 4. Check **Person Information** as the content to export.
 5. Check desired items to export.
 6. Click **Export** to save the exported file in CSV/Excel file on your PC.

Export Person Pictures

You can export face picture file of the added persons and save in your PC.

Before You Start

Make sure you have added persons and their face pictures to an organization.

Steps

1. Enter the Person module.
2. **Optional:** Select an organization in the list.

Note

All persons' face pictures will be exported if you do not select any organization.

-
3. Click **Export** to open the Export panel and check **Face** as the content to export.
 4. Click **Export** to start exporting.

Note

- The exported file is in ZIP format.
 - The exported face picture is named as "Person ID_Name_0" ("0" is for a full-frontal face).
-

10.4.3 Get Person Information from Access Control Device

If the access control device has been configured with person information (including person details, fingerprint, and issued card information), you can get the person information from the added device and import them to the client for further operations.

Steps

Note

- If the person name stored in the device is empty, the person name will be filled with the issued card No. after importing to the client.
 - The gender of the persons will be **Male** by default.
 - If the card number or person ID (employee ID) stored on the device already exists in the client database, the person with this card number or person ID will not be imported to the client.
-

1. Enter **Person** module.
 2. Select an organization to import the persons.
 3. Click **Get from Device**.
 4. Select an added access control device or the enrollment station from the drop-down list.
-

Note

If you select the enrollment station, you should click **Login**, and enter IP address, port No., user name and password of the device.

5. Select the **Getting Mode**.
-

Note

The getting mode varies according to different devices. The access control device supports getting the person information by employee ID. Up to 5 employee IDs can be specified each time.

6. Click **Import** to start importing the person information to the client.
-

Note

Up to 2,000 persons and 5,000 cards can be imported.

The person information, including person details, person's fingerprint information (if configured), and the linked cards (if configured), will be imported to the selected organization.

10.4.4 Issue Cards to Persons in Batch

The client provides a convenient way to issue cards to multiple persons in a batch.

Steps

1. Enter **Person** module.
2. Click **Batch Issue Cards**.
All the added persons with no card issued will be displayed in the right panel.
3. **Optional:** Enter key words (name or person ID) in the input box to filter the person(s) that need issuing cards.
4. **Optional:** Click **Settings** to set the card issuing parameters. For details, refer to .
5. Click **Initialize** to initialize the card enrollment station or card reader to make it ready for issuing cards.
6. Click the **Card No.** column and enter the card number.
 - Place the card on the card enrollment station.
 - Swipe the card on the card reader.
 - Manually enter the card number and press the **Enter** key.

The person(s) in the list will be issued with card(s).

10.4.5 Report Card Loss

If the person lost his/her card, you can report the card loss so that the card's related access authorization will be inactive.

Steps

1. Enter **Person** module.
2. Select the person you want to report card loss for and click **Edit** to open the Edit Person window.
3. In the **Credential → Card** panel, click  on the added card to set this card as lost card.
After reporting card loss, the access authorization of this card will be invalid and inactive. Other person who gets this card cannot access the doors by swiping this lost card.
4. **Optional:** If the lost card is found, you can click  to cancel the loss.
After cancelling card loss, the access authorization of the person will be valid and active.
5. If the lost card is added in one access group and the access group is applied to the device already, after reporting card loss or cancelling card loss, a window will pop up to notify you to apply the changes to the device. After applying to device, these changes can take effect on the device.

10.4.6 Set Card Issuing Parameters

The client provides two modes for reading a card's number: via card enrollment station or via the card reader of the access control device. If a card enrollment station is available, connect it to the PC running the client by USB interface or COM, and place the card on the card enrollment to read

the card number. If not, you can also swipe the card on the card reader of the added access control device to get the card number. As a result, before issuing a card to one person, you need to set the card issuing parameters including the issuing mode and related parameters.

When adding a card to one person, click **Settings** to open the Card Issuing Settings window.

Local Mode: Issue Card by Card Enrollment Station

Connect a card enrollment station to the PC running the client. You can place the card on the card enrollment station to get the card number.

Card Enrollment Station

Select the model of the connected card enrollment station



Note

Currently, the supported card enrollment station models include DS-K1F100-D8, DS-K1F100-M, DS-K1F100-D8E, and DS-K1F180-D8E.

Card Type

This field is only available when the model is DS-K1F100-D8E or DS-K1F180-D8E.

Select the card type as EM card or IC card according to the actual card type.

Serial Port

It is only available when the model is DS-K1F100-M.

Select the COM the card enrollment station connects to.

Buzzing

Enable or disable the buzzing when the card number is read successfully.

Card No. Type

Select the type of the card number according to actual needs.

M1 Card Encryption

This field is only available when the model is DS-K1F100-D8, DS-K1F100-D8E, or DS-K1F180-D8E.

If the card is M1 card, and if you need to enable the M1 Card Encryption function, you should enable this function and select the sector of the card to encrypt.

Remote Mode: Issue Card by Card Reader

Select an access control device added in the client and swipe the card on its card reader to read the card number.

10.5 Configure Schedule and Template

You can configure the template including holiday and week schedule. After setting the template, you can adopt the configured template to access groups when setting the access groups, so that the access group will take effect in the time durations of the template.

Note

For access group settings, refer to **Set Access Group to Assign Access Authorization to Persons** .

10.5.1 Add Holiday

You can create holidays and set the days in the holidays, including start date, end date, and holiday duration in one day.

Steps

Note

You can add up to 64 holidays in the software system.

1. Click **Access Control** → **Schedule** → **Holiday** to enter the Holiday page.
 2. Click **Add** on the left panel.
 3. Create a name for the holiday.
 4. **Optional:** Enter the descriptions or some notifications of this holiday in the Remark box.
 5. Add a holiday period to the holiday list and configure the holiday duration.
-

Note

Up to 16 holiday periods can be added to one holiday.

- 1) Click **Add** in the Holiday List field.
 - 2) Drag the cursor to draw the time duration, which means in that duration of time, the configured access group is activated.
-

Note

Up to 8 time durations can be set to one holiday period.

- 3) **Optional:** Perform the following operations to edit the time durations.
 - Move the cursor to the time duration and drag the time duration on the timeline bar to the desired position when the cursor turns to  .
 - Click the time duration and directly edit the start/end time in the appeared dialog.
 - Move the cursor to the start or the end of time duration and drag to lengthen or shorten the time duration when the cursor turns to  .
 - 4) **Optional:** Select the time duration(s) that need to be deleted, and then click  in the Operation column to delete the selected time duration(s).
 - 5) **Optional:** Click  in the Operation column to clear all the time duration(s) in the time bar.
 - 6) **Optional:** Click  in the Operation column to delete this added holiday period from the holiday list.
6. Click **Save**.
-

10.5.2 Add Template

Template includes week schedule and holiday. You can set week schedule and assign the time duration of access authorization for different person or group. You can also select the added holiday(s) for the template.

Steps

Note

You can add up to 255 templates in the software system.

1. Click **Access Control** → **Schedule** → **Template** to enter the Template page.
-

Note

There are two default templates: All-Day Authorized and All-Day Denied, and they cannot be edited or deleted.

All-Day Authorized

The access authorization is valid in each day of the week and it has no holiday.

All-Day Denied

The access authorization is invalid in each day of the week and it has no holiday.

2. Click **Add** on the left panel to create a new template.
 3. Create a name for the template.
 4. Enter the descriptions or some notification of this template in the Remark box.
 5. Edit the week schedule to apply it to the template.
 - 1) Click **Week Schedule** tab on the lower panel.
 - 2) Select a day of the week and draw time duration(s) on the timeline bar.
-

Note

Up to 8 time duration(s) can be set for each day in the week schedule.

- 3) **Optional:** Perform the following operations to edit the time durations.
 - Move the cursor to the time duration and drag the time duration on the timeline bar to the desired position when the cursor turns to .
 - Click the time duration and directly edit the start/end time in the appeared dialog.
 - Move the cursor to the start or the end of time duration and drag to lengthen or shorten the time duration when the cursor turns to .
 - 4) Repeat the two steps above to draw more time durations on the other days of the week.
6. Add a holiday to apply it to the template.
-

Note

Up to 4 holidays can be added to one template.

- 1) Click **Holiday** tab.
 - 2) Select a holiday in the left list and it will be added to the selected list on the right panel.
-

3) **Optional:** Click **Add** to add a new holiday.

 **Note**

For details about adding a holiday, refer to **Add Holiday**.

4) **Optional:** Select a selected holiday in the right list and click  to remove the selected one, or click **Clear** to clear all the selected holiday(s) in the right list.

7. Click **Save** to save the settings and finish adding the template.

10.6 Set Access Group to Assign Access Authorization to Persons

After adding the person and configuring the person's credentials, you can create the access groups to define which person(s) can get access to which door(s) and then apply the access group to the access control device to take effect.

Before You Start

- Add person to the client.
- Add access control device to the client and group access points. For details, refer to **Group Management**.
- Add template.

Steps

When the access group settings are changed, you need to apply the access groups to the devices again to take effect. The access group changes include changes of template, access group settings, person's access group settings, and related person details (including card number, fingerprint, face picture, linkage between card number and fingerprint, linkage between card number and fingerprint, card password, card effective period, etc).

1. Click **Access Control** → **Authorization** → **Access Group** to enter the Access Group interface.
2. Click **Add** to open the Add window.
3. In the **Name** text field, create a name for the access group as you want.
4. Select a template for the access group.

 **Note**

You should configure the template before access group settings. Refer to **Configure Schedule and Template** for details.

5. In the left list of the Select Person field, select person(s) to assign access authority.
6. In the left list of the Select Access Point field, select door(s), door station(s) or floor(s) for the selected persons to access.
7. Click **Save**.

You can view the selected person(s) and the selected access point(s) on the right side of the interface.

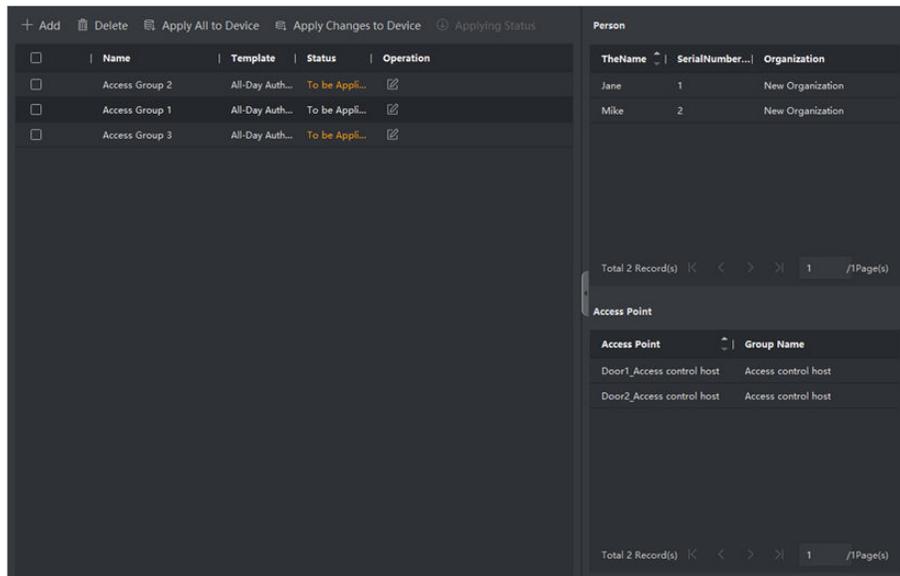


Figure 10-2 Display the Selected Person(s) and Access Point(s)

8. After adding the access groups, you need to apply them to the access control device to take effect.
 - 1) Select the access group(s) to apply to the access control device.
 - 2) Click **Apply All to Devices** start applying all the selected access group(s) to the access control device or door station.
 - 3) Click **Apply All to Devices** or **Apply Changes to Devices**.

Apply All to Devices

This operation will clear all the existed access groups of the selected devices and then apply the new access group to the device.

Apply Changes to Devices

This operation will not clear the existed access groups of the selected devices and only apply the changed part of the selected access group(s) to the device(s).

- 4) View the applying status in the Status column or click **Applying Status** to view all the applied access group(s).

Note

You can check **Display Failure Only** to filter the applying results.

The selected persons in the applied access groups will have the authorization to enter/exit the selected doors/door stations with their linked card(s) or fingerprints.

9. **Optional:** Click to edit the access group if necessary.

Note

If you change the persons' access information or other related information, you will view the prompt **Access Group to Be Applied** on the right corner of the client.

You can click the prompt to apply the changed data to the device. You can select either **Apply Now** or **Apply Later**.

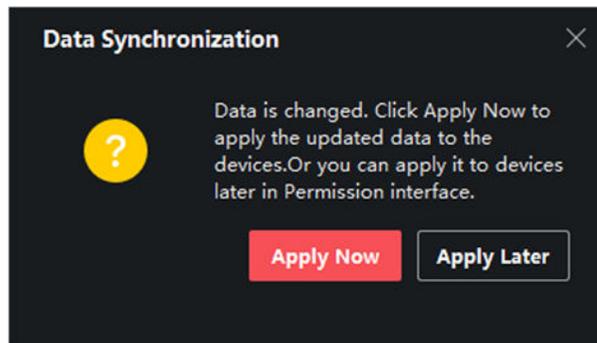


Figure 10-3 Data Synchronization

10.7 Configure Advanced Functions

You can configure the advanced functions of access control to meet some special requirements in different scene.

Note

- For the card related functions(the type of access control card), only the card(s) with access group applied will be listed when adding cards.
 - The advanced functions should be supported by the device.
 - Hover the cursor on the Advanced Function, and then Click  to customize the advanced function(s) to be displayed.
-

10.7.1 Configure Device Parameters

After adding the access control device, you can configure the parameters of access control device, access control points.

Configure Parameters for Access Control Device

After adding the access control device, you can configure its parameters, including overlaying user information on picture, uploading pictures after capturing, saving captured pictures, etc.

Before You Start

Add access control device to the client.

Steps

1. Click **Access Control** → **Advanced Function** → **Device Parameter** .

Note

If you can not find Device Parameter in the Advanced Function list, hover the cursor on the Advanced Function, and then Click  to select the Device Parameter to be displayed.

2. Select an access device to show its parameters on the right page.
3. Turn the switch to ON to enable the corresponding functions.

Note

- The displayed parameters may vary for different access control devices.
- Some of the following parameters are not listed in the Basic Information page, click **More** to edit the parameters.

RS-485 Comm. Redundancy

You should enable this function if you wire the RS-485 card reader to the access control device redundantly.

Display Detected Face

Display face picture when authenticating.

Display Card Number

Display the card information when authenticating.

Display Person Information

Display the person information when authenticating.

Overlay Person Info. on Picture

Display the person information on the captured picture.

Voice Prompt

If you enable this function, the voice prompt is enabled in the device. You can hear the voice prompt when operating in the device.

Upload Pic. After Linked Capture

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

Save Pic. After Linked Capture

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

Press Key to Enter Card Number

If you enable this function, you can input the card No. by pressing the key.

Wi-Fi Probe

If you enable this function, the device can probe the surrounding communication devices' MAC address and upload the MAC address to the system. If the MAC address match the specified MAC address, the system can trigger some linkage actions.

3G/4G

If you enable this function, the device can communicate in 3G/4G network.

NFC Anti-Cloning

If you enable this function, you cannot use the cloned card for authentication and further enhance security.

4. Click **OK**.

5. **Optional:** Click **Copy to**, and then select the access control device(s) to copy the parameters in the page to the selected device(s).

Configure Parameters for Door

After adding the access control device, you can configure its access point (door) parameters.

Steps

1. Click **Access Control** → **Advanced Function** → **Device Parameter** .

2. Select an access control device on the left panel, and then click  to show the doors or floors of the selected device.

3. Select a door to show its parameters on the right page.

4. Edit the door parameters.



Note

- The displayed parameters may vary for different access control devices.
- Some of the following parameters are not listed in the Basic Information page, click **More** to edit the parameters.

Dismiss Code

Create a dismiss code which can be used to stop the buzzer of the card reader (by entering the dismiss code on the keypad).



Note

- The dismiss code should be different from the authentication password.
- The length of the dismiss code is according the device, usually it should contains 4 to 8 digits.

5. Click **OK**.

6. **Optional:** Click **Copy to** , and then select the door(s) to copy the parameters in the page to the selected door(s).



Note

The door's status duration settings will be copied to the selected door(s) as well.

Configure Parameters for Card Reader

After adding the access control device, you can configure its card reader parameters.

Steps

1. Click **Access Control** → **Advanced Function** → **Device Parameter** .

- In the device list on the left, click  to expand the door, select a card reader and you can edit the card reader's parameters on the right.
- Edit the card reader basic parameters in the Basic Information page.



Note

- The displayed parameters may vary for different access control devices. There are part of parameters listed as follows. Refer to the user manual of the device for more details.
- Some of the following parameters are not listed in the Basic Information page, click **More** to edit the parameters.

Name

Edit the card reader name as desired.

Minimum Card Swiping Interval

If the interval between card swiping of the same card is less than the set value, the card swiping is invalid. You can set it as 0 to 255.

Alarm of Max. Failed Attempts

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

Max. Times of Card Failure

Set the max. failure attempts of reading card.

Card Reader Type/Card Reader Description

Get card reader type and description. They are read-only.

Default Authentication Mode

View the default card reader authentication mode.

Fingerprint Capacity

View the maximum number of available fingerprints.

Existing Fingerprint Number

View the number of existed fingerprints in the device.

- Click **Advanced** and you can configure more parameters.

Enable Card Reader

Enable the function and you can operate the functions below on the card reader.

Buzzer Polarity

Set Buzzer Polarity of main board according to the card reader parameters. Generally, adopts the default settings.

Max. Interval When Entering PWD

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

Fingerprint Recognition Level

Select the fingerprint recognition level from the drop-down list.

Fingerprint Recognition Interval

Select the fingerprint recognition interval from the drop-down list.

5. Click **OK**.

6. **Optional:** Click **Copy to**, and then select the card reader(s) to copy the parameters in the page to the selected card reader(s).

Configure Parameters for Alarm Output

After adding the access control device, if the device links to alarm outputs, you can configure the parameters.

Before You Start

Add access control device to the client, and make sure the device supports alarm output.

Steps

1. Click **Access Control** → **Advanced Function** → **Device Parameter** to enter access control parameter configuration page.
2. In the device list on the left, click  to expand the door, select an alarm input and you can edit the alarm input's parameters on the right.
3. Set the alarm output parameters.

Name

Edit the card reader name as desired.

Alarm Output Active Time

How long the alarm output will last after triggered.

4. Click **OK**.

5. **Optional:** Set the switch on the upper right corner to **ON** to trigger the alarm output.

Configure Parameters for Lane Controller

After adding the lane controller to the client, you can configure its parameters for passing through the lane.

Before You Start

Add access control device to the client.

Steps

1. Click **Access Control** → **Advanced Function** → **Device Parameter** to enter Parameter Settings page.
2. In the device list on the left, select a lane controller and you can edit the lane controller's parameters on the right.
3. Edit the parameters.

Passing Mode

Select the controller which will control the barrier status of the device.

- If you select **According to Lane Controller's DIP Settings**, the device will follow the lane controller's DIP settings to control the barrier. The settings on the software will be invalid.
- If you select **According to Main Controller's Settings**, the device will follow the settings of the software to control the barrier. The DIP settings of the lane controller will be invalid.

Free Passing Authentication

If you enable this function, when both entrance and exit's barrier mode is Remain Open, the pedestrians should authenticate each time passing through the lane. Or an alarm will be triggered.

Opening/Closing Barrier Speed

Set the barrier's opening and closing speed. You can select from 1 to 10. The greater the value, the faster the speed.



Note

The recommended value is 6.

Audible Prompt Duration

Set how long the audio will last, which is played when an alarm is triggered .



Note

0 refers to the alarm audio will be played until the alarm is ended.

Temperature Unit

Select the temperature unit that displayed in the device status.

4. Click **OK**.

10.7.2 Configure Device Parameters

After adding the access control device, you can set its parameters such as network parameters.

Set Parameters for Face Recognition Terminal

For face recognition terminal, you can set its parameters including face picture database, QR code authentication, etc.

Steps



Note

This function should be supported by the device.

1. Enter the Access Control module.
2. On the navigation bar on the left, enter **Advanced Function** → **More Parameters** .
3. Select an access control device in the device list and click **Face Recognition Terminal**.

4. Set the parameters.

Note

These parameters displayed vary according to different device models.

COM

Select a COM port for configuration. COM1 refers to the RS-485 interface and COM2 refers to the RS-232 interface.

Face Picture Database

select Deep Learning as the face picture database.

Authenticate by QR Code

If enabled, the device camera can scan the QR code to authenticate. By default, the function is disabled.

Blocklist Authentication

If enabled, the device will compare the person who want to access with the persons in the blocklist.

If matched (the person is in the blocklist), the access will be denied and the device will upload an alarm to the client.

If mismatched (the person is not in the blocklist), the access will be granted.

Save Authenticating Face Picture

If enabled, the captured face picture when authenticating will be saved on the device.

MCU Version

View the device MCU version.

5. Click **Save**.

Set RS-485 Parameters

You can set the access control device's RS-485 parameters including the baud rate, data bit, the stop bit, parity type, flow control type, communication mode, work mode, and connection mode.

Steps

Note

The RS-485 Settings should be supported by the device.

1. Enter the Access Control module.
2. On the navigation bar on the left, enter **Advanced Function → More Parameters** .
3. Select an access control device in the device list and click **RS-485** to enter the RS-485 Settings page.
4. Select the serial port number from the drop-down list to set the RS-485 parameters.

5. Set the serial number, external device, authentication center, baud rate, data bit, stop bit, parity type, flow control type, communication mode, and working mode in the drop-down list.
6. Click **Save**.
 - The configured parameters will be applied to the device automatically.
 - When you change the working mode or connection mode, the device will reboot automatically.

Set Wiegand Parameters

You can set the access control device's Wiegand channel and the communication mode. After setting the Wiegand parameters, the device can connect to Wiegand card reader via Wiegand communication.

Steps

Note

This function should be supported by the device.

1. Enter the Access Control module.
 2. On the navigation bar on the left, enter **Advanced Function → More Parameters**.
 3. Select an access control device in the device list and click **Wiegand** to enter the Wiegand Settings page.
 4. Set the switch to on to enable the Wiegand function for the device.
 5. Select the Wiegand channel No. and the communication mode from the drop-down list.
-

Note

If you set **Communication Direction** as **Sending**, you are required to set the **Wiegand Mode** as **Wiegand 26** or **Wiegand 34**.

6. Check **Enable Wiegand** to enable the Wiegand function.
7. Click **Save**.
 - The configured parameters will be applied to the device automatically.
 - After changing the communication direction, the device will reboot automatically.

Enable M1 Card Encryption

M1 card encryption can improve the security level of authentication.

Steps

Note

The function should be supported by the access control device and the card reader.

1. Enter the Access Control module.
2. On the navigation bar on the left, enter **Advanced Function → More Parameters**.

3. Select an access control device in the device list and click **M1 Card Encryption Verification** to enter the M1 Card Encryption Verification page.
4. Set the switch to on to enable the M1 card encryption function.
5. Set the sector ID.

 **Note**

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

-
6. Click **Save** to save the settings.

10.8 Door Control

In Monitoring module, you can view the real-time status of the doors managed by the added access control device. You can also view the access details and person details.

 **Note**

For the user with door control permission, the user can enter the Monitoring module and control the door. Or the icons used for control will not show. For setting the user permission, refer to *Add User* in the user manual of the client software.

10.8.1 Control Door Status

You can control the status for the door(s), including unlock door, locking door, remaining the door unlock, remaining the door locked, remain all unlocked, etc.

Before You Start

- Add person and assign access authorization to designed person, and person will have the access authorization to the access points (doors). For details, refer to ***Person Management*** and ***Set Access Group to Assign Access Authorization to Persons*** .
- Make sure the operation user has the permission of the access points (doors). For details, refer to .

Steps

1. Click **Monitoring** to enter the status monitoring page.
2. Select an access point group on the upper-right corner.

 **Note**

For managing the access point group, refer to ***Group Management*** .

The doors in the selected access control group will display.

3. Click a door icon to select a door, or press **Ctrl** and select multiple doors.

 **Note**

For **Remain All Unlocked** and **Remain All Locked**, ignore this step.

4. Click the following buttons to control the door.

Unlock

When the door is locked, unlock it and it will be open for once. After the open duration, the door will be closed and locked again automatically.

Lock

When the door is unlocked, lock it and it will be closed. The person who has the access authorization can access the door with credentials.

Remain Unlocked

The door will be unlocked (no matter closed or open). All the persons can access the door with no credentials required.

Remain Locked

The door will be closed and locked. No person can access the door even if he/she has the authorized credentials, except the super users.

Remain All Unlocked

All doors in the group will be unlocked (no matter closed or open). All the persons can access the doors with no credentials required.

Remain All Locked

All doors in the group will be closed and locked. No person can access the doors even if he/she has the authorized credentials, except the super users.

Capture

Capture a picture manually.

 **Note**

The **Capture** button is available when the device supports capture function. The picture is saved in the PC running the client. For setting the saving path, refer to *Set File Saving Path* in the user manual of the client software.

Result

The icon of the doors will change in real-time according to the operation if the operation is succeeded.

10.8.2 Check Real-Time Access Records

The real-time access records can be displayed in the client, including card swiping records, face recognition records, skin-surface temperature information, etc. Also, you can view the person information and view the picture captured during access.

Before You Start

You have added person(s) and access control device(s) to the client. For details, refer to ***Person Management*** and ***Add Device*** .

Steps

1. Click **Monitoring** to enter monitoring module.

Real-time access records are displayed on the bottom of the page. You can view record details, including card No., person name, event time, door location, temperature, authentication type etc.

Event Type	Access Event	Other	Event Status	Normal	Exception	Show Latest Event	Enable Abnormal Temperature Prompt	
Card No.	Person Name	Event Time	Door Location	Temperature	Abnormal Temperature	Authentication Type	Person	Linked Capture Picture
		2020-05-15 17:03:44	Door1	35.6°C	No	Card/Face		
		2020-05-15 17:03:41	Door1	35.6°C	No	Card/Face		
		2020-05-15 17:03:39	Door1	35.6°C	No	Card/Face		
		2020-05-15 17:03:39	101:Door1	-	-	-		

Figure 10-4 Real-time Access Records

Note

You can right click the column name of access event table to show or hide the column according to actual needs.

2. **Optional:** Select an access point group from the drop-down list in the upper-right corner to show the real time access records of the selected group.
3. **Optional:** Check the event type and event status.

The detected events of checked type and status will be displayed in the list below.

4. **Optional:** Check **Show Latest Event** to view the latest access record.

The record list will be listed reverse chronologically.

5. **Optional:** Check **Enable Abnormal Temperature Prompt** to enable abnormal skin-surface temperature prompt.

Note

When enabled, if there is abnormal temperature information, an Abnormal Temperature window pops up when you enter Monitoring module, displaying person's picture, skin-surface temperature, card No., person name, etc.

6. **Optional:** Click an event to view person pictures (including captured picture and profile).

Note

In **Linked Capture Picture** field, you can double click the captured picture to view an enlarged picture.

7. **Optional:** Click to view surveillance details (including person's detailed information and the captured picture).

 **Note**

In the pop-up window, you can click  to view surveillance details in full screen.

Chapter 11 Dimensions

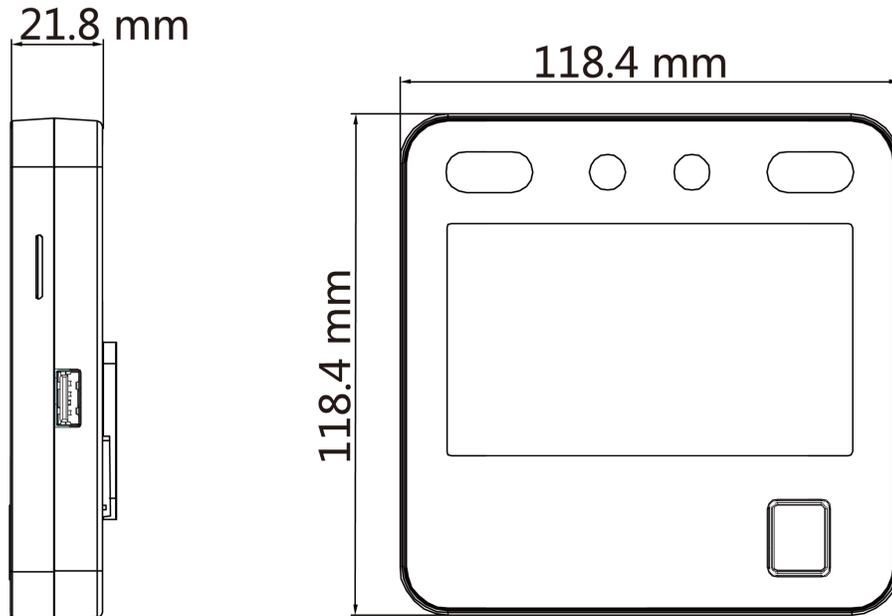


Figure 11-1 Dimensions (With Fingerprint)

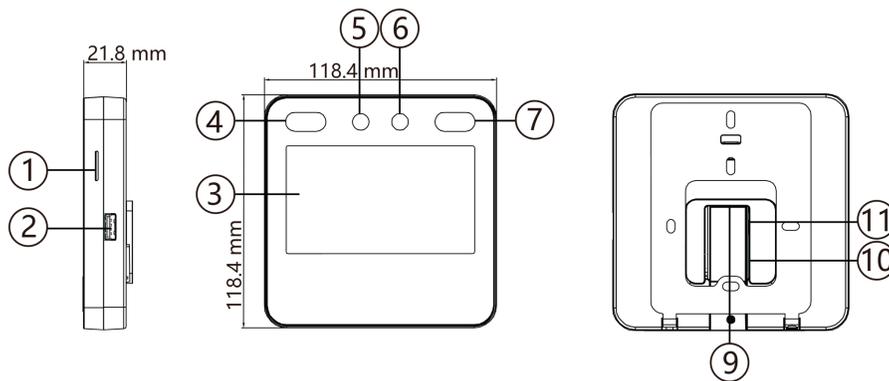


Figure 11-2 Dimensions (Without Fingerprint)

Appendix A. Tips for Installation Environment

1. Light Source Illumination Reference Value



Candle: 10Lux

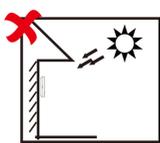


Bulb: 100~850Lux

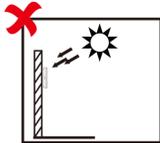


Sunlight: More than 1200Lux

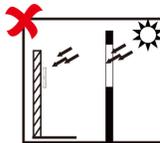
2. Avoid backlight, direct and indirect sunlight



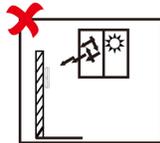
Backlight



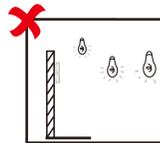
Direct Sunlight



Direct Sunlight
through Window



Indirect Light
through Window



Close to Light

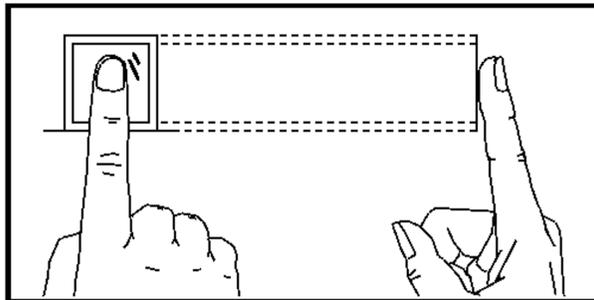
Appendix B. Tips for Scanning Fingerprint

Recommended Finger

Forefinger, middle finger or the third finger.

Correct Scanning

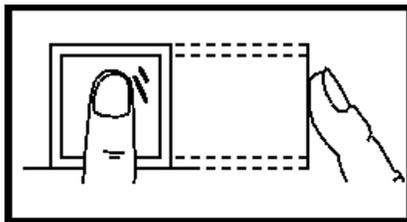
The figure displayed below is the correct way to scan your finger:



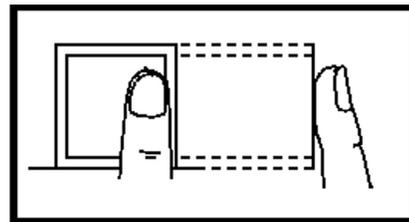
You should press your finger on the scanner horizontally. The center of your scanned finger should align with the scanner center.

Incorrect Scanning

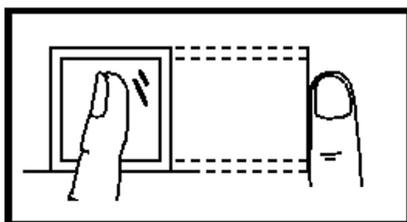
The figures of scanning fingerprint displayed below are incorrect:



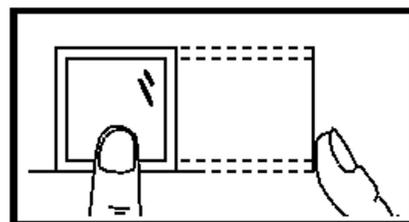
Vertical



Edge I



Side



Edge II

Environment

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

Others

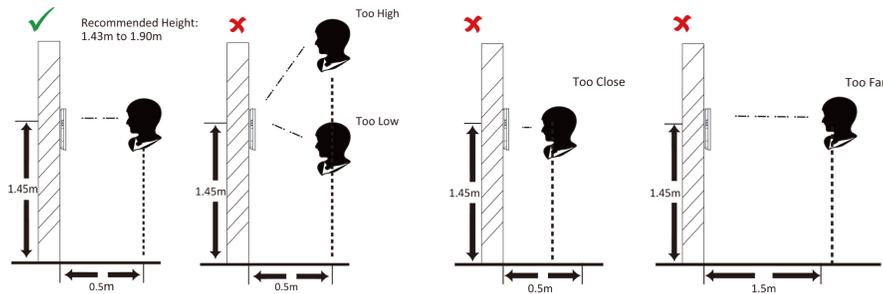
If your fingerprint is shallow, or it is hard to scan your fingerprint, we recommend you to use other authentication methods.

If you have injuries on the scanned finger, the scanner may not recognize. You can change another finger and try again.

Appendix C. Tips When Collecting/Comparing Face Picture

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

Positions (Recommended Distance: 0.5 m)



Expression

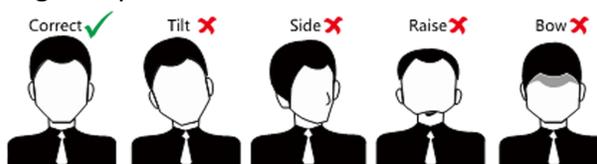
- Keep your expression naturally when collecting or comparing face pictures, just like the expression in the picture below.



- 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.

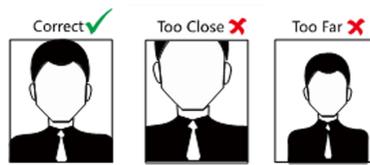
Posture

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 D. Attendance Capacity

View the attendance data capacity, including department, normal shift, man-hour shift, etc.

Content		Maximum Configuration Parameters
Department	Department Number	128
	Shift Schedule Duration (Department)	8
Shift	Normal Shift	256
	Man-Hour Shift	256
Holiday	Holiday Schedule	64
	Holiday Group	The same as the shift schedule number.
Shift Schedule	Schedule by Department	128 The same as the department number.
	Schedule by Individual	512
Time and Attendance Schedule	Shift Schedule Duration	640 The same as the shift schedule number.
	Week Schedule	The same as the shift schedule number.
	Holiday Schedule	64
	Holiday Group	The same as the shift schedule number.
	Shift Schedule Template	The same as the shift schedule number.

Appendix E. Attendance Report Table

View the exported attendance table name, content, data name, etc.

Description of Attendance Report File Name

- KaoQinHuiZong.xls: Attendance Summary Table
- Attendance Record.xls: Attendance Summary Table
- KaoQinYiChang.xls: Attendance Abnormal Table
- KaoQinYiChang2.xls: When the abnormal table is more than 60,000 rows, the record will be exported in two tables. Here KaoQinYiChang2 refers to the second abnormal attendance table.
- KaoQinPaiBan.xls: Attendance Schedule Table
- PuTongBan.xls: Normal Shift Table
- export_pic: Face Data Exporting File Name
- recordList_Serial No.csv: Event and Data
- acs.db/attend.db/userdata_config/enrIFace: User Data
- devCfg.json: Configuration File

Attendance Report Table Content

Table E-1 Attendance Schedule Table

Attendance Schedule														
Create Time: 2021/02/22 10:35														
Export Date: 2021/02/01														
Employee ID	Name	Department	Shift Schedule Type	01	02	03							
				One	Two	Three							

Attendance Schedule Table: All users' shift schedules for a duration will be displayed in this table. You are able to set the shift schedule and the holiday (No attendance recorded during the holiday) in shift schedule configuration.

- Employee ID: The user's ID No.
- Name: The user's name.
- Department: The department of the user.
- Shift Schedule Type: Schedule by department or by individual.

Table E-2 Shift Table

Shift Table									
Create Time: 2021/02/22 10:35									
Shift No.	Shift Name	Duration 1		Duration 2		Duration 3		Duration 4	
		Start	End	Start	End	Start	End	Start	End
1	Normal Shift 1	09:00	18:00	00:00	00:00	00:00	00:00	00:00	00:00
2	Normal Shift 2	08:00	17:00	00:00	00:00	00:00	00:00	00:00	00:00
3	Normal Shift 3	09:00	12:00	13:00	18:00	00:00	00:00	00:00	00:00

Shift Table: Attendance by the configured time duration.

For example: If set Duration 1 as 9:00 (Start) and 18:00 (End), it is effective for the user to take attendance between 9:00 and 18:00.

Combining with the attendance rule, you are able to set multiple attendance types.

Table E-3 Attendance Abnormal Table

Attendance Abnormal Table																
Create Time: 2020-02-22 10:34																
Export Date: 2021-02-01 2021-02-22																
Employee ID	Name	Department	Date	Duration 1		Duration 2		Duration 3		Duration 4		Late Duration (min)	Early Leave (min)	Insufficient Work Hour (min)	Total (min)	Note
				Start Work	End Work											

Abnormal Attendance Table: Calculate the abnormal attendance according to the attendance records and the shift schedule configuration.

- Employee ID: The user's ID No.
- Card No.: The user's card No.
- Department: The department of the user.
- Date: The date of the abnormal attendance generated.
- Start Work - End Work: Set 4 time durations (start work and end work). It records the attendance time of each user every day.

- Late Duration (min): The start work attendance time is later than the normal start work time.
- Early Leave Duration (min): The end work attendance time is earlier than the normal end work time.
- Insufficient Work Hour: The start work duration is not sufficient.
- Total: The absence time duration of the day.

Table E-4 Attendance Summary Table

Attendance Summary Table																								
Create Time: 2021-02-22 08:36:26																								
Export Date: 2021-02-01 20201-02-22																								
Employee ID	Name	Department	Work Duration		Late		Early Leave		Overtime Work		Insufficient Work Hour		Attendance (Day)	Absences (Day)	Business Trip (Day)	Ask for Leave (Day)	Additional Salary					Actual Salary	Note	
			Standard (min)	Actual (min)	Times	Duration (min)	Times	Duration (min)	Normal	Special	Times	Duration (min)					Remark	Overtime Work	Subsidy	Late / Early Leave	Personal Leave			Deduction

Attendance Summary Table: Calculate the user attendance information in a duration of time.

- Employee ID: User ID
- Name: The user's name.
- Department: The user's department.
- Work Duration: Standard work duration and actual work duration.
- Late: The start work attendance time is later than the normal start work time. Late arriving for no more than once every day.
- Early Leave: The end work attendance time is earlier than the normal end work time. Early leave for no more than once every day.
- Overtime Work: Normal overtime work duration and special overtime work duration.
- Insufficient Work Hour: Times and duration of insufficient work hours.
- Absence: Total absence days.
- Business trip: Total business trip days.
- Ask for Leave: Total ask for leave days.

- Subsidy: According to remarks, overtime work, late/early leave, personal leave, and deduction, the company can view the increase and decrease.
- Actual Salary: Calculate the user's actual salary.

Table E-5 Attendance Record Table

Attendance Record Table			
Create Time: 2021/05/20 14:49			
Made Date: 2021/05/01			
Employee ID	Name	Department	Attendance Record

- Employee ID: User ID
- Name: The user's name.
- Department: The user's department.
- Attendance Record: The user attendance record on that day.



Note

Up to 31 days attendance record can be exported.

Appendix F. 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 F-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 F-2 Device Command



See Far, Go Further