Payment Terminal

User Manual

Legal Information

About this Document

- This Document includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only.
- The information contained in the Document is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of the Document at the Hikvision website (***https://www.hikvision.com***). Unless otherwise agreed, Hangzhou Hikvision Digital Technology Co., Ltd. or its affiliates (hereinafter referred to as "Hikvision") makes no warranties, express or implied.
- Please use the Document with the guidance and assistance of professionals trained in supporting the Product.

About this Product

- This product can only enjoy the after-sales service support in the country or region where the purchase is made.
- If the product you choose is a video product, please scan the following QR code to obtain the "Initiatives on the Use of Video Products", and read it carefully.

Acknowledgment of Intellectual Property Rights

- Hikvision owns the copyrights and/or patents related to the technology embodied in the Products described in this Document, which may include licenses obtained from third parties.
- Any part of the Document, including text, pictures, graphics, etc., belongs to Hikvision. No part of this Document may be excerpted, copied, translated, or modified in whole or in part by any means without written permission.
- HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.
- Other trademarks and logos mentioned are the properties of their respective owners.

LEGAL DISCLAIMER

- TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR

IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.

- YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.
- YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.
- IN THE EVENT OF ANY CONFLICTS BETWEEN THIS DOCUMENT AND THE APPLICABLE LAW, THE LATTER PREVAILS.

Data Protection

- To protect data, the development of Hikvision Products incorporates privacy by design principles. For example, for Products with facial recognition features, biometrics data is stored in your Products with encryption method; for fingerprint Products, only fingerprint template will be saved, which is impossible to reconstruct a fingerprint image.
- As a data controller/processor, you may process personal data, including collection, storage, use, processing, disclosure, deletion, etc. You are advised to pay attention to and comply with applicable laws and regulations related to the protection of personal data, including without limitation, conducting security controls to safeguard personal data, such as, implementing reasonable administrative and physical security controls, conduct periodic reviews and the assessments of the effectiveness of your security controls.

Symbol Conventions

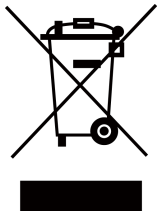
The symbols that may be found in this document are defined as follows.

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

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

This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions:
(1) this device may not cause interference, and
(2) this device must accept any interference, including interference that may cause undesired operation of the device.
Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radioexempts de licence. L'exploitation est autorisée aux deux conditions suivantes :
(1) l'appareil ne doit pas produire de brouillage, et
(2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.
This equipment complies with FCC/IC RSS-102 radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator & your body.
ce matériel est conforme aux limites de dose d'exposition aux rayonnements, FCC / CNR-102 énoncée dans un autre environnement.cette eqipment devrait être installé et exploité avec distance minimale de 20 entre le radiateur et votre corps.

Safety Instruction

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

The precaution measure is divided into Dangers and Cautions:

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

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

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

⚠ Danger:

- In the use of the product, you must be in strict compliance with the electrical safety regulations of the nation and region.
- Please use the power adapter, which is provided by normal company. The power consumption cannot be less than the required value.
- Do not connect several devices to one power adapter as adapter overload may cause over-heat or fire hazard.
- Please make sure that the power has been disconnected before you wire, install or dismantle the device.
- When the product is installed on wall or ceiling, the device shall be firmly fixed.
- If smoke, odors or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service center.
- If the product does not work properly, please contact your dealer or the nearest service center. Never attempt to disassemble the device yourself. (We shall not assume any responsibility for problems caused by unauthorized repair or maintenance.)
- The socket-outlet shall be installed near the equipment and shall be easily accessible.
- An all-pole mains switch shall be incorporated in the electrical installation of the building.
- The equipment has been designed, when required, modified for connection to an IT power distribution system.
- 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

- This equipment is not suitable for use in locations where children are likely to be present.
- This equipment is for use only with DS-K1T341 mounting plate, bracket. Use with other (carts, stands, or carriers) may result in instability causing injury.
- To prevent possible hearing damage, do not listen at high volume levels for long periods.

⚠ Cautions:

- No naked flame sources, such as lighted candles, should be placed on the equipment The USB port of the equipment is used for connecting to a mouse, a keyboard, or a USB flash drive only.
- The serial port of the equipment is used for debugging only.
- Burned fingers when handling the back panel. Wait one-half hour after switching off before handling the parts.
- 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).
- Install the equipment according to the instructions in this manual. To prevent injury, this equipment must be securely attached to the floor/wall in accordance with the installation instructions.
- Do not place the device in extremely hot (refer to the specification of the device for the detailed operating temperature), cold, dusty or damp locations, and do not expose it to high electromagnetic radiation.
- The device cover for indoor use shall be kept from rain and moisture.
- Exposing the equipment to direct sun light, low ventilation or heat source such as heater or radiator is forbidden (ignorance can cause fire danger).
- Do not aim the device at the sun or extra bright places. A blooming or smear may occur otherwise (which is not a malfunction however), and affecting the endurance of sensor at the same time.
- Please use the provided glove when open up the device cover, avoid direct contact with the device cover, because the acidic sweat of the fingers may erode the surface coating of the device cover.
- Please use a soft and dry cloth when clean inside and outside surfaces of the device cover, do not use alkaline detergents.
- Please keep all wrappers after unpack them for future use. In case of any failure occurred, you need to return the device to the factory with the original wrapper. Transportation without the original wrapper may result in damage on the device and lead to additional costs.

- Improper use or replacement of the battery may result in hazard of explosion. Replace with the same or equivalent type only. Dispose of used batteries according to the instructions provided by the battery manufacturer.
- Biometric recognition products are not completely applicable to anti-spoofing environments. If you require a higher security level, use multiple authentication modes.
- Indoor and outdoor use. If installing the device indoors, the device should be at least 2 meters away from the light, and at least 3 meters away from the window or the door. If installing the device outdoors, you should apply Silicone sealant among the cable wiring area to keep the raindrop from entering.
- Input voltage should meet both the SELV (Safety Extra Low Voltage) and the Limited Power Source with 100~240 VAC or 12 VDC according to the IEC60950-1 standard. Please refer to technical specifications for detailed information.

Available Models

Product Name	Model	Wireless
Payment Terminal	DS-K6301X-DT	13.56 MHz Card Presenting Frequency, Wi-Fi, 2.4 G
	DS-K6301X-T	13.56 MHz Card Presenting Frequency, Wi-Fi, 2.4 G
	DS-K6301X-Z	13.56 MHz Card Presenting Frequency, Wi-Fi, 2.4 G

Contents

Chapter 1 Overview 1
1.1 Overview 1
1.2 Features 1
1.3 Appearance 1
Chapter 2 Installation 8
2.1 Installation Environment 8
2.2 Mount With Cylinder Bracket 8
2.2.1 Preparation before Mounting with Bracket 8
2.2.2 Cylinder Bracket Mounting 9
2.3 Base Mounting 13
Chapter 3 Device Wiring 15
3.1 Wire on Base 15
3.2 Wire with Turnstile 15
Chapter 4 Activation 17
4.1 Activate via Device 17
4.2 Activate via Web Browser 19
4.3 Activate via SADP 19
Chapter 5 Quick Operation 21
5.1 Select Language 21
5.2 Set Network Parameters 22
5.3 Access to Platform 23
5.4 Remote Operation via APP 25
5.5 Privacy Settings 26
5.6 Add Operator 28
Chapter 6 Transaction 31
Chapter 7 Operator Mode 33

7.1 Operator Login 33
7.2 Payment Settings (Operator) 34
7.3 View Payment Statistics (Operator) 36
Chapter 8 Administrator Mode 38
8.1 Administrator Login 38
8.2 Add Operator 39
8.3 View Consumer Information 41
8.4 Payment Settings (Administrator) 42
8.5 View Payment Statistics (Administrator) 45
8.6 Communication Settings 46
8.6.1 Set Wired Network Parameters 47
8.6.2 Set Wi-Fi Parameters 48
8.6.3 Set Bluetooth 51
8.6.4 Platform Access 51
8.7 Basic Settings 52
8.8 Set Biometric Parameters 54
8.9 Data Management 55
8.9.1 Delete Data 55
8.9.2 Export Data 55
8.9.3 Import Data 56
8.10 System Maintenance 56
Chapter 9 Quick Operation via Web Browser 59
9.1 Language Settings 59
9.2 Time Settings 59
9.3 Privacy Settings 60
Chapter 10 Operation via Web Browser 61
10.1 Login 61
10.2 Overview 61

10.3 Check Transaction 62
10.4 Search Event 62
10.5 Configuration 63
10.5.1 View Device Information 63
10.5.2 Set Time 63
10.5.3 Change Administrator's Password 64
10.5.4 Online Users 64
10.5.5 View Device Arming/Disarming Information 64
10.5.6 Network Settings 65
10.5.7 Set Video and Audio Parameters 68
10.5.8 Set Image Parameters 70
10.5.9 Set Payment 70
10.5.10 Set Authentication Parameters 72
10.5.11 Set Card Security 72
10.5.12 Set Privacy Parameters 73
10.5.13 Set Biometric Parameters 74
10.5.14 Set Screen Sleep Time 76
10.5.15 Set Theme 76
10.5.16 Set Payment Prompt 76
10.5.17 Customize Audio Content 77
10.5.18 Upgrade and Maintenance 78
10.5.19 Device Debugging 79
10.5.20 Log Query 79
10.5.21 Certificate Management 79
10.5.22 View Open Source Software Statement and Help 81
Chapter 11 Operation via HikCentral Professional 82
11.1 Login 82
11.1.1 First Time Login 82

11.1.2 Login via Web Client (Administrator) 84
11.1.3 Login via Web Client (Employee) 85
11.1.4 Change Password for Reset User 86
11.1.5 Forgot Password 87
11.2 Download Mobile Client 89
11.3 Web Control 89
11.4 Home Page Overview 89
11.4.1 Customize Navigation Bar 93
11.4.2 View Digital Dashboard 95
11.4.3 Customize Preset Workbench 96
11.4.4 Customize Personal Workbench 97
11.5 Getting Started 97
11.6 License Management 98
11.6.1 Activate License - Online 99
11.6.2 Activate License - Offline 100
11.6.3 Update License - Online 103
11.6.4 Update License - Offline 104
11.6.5 Deactivate License - Online 106
11.6.6 Deactivate License - Offline 107
11.6.7 View License Details 109
11.6.8 Set SSP Expiration Prompt 112
11.7 Consumption Management 112
11.7.1 Flow Chart of Consumption Management 113
11.7.2 Configure Consumption Parameters 115
11.7.3 Manage Merchants 119
11.7.4 Add a Consumption Rule 119
11.7.5 Manage Consumption Permissions 120
11.7.6 Search for Consumption Records 127

11.7.7 Manage Consumption Report 128

Appendix A. Tips When Collecting/Comparing Face Picture 133

Appendix B. Tips for Installation Environment 134

Appendix C. Dimension 135

Chapter 1 Overview

1.1 Overview

Payment terminal is a kind of face recognition terminal for payment that supports payment via face, card, etc., which is mainly applied in department stores, canteens, companies, schools, and other situations.

1.2 Features

- Supports payment via card, and face.
- Supports custom payment prompt.
- Supports various payment modes, including unfixed amount (supported by dual screen device), fixed amount mode and time count mode.
- Supports detecting IP conflict.
- Supports max. 500,000 payment records and 100,000 user information.
- Supports circulated storage of payment records.
- Supports configuration via local device, HikCentral Professional (HCP) and Web.
- Supports communication via ISAPI.
- Supports time correction via NTP.

1.3 Appearance

Device on Turnstile Description

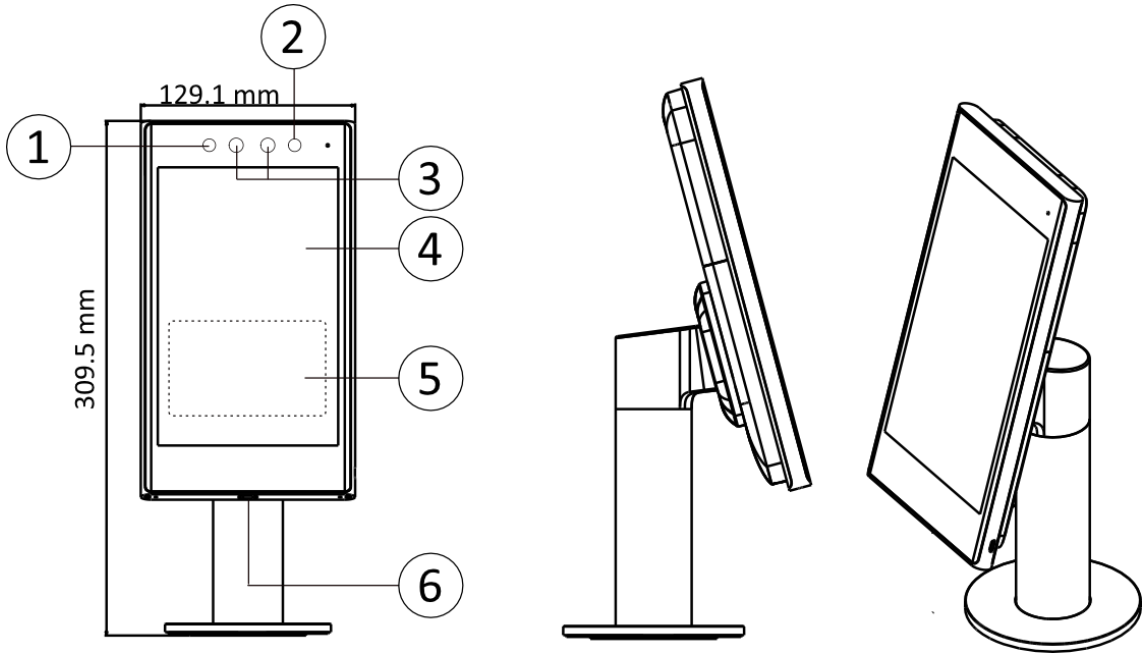


Figure 1-1 Device on Turnstile

Table 1-1 Description of Device on Turnstile

No.	Description
1	IR Light
2	IR Light
3	Camera
4	Touch Screen
5	Card Presenting Area
6	Type C interface

Device on Base (Single Screen)

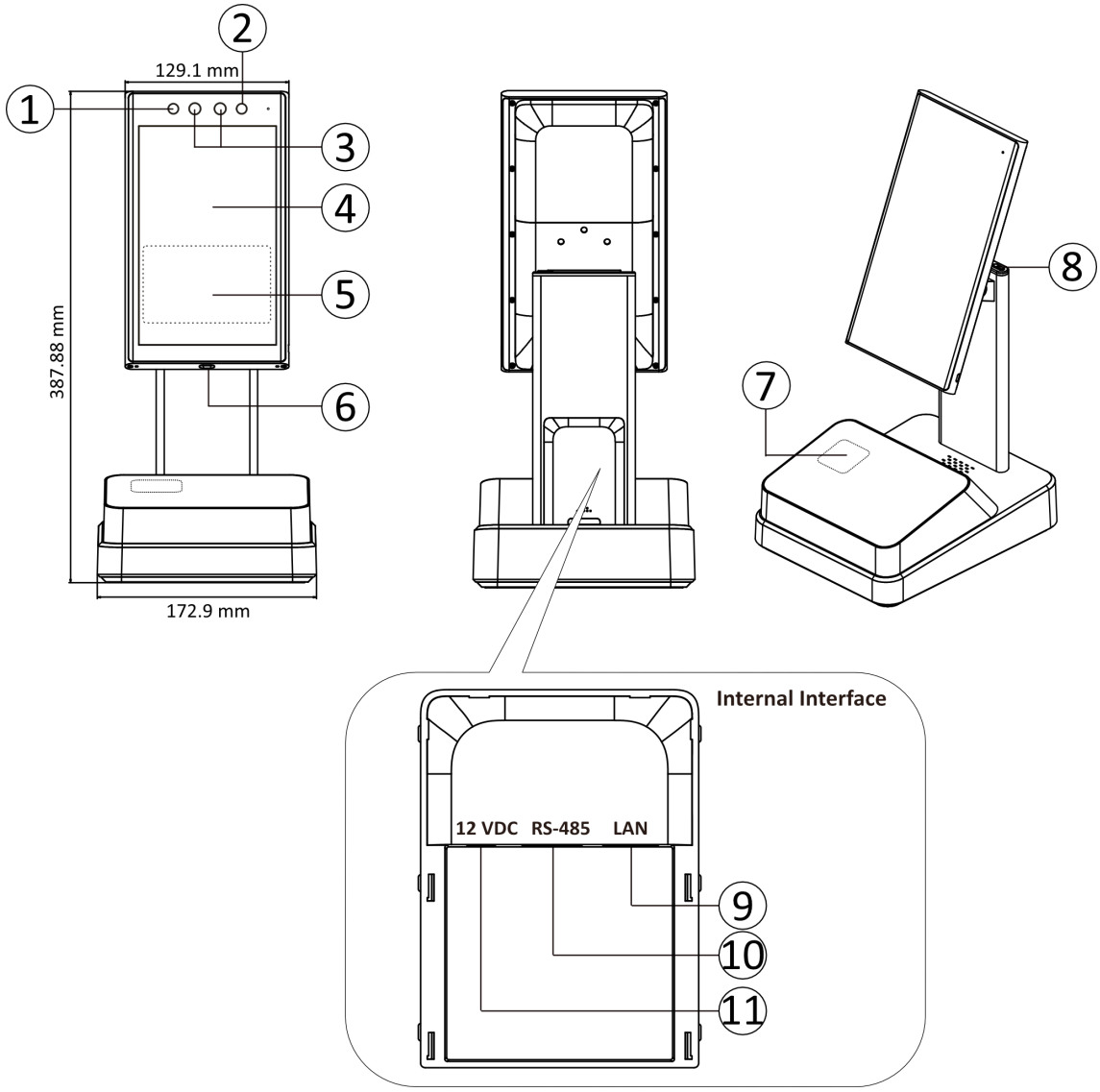


Figure 1-2 Device on Base (Single Screen)

Table 1-2 Description of Device on Base (Single Screen)

No.	Description
1	IR Light
2	IR Light
3	Camera
4	Touch Screen

No.	Description
5	Card Presenting Area
6	Type C Interface **Note** • The interface can be a debugging port. • By using a Type C to Type A cable, you can import/export data via the Type C interface with USB flash drive.
7	QR Code Recognition Area (Reserved)
8	Power Switch
9	Network Interface
10	Reserved
11	12 VDC Input

Device on Base (Dual Screen)

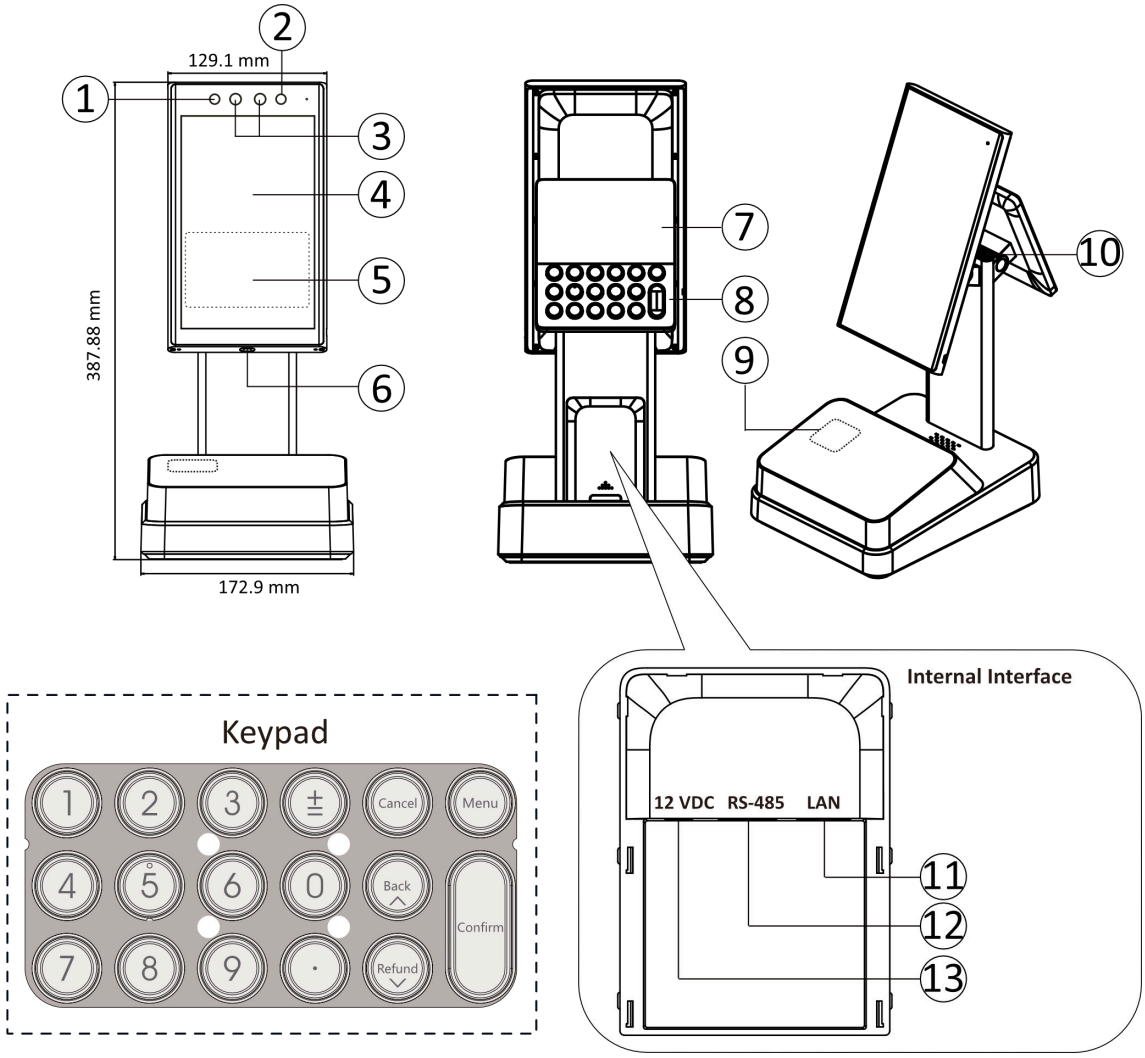


Figure 1-3 Device on Base (Dual Screen)

Table 1-3 Description of Device on Base (Single Screen)

No.	Description
1	IR Light
2	IR Light
3	Camera
4	Touch Screen
5	Card Presenting Area

No.	Description
6	Type C Interface **Note** • The interface can be a debugging port. • By using a Type C to Type A cable, you can import/export data via the Type C interface with USB flash drive.
7	Sub Screen
8	Keypad
9	QR Code Recognition Area (Reserved)
10	Power Switch
11	Network Interface
12	Reserved
13	12 VDC Input

Keypad Description

Note

Only dual screen device supports keypad.

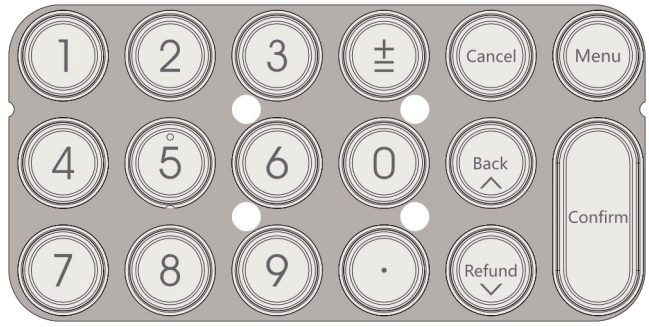


Figure 1-4 Keypad

1 to 9

Number button.

±

Plus button.

Cancel

Cancel the operation.

Back

Press once to delete one number.

Refund

The function is reserved.

Menu

Enter the function page. You can view the transaction record and statistics. Use up and down button to scroll. Press **Confirm** to make confirmation.

Confirm

Press the button to confirm the payment amount.

Chapter 2 Installation

2.1 Installation Environment

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

Note

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

2.2 Mount With Cylinder Bracket

2.2.1 Preparation before Mounting with Bracket

Make sure you have drilled holes on the turnstile. If not, follow the steps below to drill holes.

Steps

1. Use 4 screws (M3 or M4), secured by flange nuts, to install the reinforcing board on the inner surface of the turnstile.

   Note

   The distance between the turnstile and the edge should be no longer than 10 mm.

2. Drill holes on the turnstile's inner surface according to the figure displayed below. And install water-proof nut.

   Note

   Solder after pressing rivets to avoid water from entering.

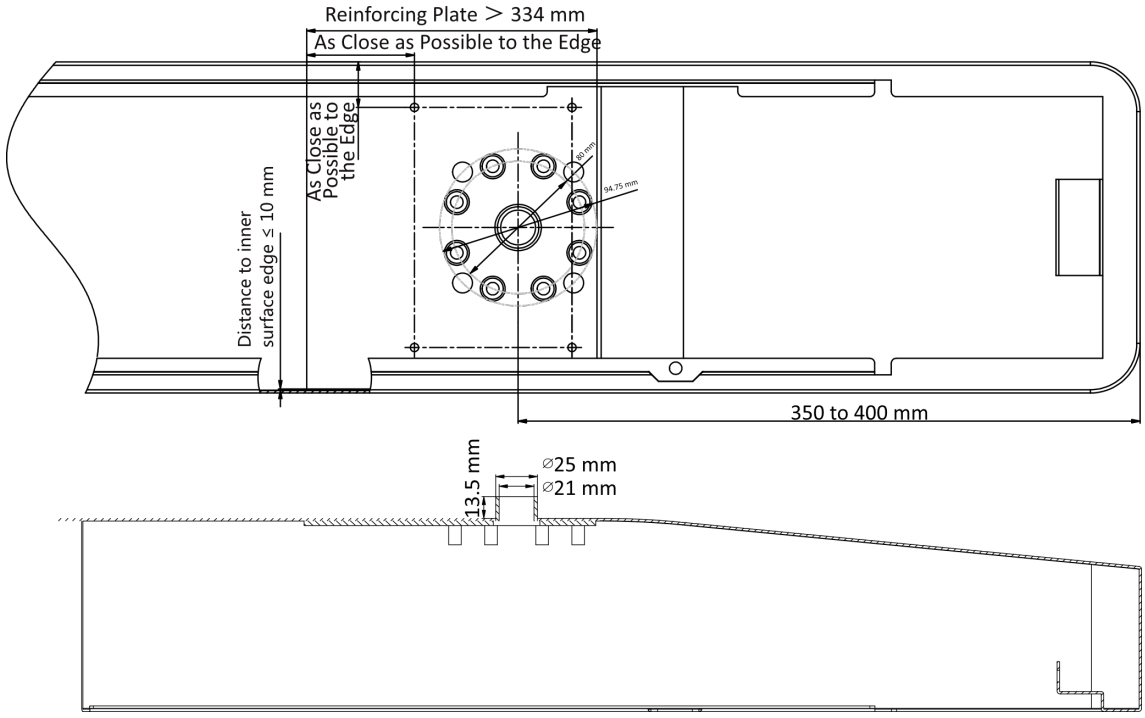


Figure 2-1 Drill Holes on Turnstile

3. Solder the other four holes, polish the surface, and implement wire drawing.
4. Solder circular tubes on the turnstile's inner surface to avoid water from entering.

2.2.2 Cylinder Bracket Mounting

Steps

1. Adjust the bracket angle.
   1) Remove 3 screws.
   2) Rotate the device sucure panel to 180° and install the 3 screws back to the bracket.

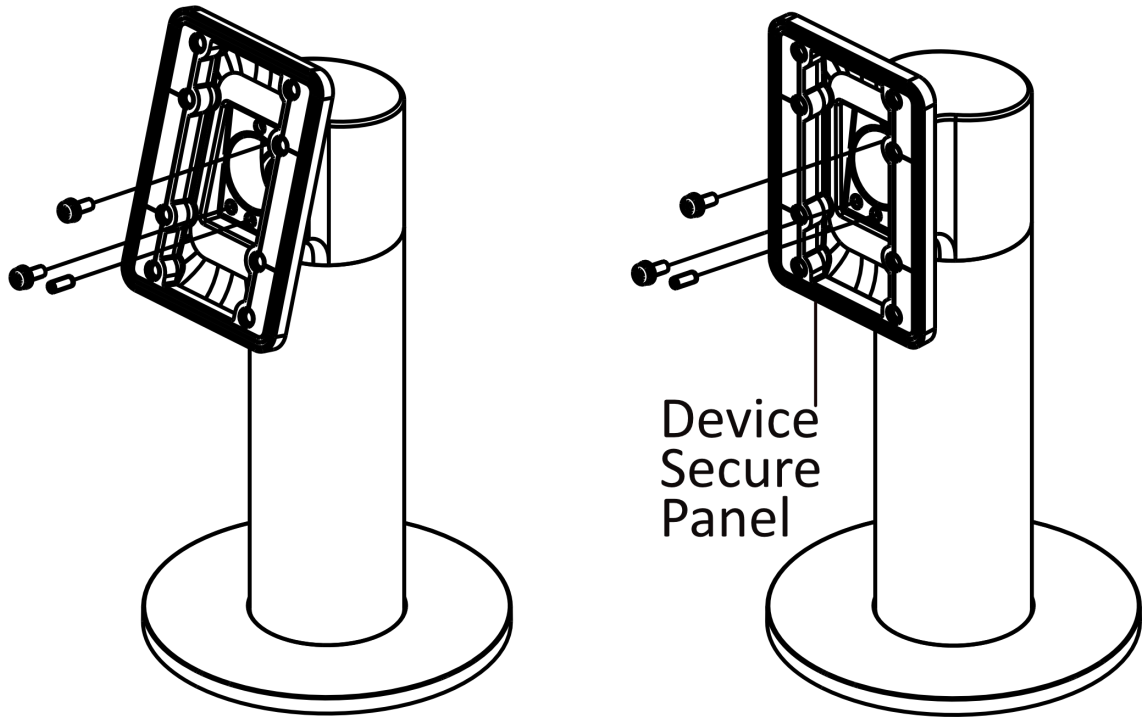


Figure 2-2 Adjust Angle

2. Route all cables through the cable hole on the turnstile. Align the holes on the bracket with those on the turnstile. Secure the bracket on the turnstile with 4 supplied screws (SC-OM6×12-H-SUS).

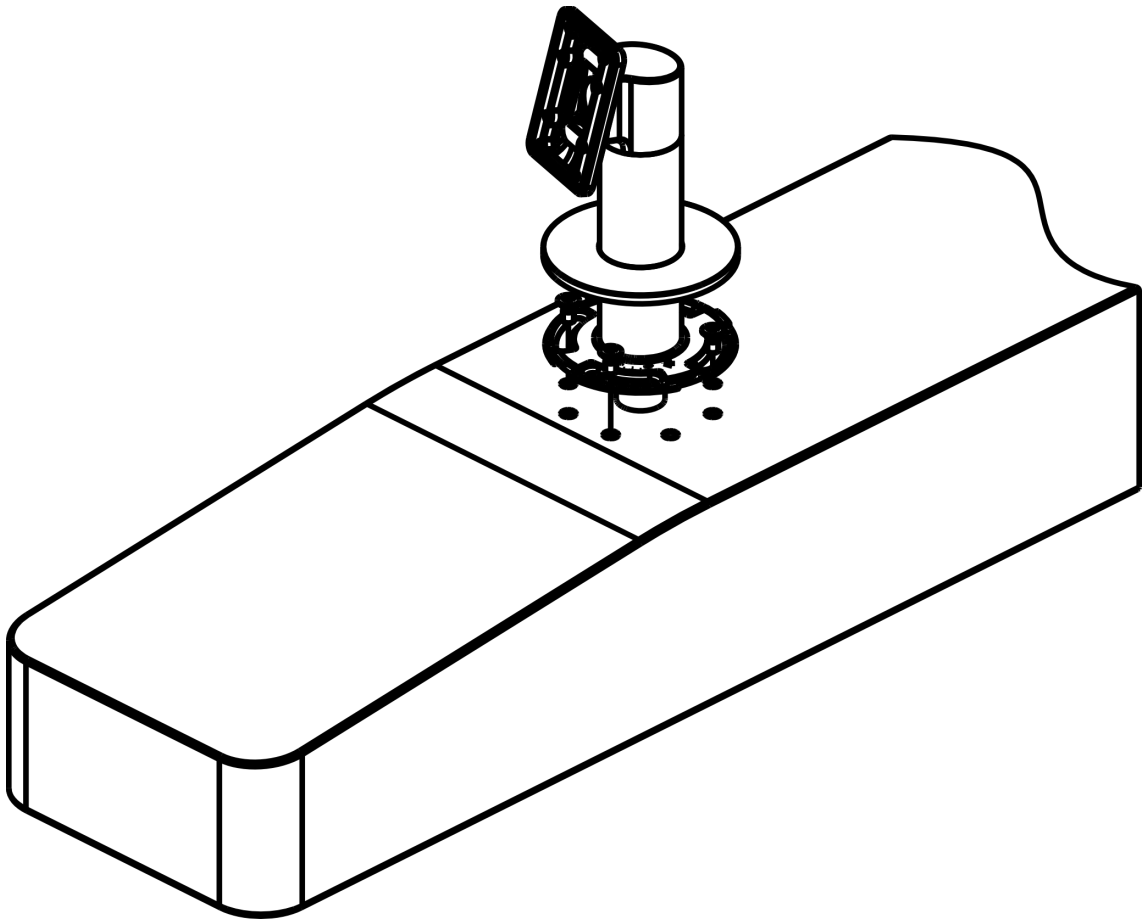


Figure 2-3 Secure Bracket

3. Secure the mounting plate on the bracket with 4 supplied screws (SC-K1M4X6-SUS).

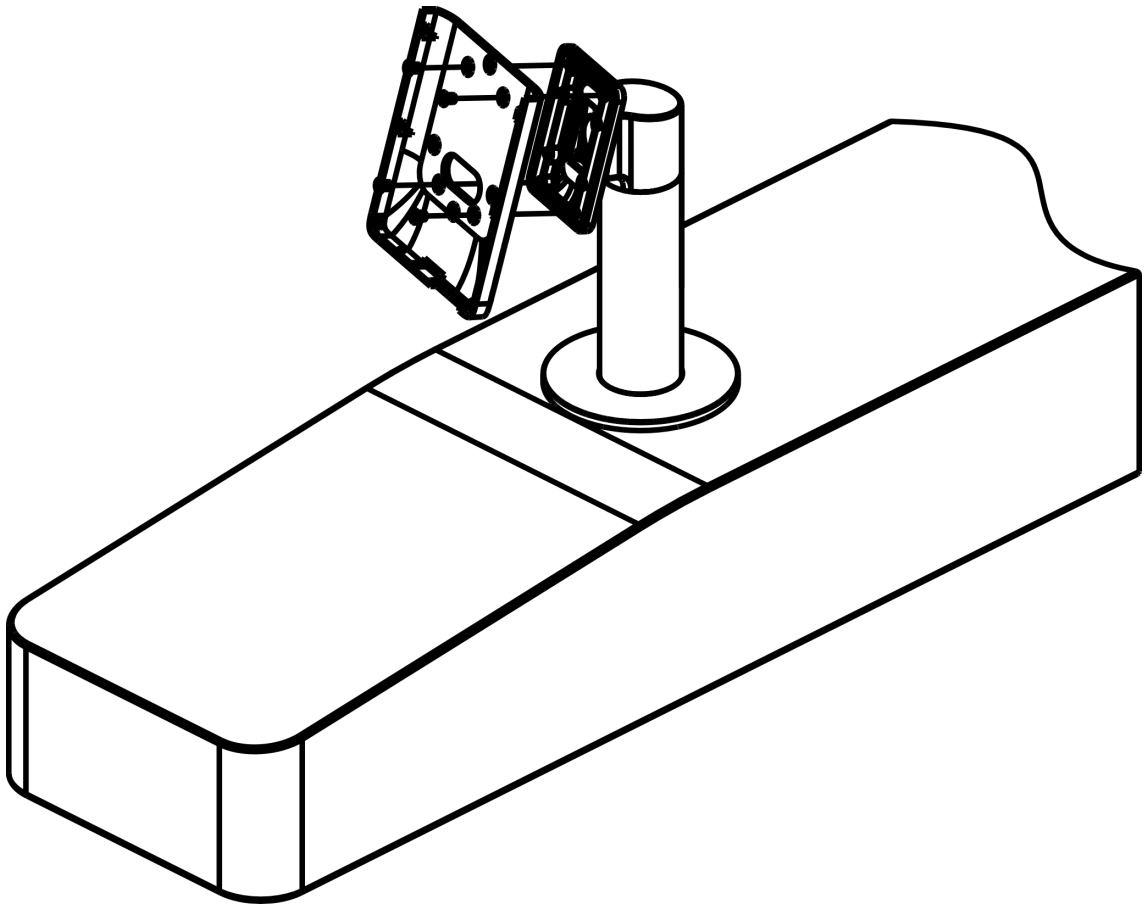


Figure 2-4 Install Mounting Plate

4. Route all cables with the terminal and hang the device on the mounting plate from top to bottom in a vertical direction, and secure the device with 1 supplied screw (SC-KM3X8-T10-SUS-NL).

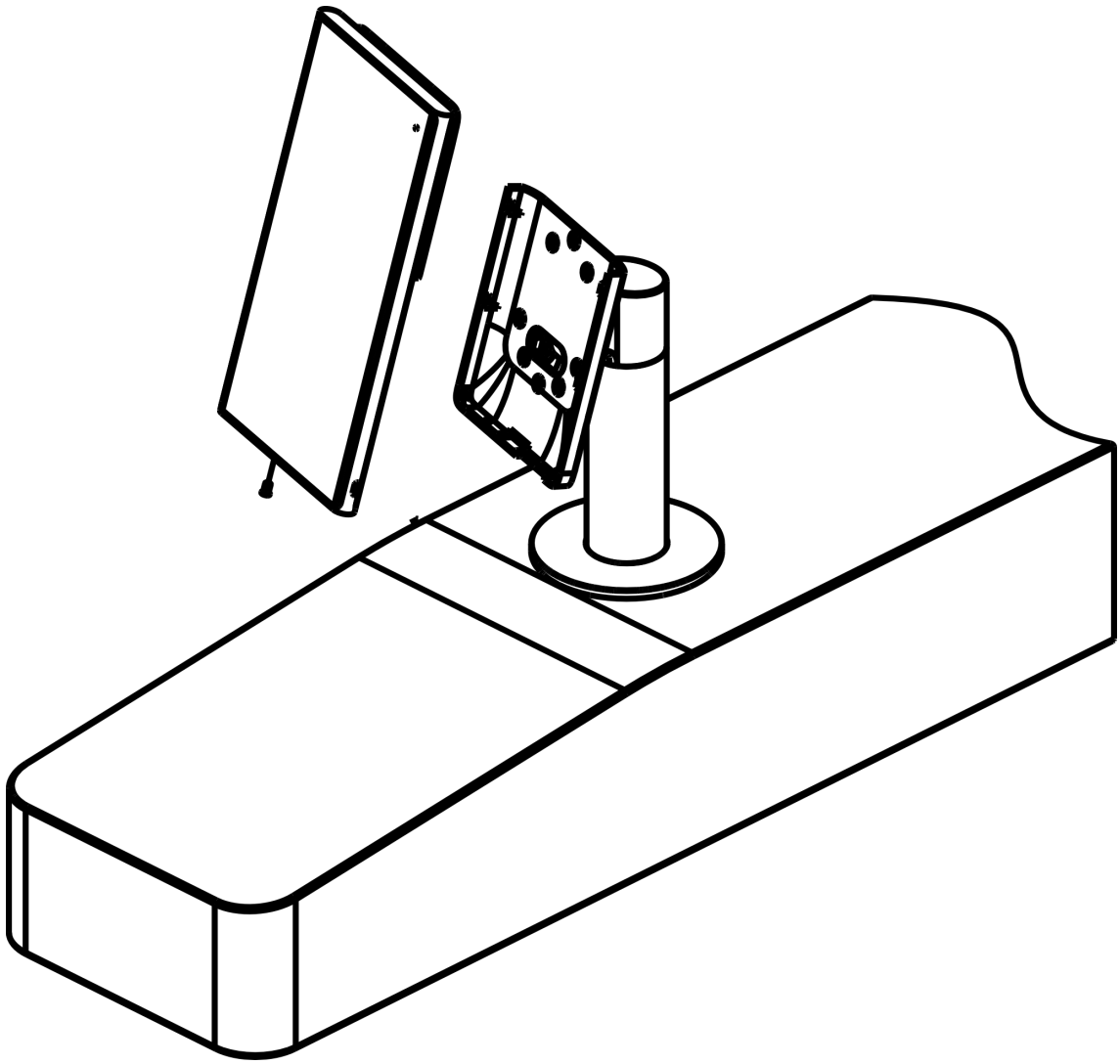


Figure 2-5 Install Device

2.3 Base Mounting

Steps

1. Place the device in a proper place.

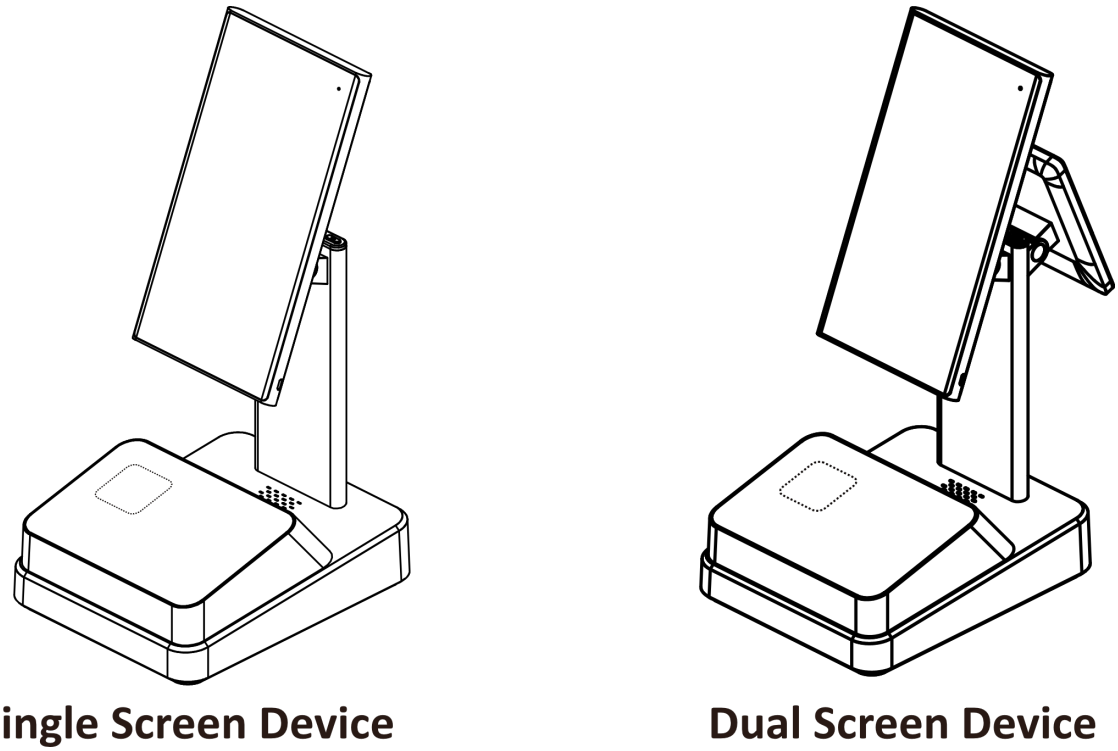


Figure 2-6 Base Mounting

2. Plug the power cable into the power input interface. After powering on, the device will enter the main interface.

Chapter 3 Device Wiring

3.1 Wire on Base

If the device can place on the base, you can follow the instructions to wire.

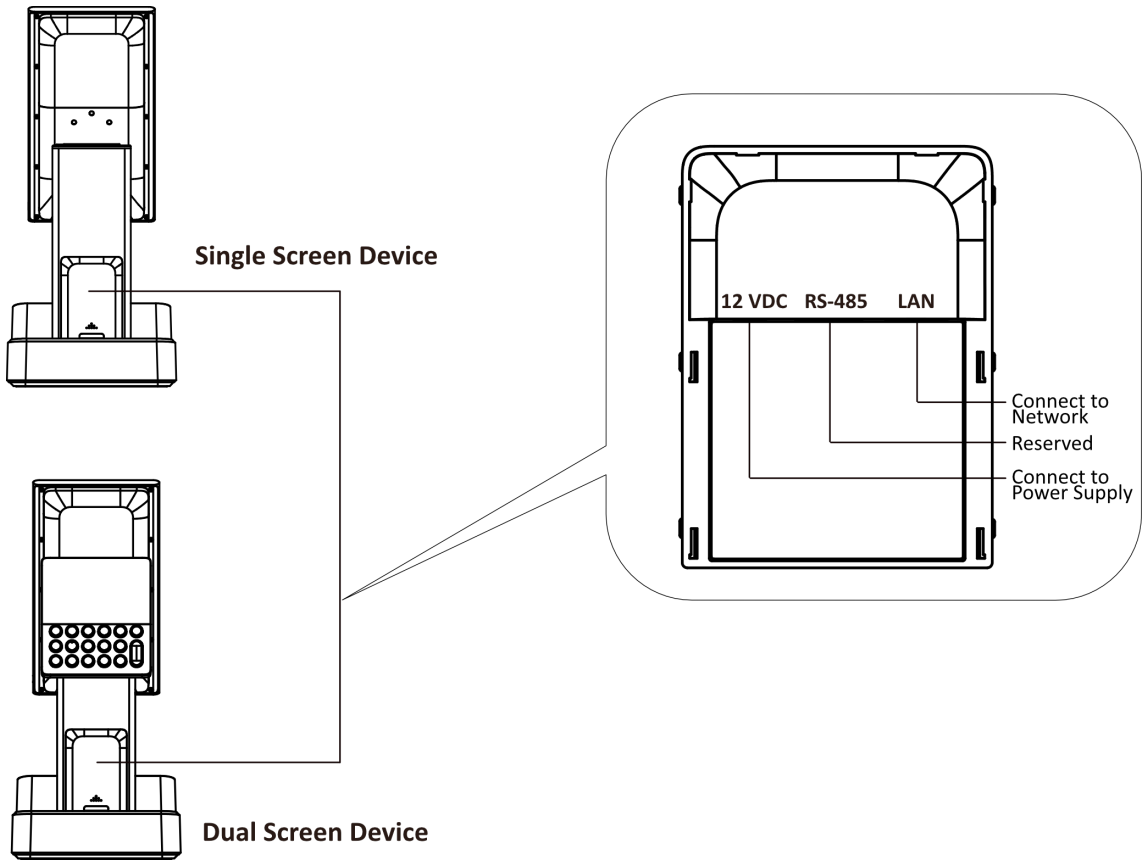


Figure 3-1 Wire on Base

3.2 Wire with Turnstile

If the device should install on the turnstile, you can follow the instructions to wire.

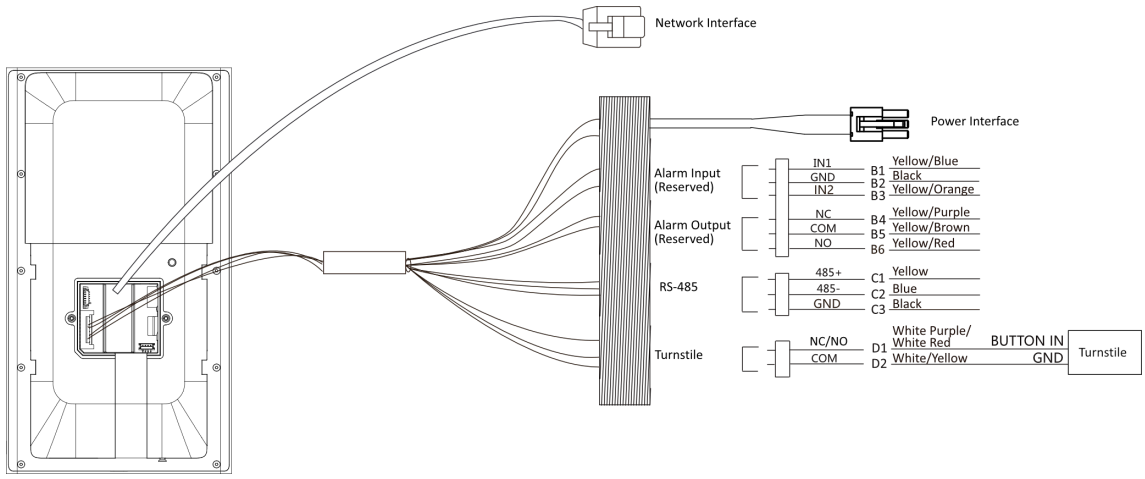


Figure 3-2 Wiring with Turnstile

Chapter 4 Activation

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

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

The default values of the device are as follows:

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

4.1 Activate via Device

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

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

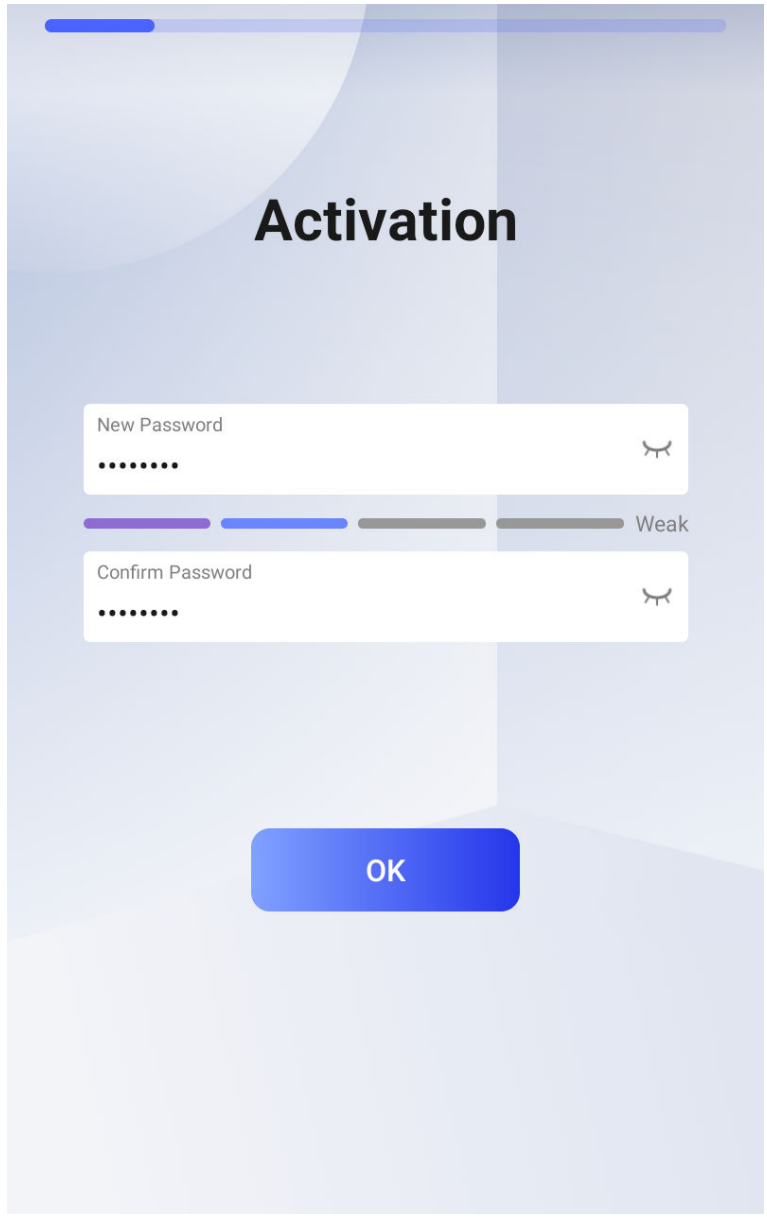


Figure 4-1 Activation Page

Caution

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

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

Note

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

4.2 Activate via Web Browser

You can activate the device via the web browser.

Steps

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

   Note

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

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

   Caution

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

   Note

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

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

4.3 Activate via SADP

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

Before You Start

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

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

Steps

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

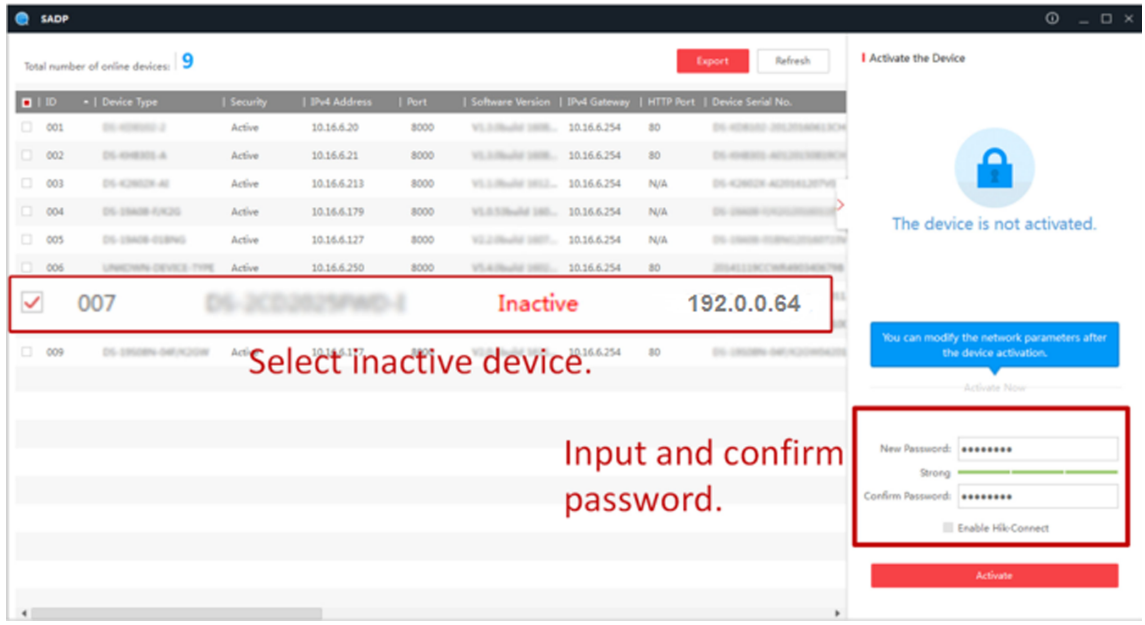
Caution

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

Note

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

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



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

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

Chapter 5 Quick Operation

5.1 Select Language

After activation, you should select a language.

Steps

1. Select a language according to the actual needs.

Figure 5-1 Select Language

2. Click **Next**.

5.2 Set Network Parameters

Set the network as wired network or wireless network.

Steps

1. Select **Wired Network** or **Wireless** and set the device network parameters.

Wired Network

Note

Make sure the device has connected to a network.

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

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

Wireless

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

Note

Disconnect the wired network before connecting a Wi-Fi.

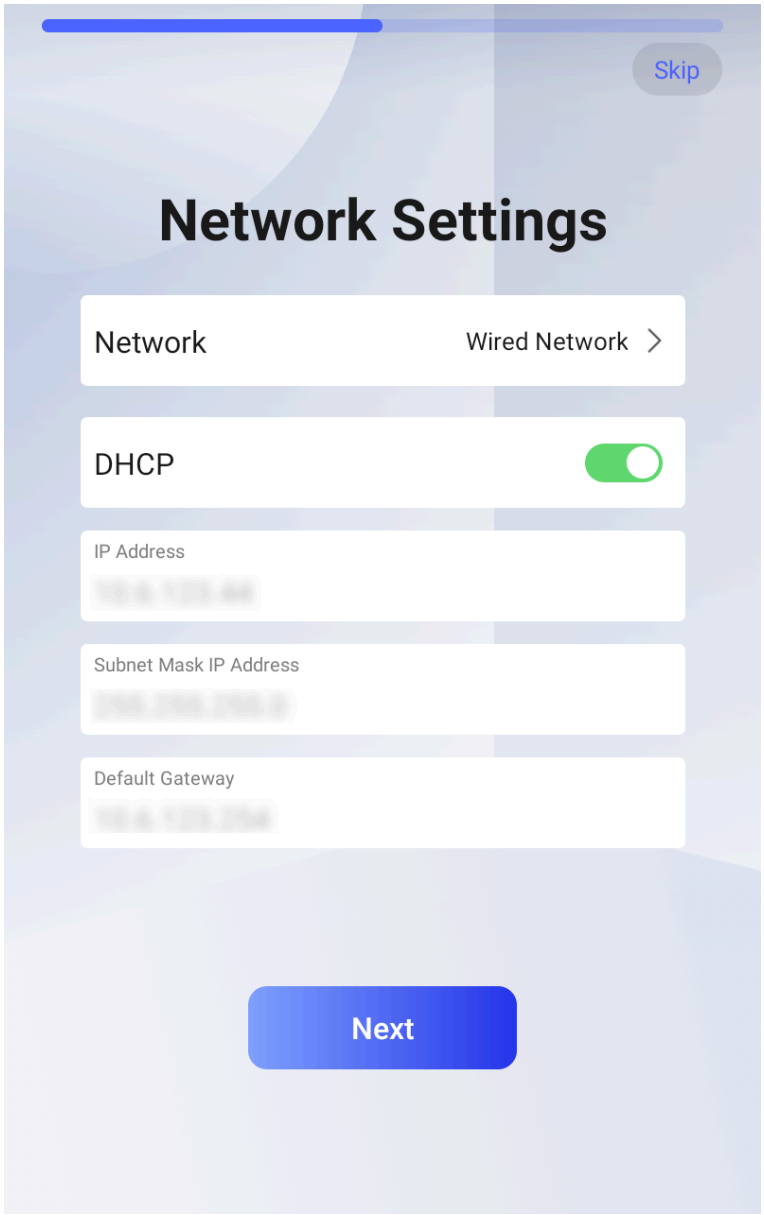


Figure 5-2 Select Network

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

5.3 Access to Platform

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

Steps

1. Enable **Hik-Connect**.

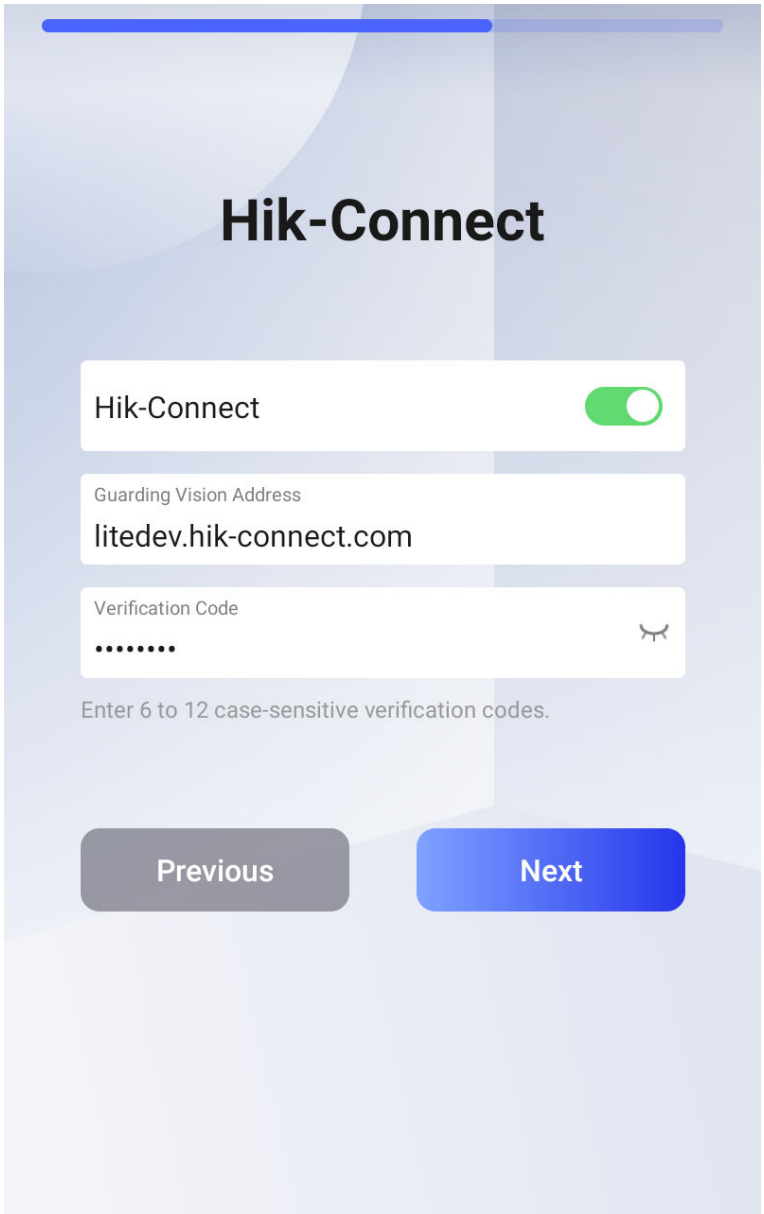


Figure 5-3 Access to Hik-Connect

2. Set the server IP and create a verification code.

Note

You should use the verification code when you adding the device to the platform.

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

Note

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

5.4 Remote Operation via APP

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

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

Follow the instruction in your mobile client to add the device. And tap **Next.**

Or tap **Previous** to go to the previous page.

Figure 5-4 Operate Remotely via APP

5.5 Privacy Settings

For personal privacy safety, you should set the privacy parameters, including the picture uploading and storage.

Check the privacy items according to your actual needs.

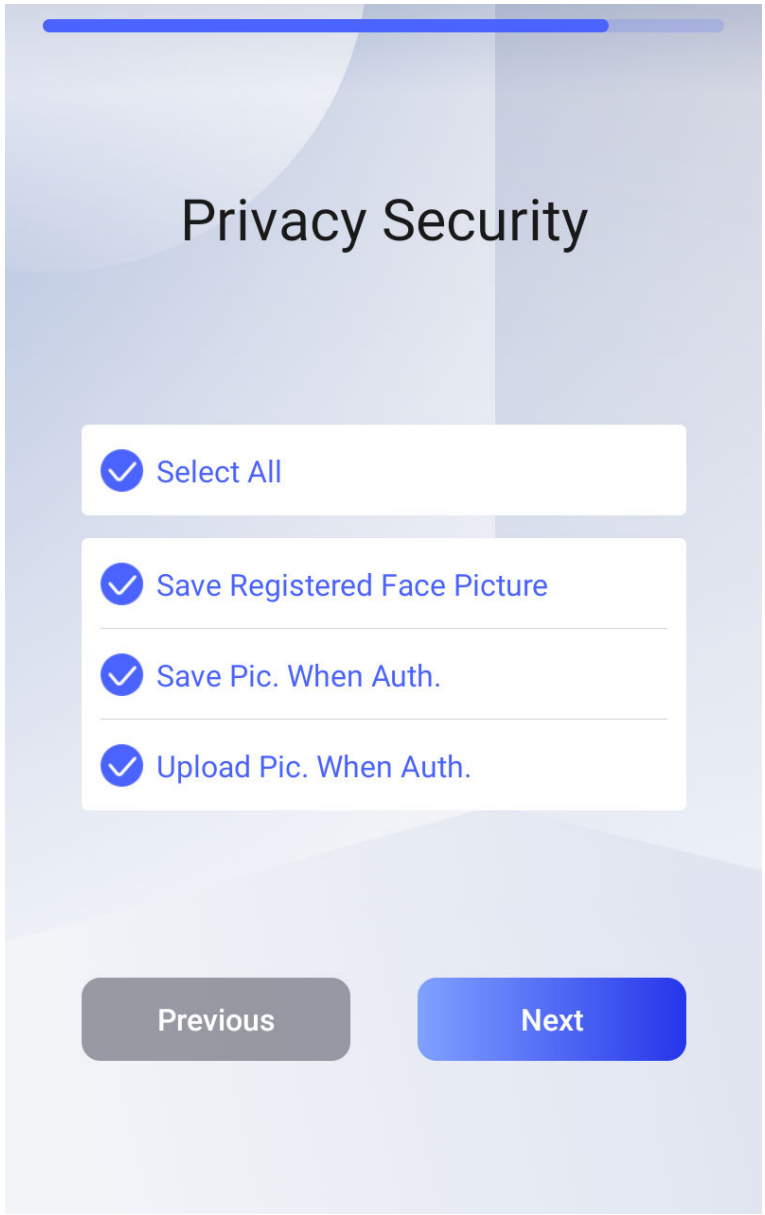


Figure 5-5 Privacy Security Settings

Note

By default, all items are selected.

Save Registered Face Picture

The registered face picture will be saved to the system.

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

The captured face pictures when authenticating will be saved to the system.

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

The captured face pictures when authenticating will be uploaded to the platform automatically.

Tap **Next** to complete the settings.

Or tap **Previous** to go to the previous page.

5.6 Add Operator

You should add an operator to manage the device parameters.

Steps

1. **Optional:** Tap **Skip** to skip adding operator if required.
2. **Optional:** Change the employee ID.
3. Enter the operator's name

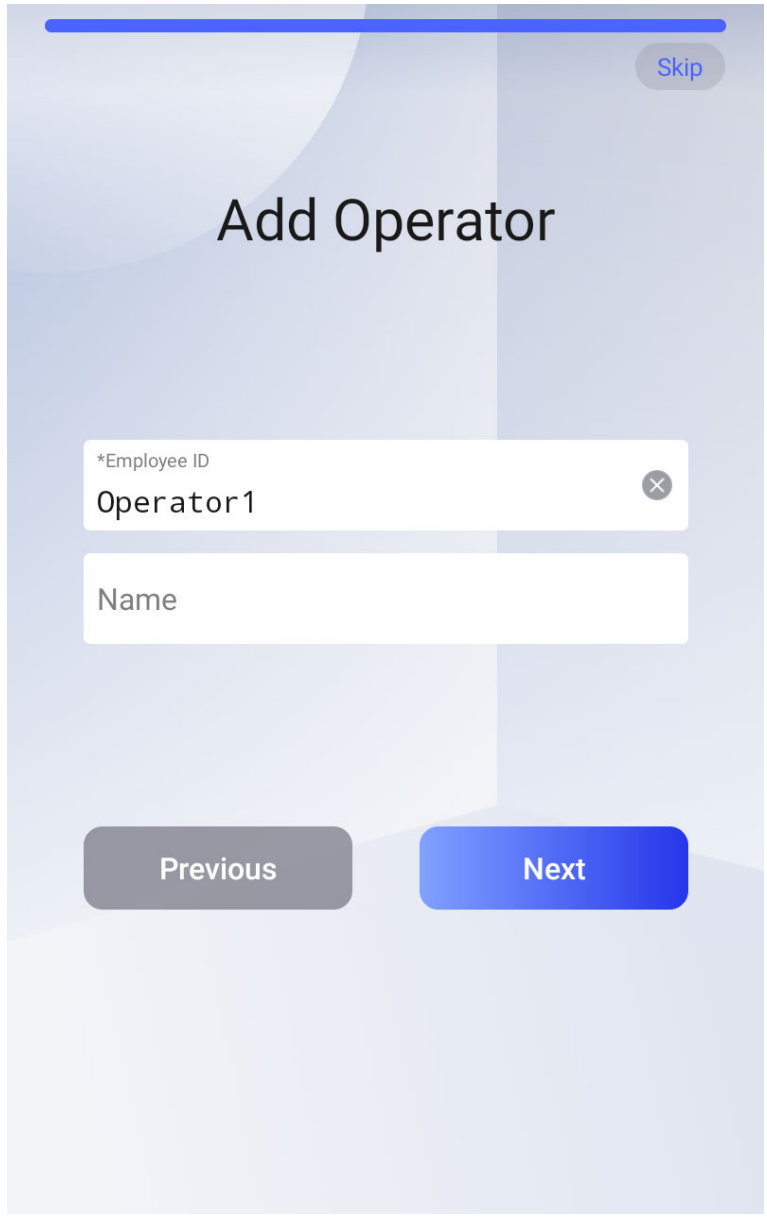


Figure 5-6 Add Operator Page

4. Tap **Next**.
5. 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.
- : Enter the card No. or present card on the card presenting area. Tap **OK**.

6. Tap **OK**.

   You will enter the authentication page.

7. Tap **Previous** to go to the previous page.

Chapter 6 Transaction

Online Transaction

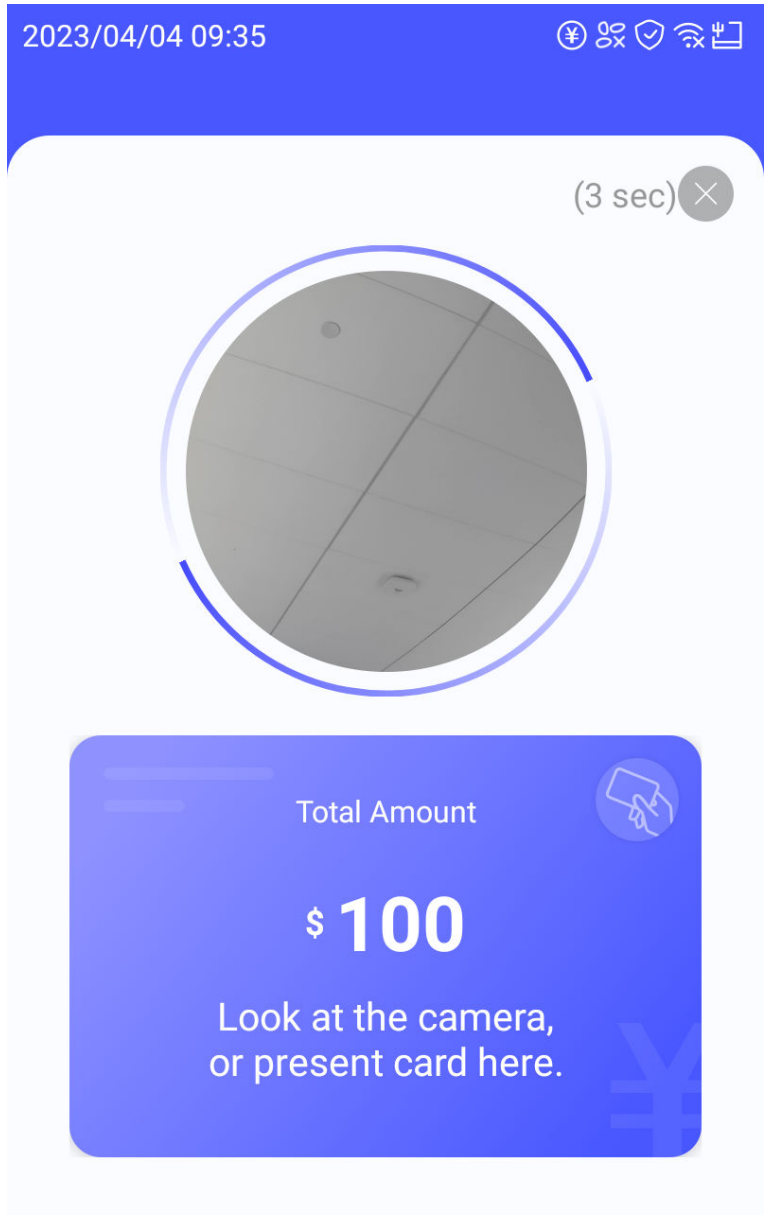


Figure 6-1 Transaction Page

Transaction via Card

Scene1: The operator enter the number on the keypad (dual screen device supported) and press **Confirm**. The consumers present card on card presenting area to pay. The device captures and

uploads pictures to the platform automatically. If the device works with other peripheral turnstiles, the gate will be automatically opened.

Scene 2: If the payment mode is fixed amount/times, the consumers can authenticate via card to transact. The device automatically uploads authentication pictures to the platform. If the device works with other peripheral turnstiles, the gate will be automatically opened.

Note

For details about settings the payment mode, see ***Payment Settings (Operator)*** or ***Payment Settings (Administrator)*** .

Transaction via Face

Scene 1: The operator enter the number on the keypad (dual screen device supported) and press **Confirm**. Consumers authenticate via face. The device automatically uploads authentication pictures to the platform. If the device works with other peripheral turnstiles, the gate will be automatically opened.

Scene 2: If the payment mode is fixed amount/times, the consumers can authenticate via face to transact. The device automatically uploads authentication pictures to the platform. If the device works with other peripheral turnstiles, the gate will be automatically opened.

Note

For details about settings the payment mode, see ***Payment Settings (Operator)*** or ***Payment Settings (Administrator)*** .

Note

- After payment via face, you need to tap **Confirm** or **Cancel**. If you have no operation in 20s, the transaction will be canceled. You can tap **Cancel** to directly cancel the transaction. The prompt for failed transaction will be triggered after the prompt is set.
- After the successful payment, if the device works with other peripheral turnstiles, the gate will be automatically opened.
- After payment via card, the device will capture pictures and upload them to the platform; After payment via face, the captured picture will be uploaded to the platform.

Chapter 7 Operator Mode

7.1 Operator Login

Operator can login the device and configure the payment parameters and view statistics.

Before You Start
You need to add an operator before operation. For details, see ***Add Operator***

Steps
1. Long tap the initial page for 3 s and slide to the left/right by following the gesture.
2. Tap **Operator**
3. Authenticate via face or card to enter the menu page of operator.

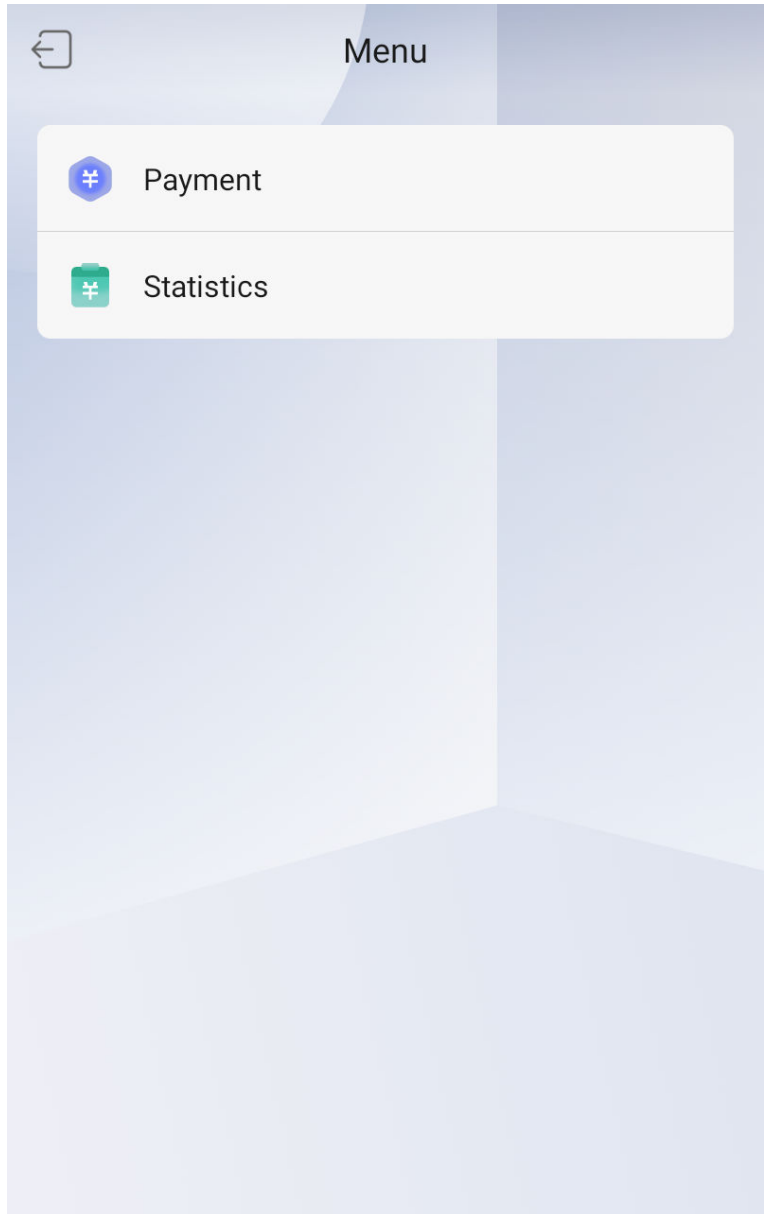


Figure 7-1 Operator Menu

4. **Optional:** Tap and you can exit the admin login page.

7.2 Payment Settings (Operator)

You can set the payment mode and other payment related parameters.

Long tap the initial page for 3 s and slide to the left/right by following the gesture. Select **Operator**, enter the password to login the menu page. Tap **Payment Settings** to enter the configuration page.

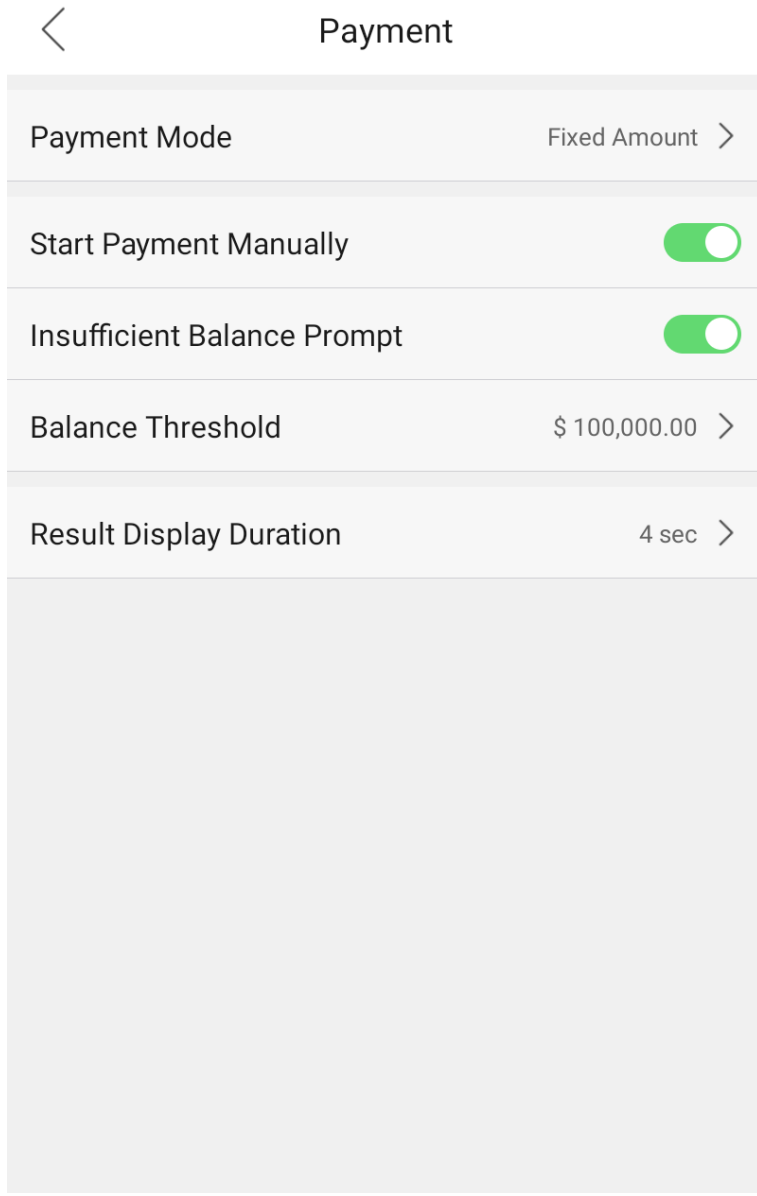


Figure 7-2 Payment Settings

Payment Mode

Current Mode

Unfixed Amount

You can set **Payment Mode** as **Unfixed Amount** if the payment amount varies. Set **Upper Limit** of the amount.

Max. Amount

By default, the Max. amount is 999,999.99.

Custom Amount

You can set a Max. amount of upper limit.

Fixed Amount

If every payment requires the same amount of money, you can set **Payment Mode** as **Fixed Amount**. **Fixed Amount** should be set for each payment between 0.00 to 999,999.99. 0 means no limits.

Enable **Show Fixed Amount**, the amount will be displayed during the payment.

Fixed Times

Pay once when use fixed times payment mode.

When the time reaches the upper limit, the system will issue prompt.

Start Payment Manually

If you select payment mode as **Fixed Amount**, and if you enable the function. You should tap **Pay** on the initial page before payment. Or the system will enter the authentication page automatically.

Insufficient Balance Prompt

If you enable the function, the system will pop up a prompt if the consumer's balance is not enough. You should set the balance threshold to complete the settings.

Result Display Duration

You can set the duration of the payment result.

7.3 View Payment Statistics (Operator)

You can view the payment records via the main device or the keypad (if supported), including **Total Payment Times**, **Total Refund Times** (reserved), **Total Payment Amount**, and **Total Refund Account** (reserved).

Operation via Main Device

Long tap the initial page for 3 s and slide to the left/right by following the gesture. Select **Operator**, and enter the password to login the menu page. Tap **Statistics** to enter the configuration page.
The device supports checking statistics within today, last 7 days, last 30 days, and custom.
If select **Custom**, you should set the **Start Time** and **End Time** of the records.
After settings the records duration, you can view **Total Payment Times**, **Total Refund Times**, **Total Payment Amount**, and **Total Refund Account**.

Note

- Due to offline records, payment statistics will be subject to data from server (client or platform).
- The refund function is reserved.

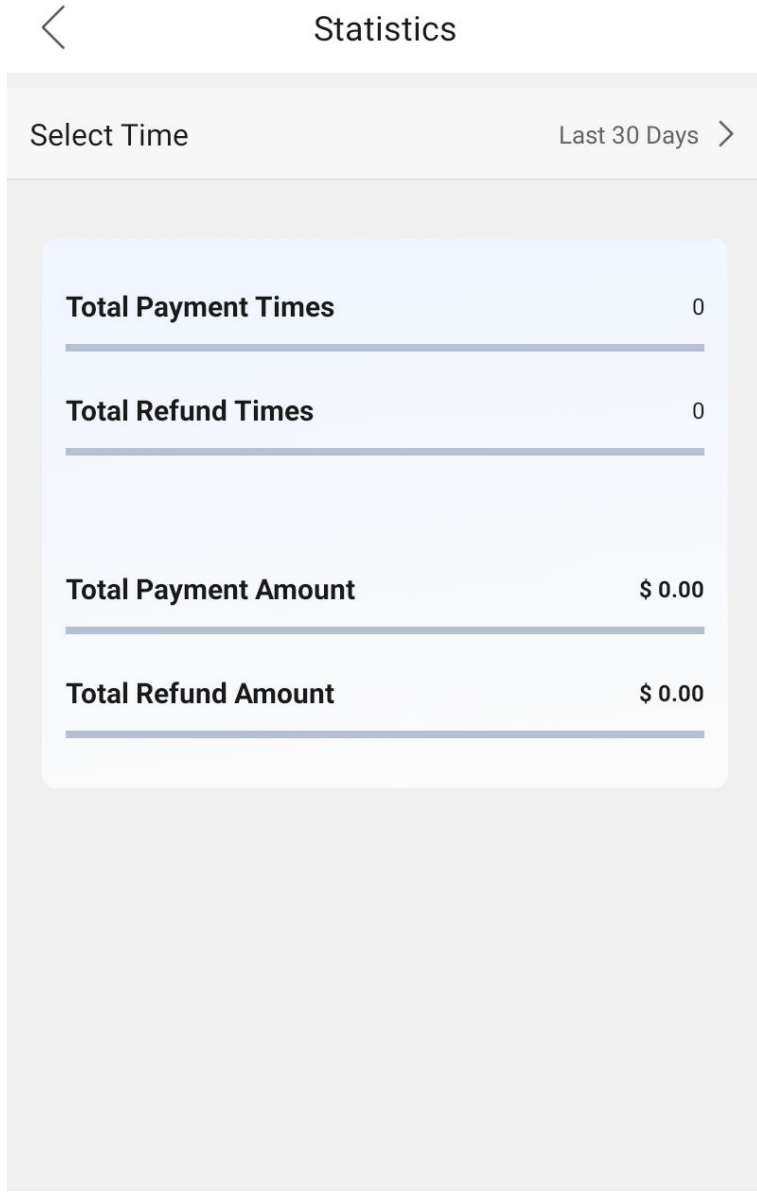


Figure 7-3 Payment Statistics

Operation via Keypad

If the device supports keypad operation, you can view the transaction record an statistics on the keypad screen.

Press **Menu** on the keypad. Press ∧ or ∨ to select **Transaction Record** or **Statistics**. Press **Confirm** to enter the page. You can view the transaction details and statistics.

Chapter 8 Administrator Mode

8.1 Administrator Login

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

Steps

1. Long tap on the initial page for 3 s and slide to the left/right by following the gesture to enter the page.
2. Tap **Administrator** on the select role page.
3. Enter the device activation password and tap **OK** to enter the administrator's menu page.

Note

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

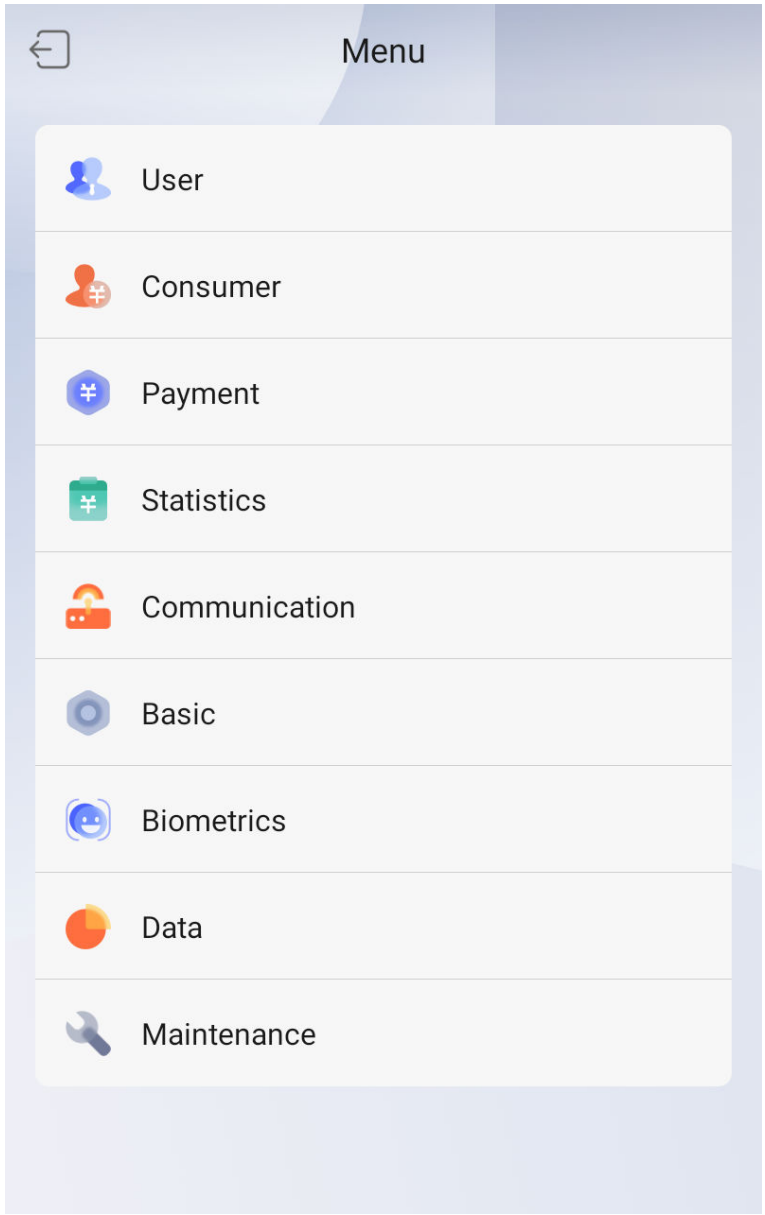


Figure 8-1 Home Page

4. **Optional:** Tap and you can exit the admin login page.

8.2 Add Operator

The operator can log in the device and configure the payment parameters and view statistics.

Steps

1. Long tap on the initial page for 3 s and slide to the left/right by following the gesture. Select **Administrator** and enter the activation password to enter the device menu page.

2. Tap **User → +** to enter the Add User page.

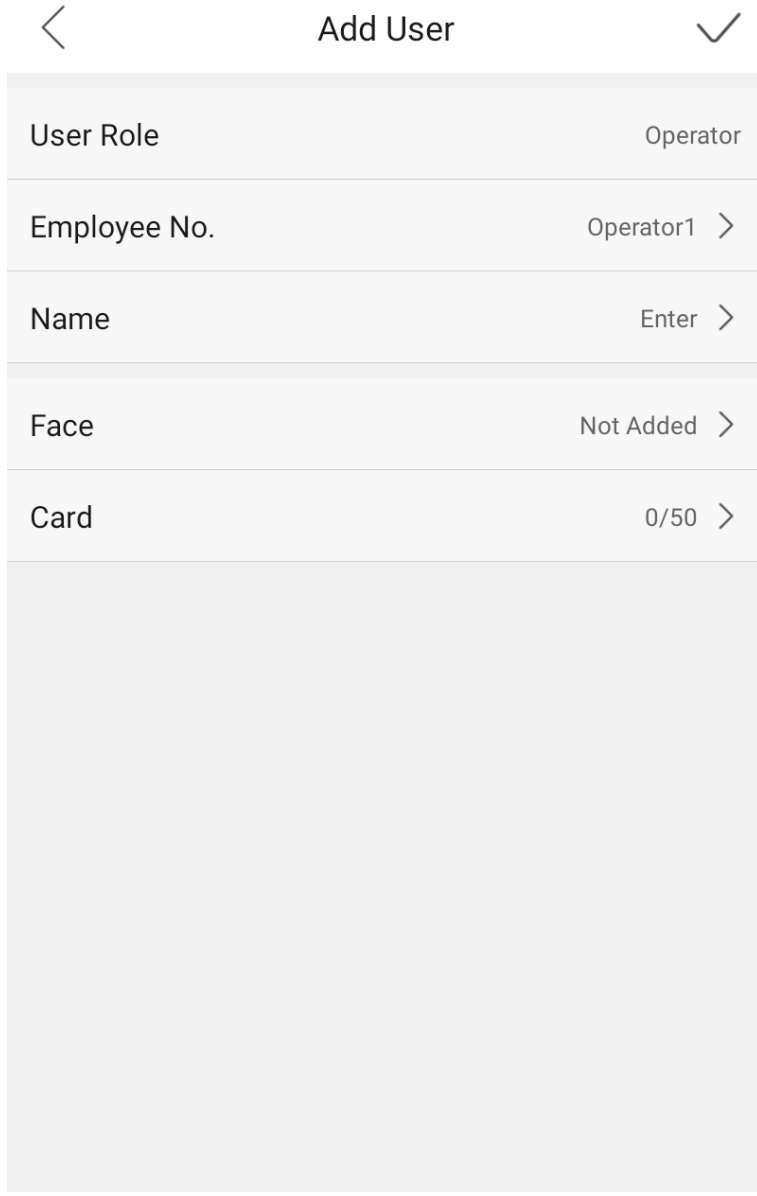


Figure 8-2 Add User

3. View the user role, change the employee No. (if needed), create a name for the operator.

Note

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

4. Optional: Add a face picture, or cards for the operator.

Note

- For details about tips of adding a face picture, see ***Tips When Collecting/Comparing Face Picture*** .

5. Tap ✓ to save the settings.

8.3 View Consumer Information

You can view consumer information by searching the ID, name or card No.

You should use HikCentral Professional (HCP) to add consumers. For details, see ***Operation via HikCentral Professional***

Long tap on the initial page for 3 s and slide to the left/right by following the gesture. Tap **Administrator** and enter the activation password to enter the device home page. Tap **Consumer**.

Enter consumer's ID, name, or card No. in the search box to view consumer information.

Note

Consumer information can be viewed here after the information is imported to the HCP platform.

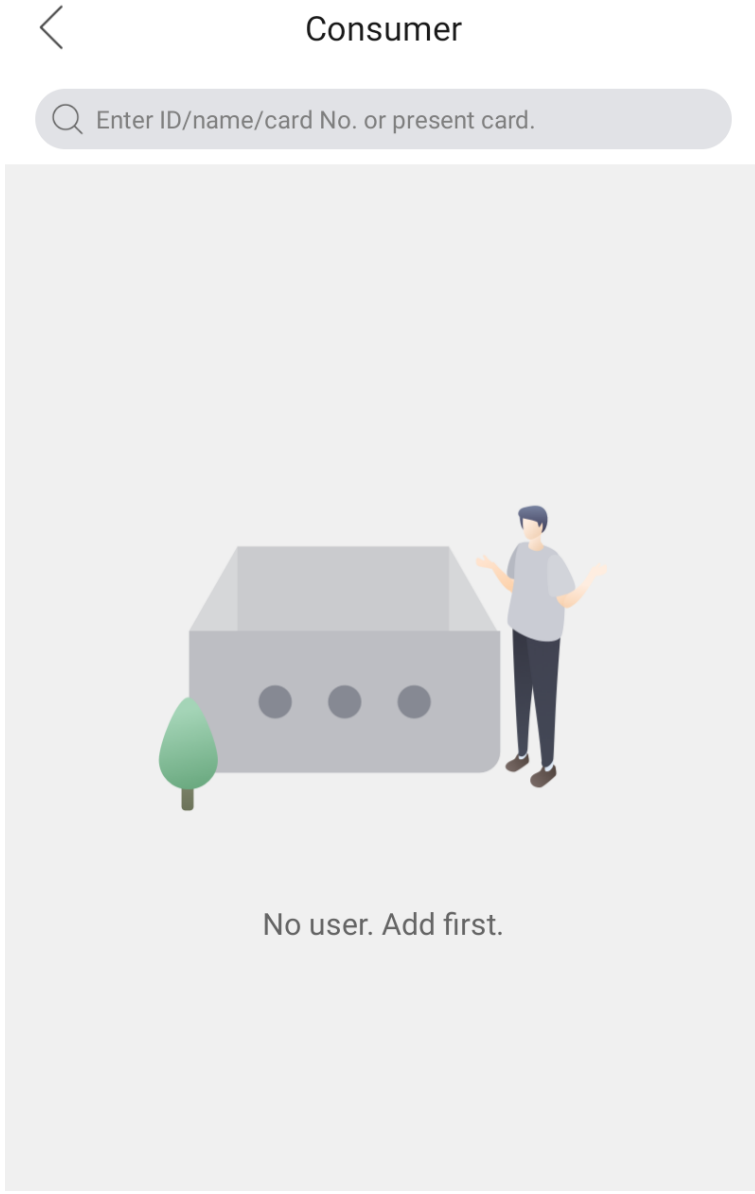


Figure 8-3 View Consumer

8.4 Payment Settings (Administrator)

You can set the payment mode, payment currency, payment parameters, and refund parameters (reserved).

Long tap the initial page for 3 s and slide to the left/right by following the gesture. Tap **Administrator**, and enter the activation password to enter home page. Tap **Payment** to enter the configuration page.

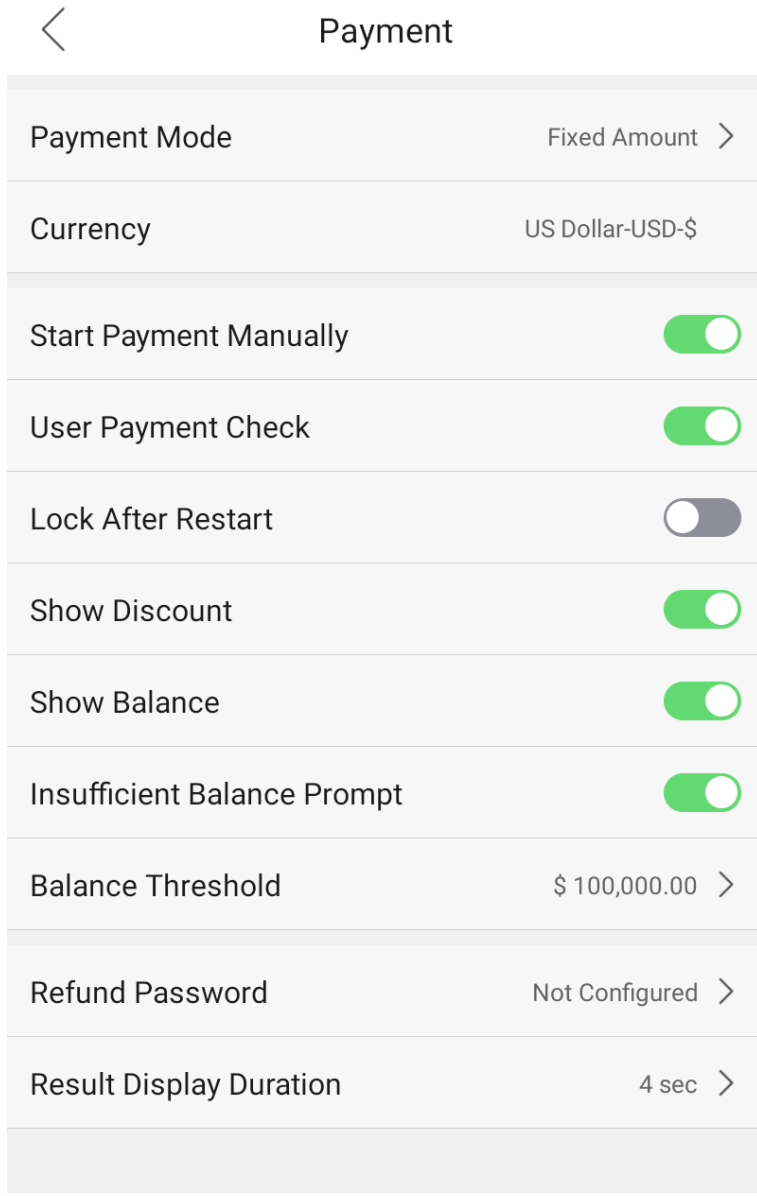


Figure 8-4 Payment Settings

Payment Mode

Current Mode

Unfixed Amount

You can set **Payment Mode** as **Unfixed Amount** if the payment amount varies. Set **Upper Limit of Single Payment** of the amount.

Max. Amount

By default, the Max. amount is 999,999.99.

Custom Amount

You can set a Max. amount of upper limit.

Fixed Amount

If every payment requires the same amount of money, you can set **Payment Mode** as **Fixed Amount**. **Fixed Amount** should be set for each payment between 0.00 to 999,999.99. 0 means no limits.

Enable **Show Fixed Amount**, the amount will be displayed during the payment.

Fixed Times

Pay once when use fixed times payment mode.

When the time reaches the upper limit, the system will issue prompt.

Currency

View the currency type. By default, it is US dollar.

You can set the currency via HikCentral Professional (HCP). For details, see ***Operation via HikCentral Professional*** .

Start Payment Manually

If you select payment mode as **Fixed Amount**, and if you enable the function. You should tap **Pay** on the initial page before payment. Or the system will enter the authentication page automatically.

User Payment Check

After enabling, you need to tap **Confirm** to finish the payment when using face authentication.

Lock After Restart

After enabling, if rebooting the device, the device will be locked. You should enter the activation password to unlock the device.

Show Discount

The discount information will be displayed on the payment page.

Show Balance

The balance will be displayed on the payment page.

Insufficient Balance Prompt

If you enable the function, the system will pop up a prompt if the consumer's balance is not enough. You should set the balance threshold to complete the settings.

Refund Password

The function is reserved.

Result Display Duration

You can set the duration of the payment result.

8.5 View Payment Statistics (Administrator)

You can view the payment records via the main device or the keypad (if supported), including **Total Payment Times**, **Total Refund Times** (reserved), **Total Payment Amount**, and **Total Refund Account** (reserved).

Long tap the initial page for 3 s and slide to the left/right by following the gesture. Select **Administrator**, and enter the password to login the menu page. Tap **Statistics** to enter the configuration page.

The device supports checking statistics within today, last 7 days, last 30 days, and custom.

If select **Custom**, you should set the **Start Time** and **End Time** of the records.

After settings the records duration, you can view **Total Payment Times**, **Total Refund Times**, **Total Payment Amount**, and **Total Refund Account**.

- Due to offline records, payment statistics will be subject to data from server (client or platform).
- The refund function is reserved.

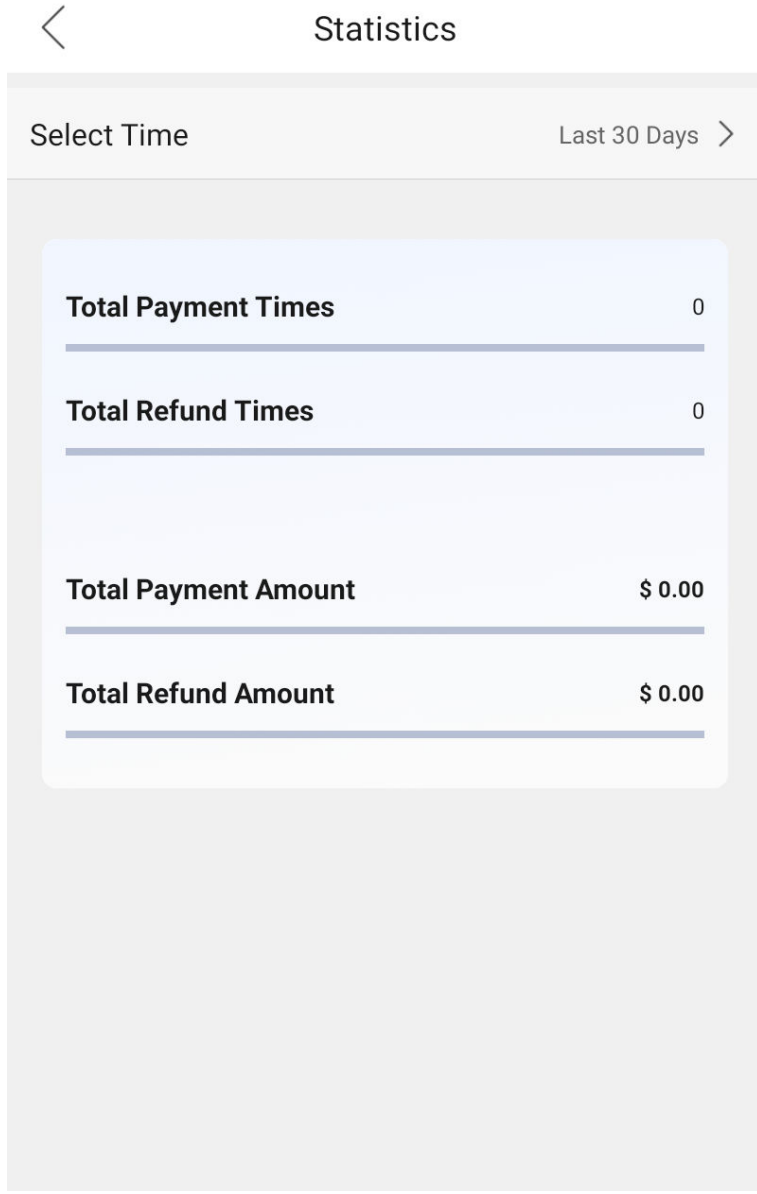


Figure 8-5 Payment Statistics

8.6 Communication Settings

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

You can set the wired network, the Wi-Fi parameter, the bluetooth parameters, and access to Guarding Vision on the communication settings page.

8.6.1 Set Wired Network Parameters

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

Steps

1. Long tap the initial page for 3 s and slide to the left/right by following the gesture. Select **Administrator**, and enter the password to enter the menu page.
2. Tap **Communication** on the menu page to enter the Communication page.

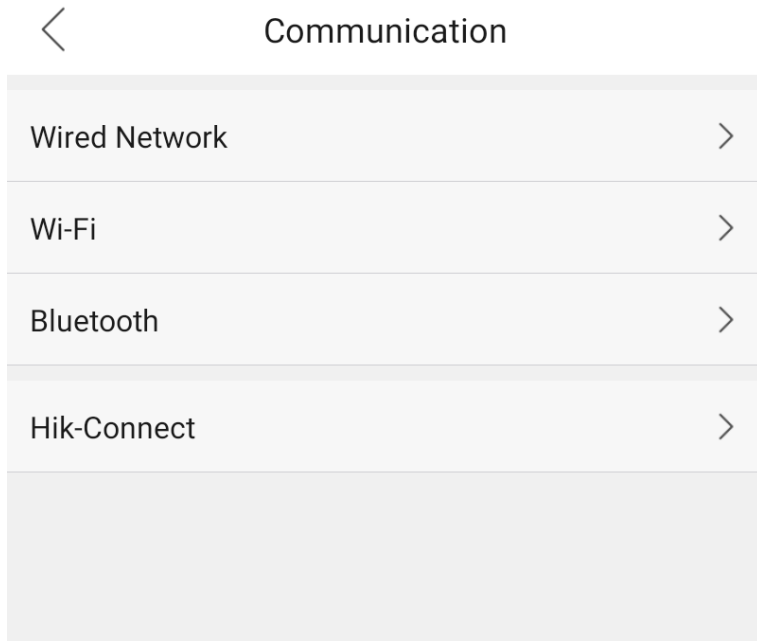


Figure 8-6 Communication Page

3. On the Communication page, tap **Wired Network**.

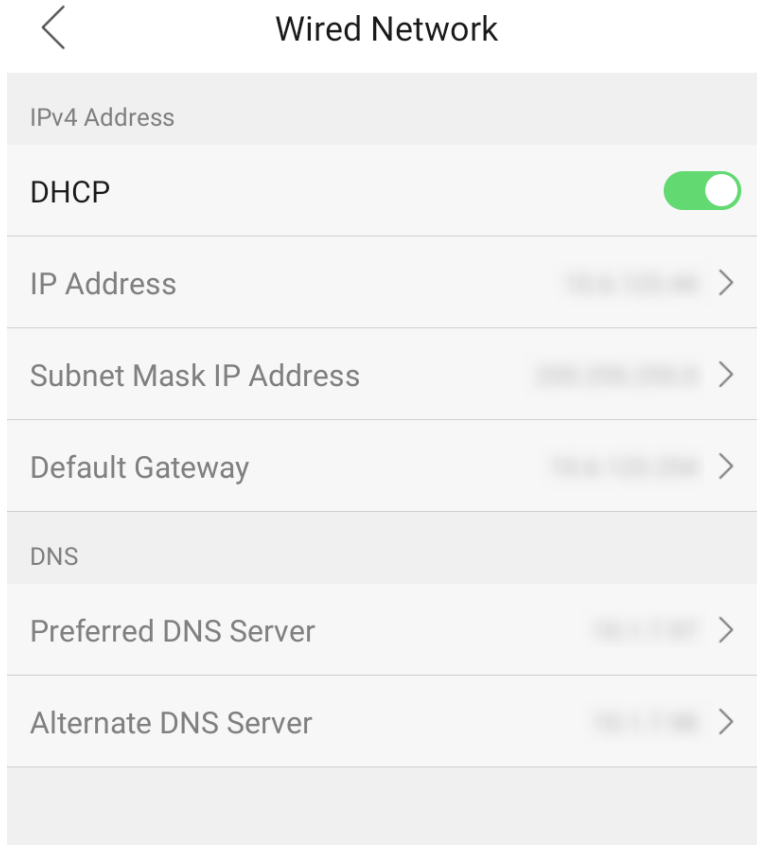


Figure 8-7 Wired Network Settings

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

   Note

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

8.6.2 Set Wi-Fi Parameters

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

Steps

Note

- The function should be supported by the device.
- If you want to use the Wi-Fi function, you should disconnect the wired network cable.

1. Long tap the initial page for 3 s and slide to the left/right by following the gesture. Select **Administrator**, and enter the password to enter the menu page.
2. Tap **Communication** on the menu page to enter the Communication page.

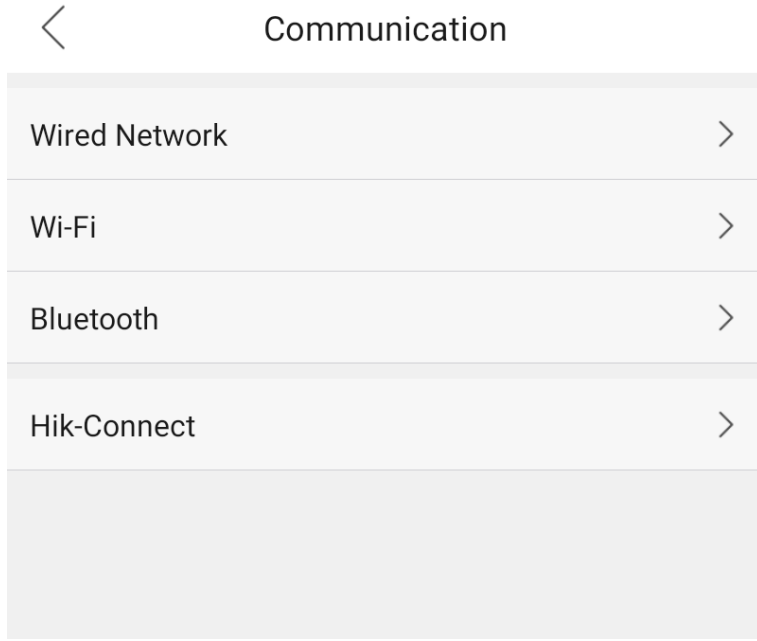


Figure 8-8 Communication Page

3. On the Communication page, tap **Wi-Fi**.

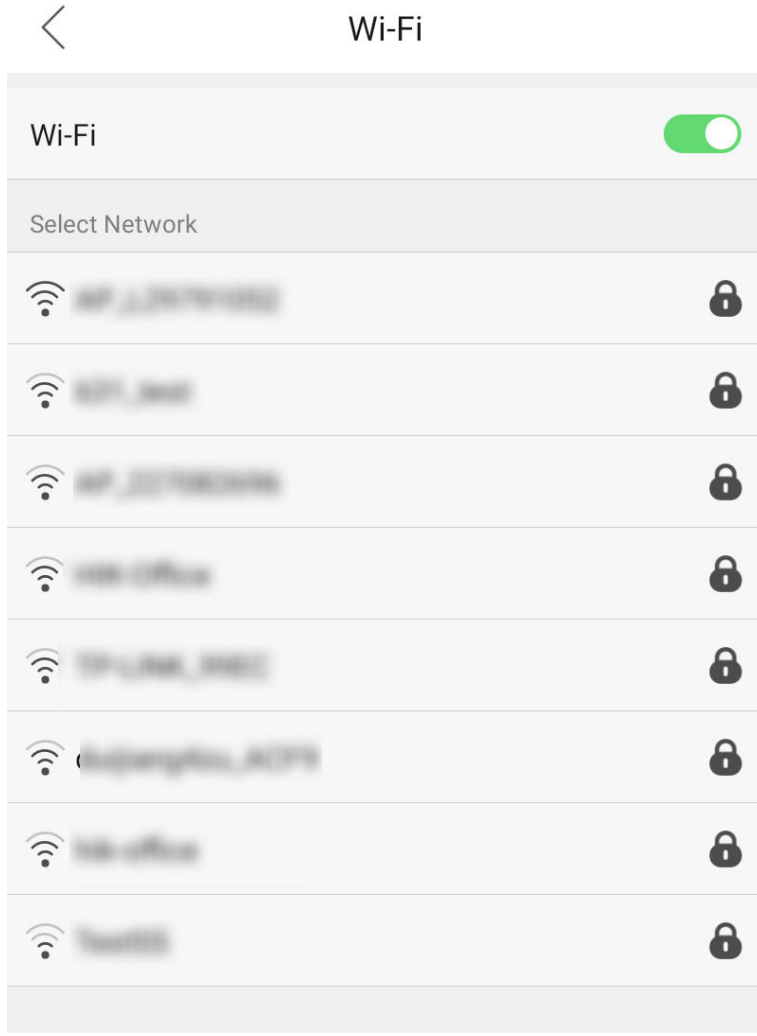


Figure 8-9 Wi-Fi Settings

4. Enable the Wi-Fi function.
5. Select a Wi-Fi from the list, and enter the Wi-Fi's password. Tap **OK**.

Note

Only 8 to 63 digits, letters, and special characters are allowed in the password.

6. **Optional:** Tap the connected Wi-Fi, and set the Wi-Fi's parameters. Tap ✓ to save the settings and go back to the Wi-Fi page.
   - By default, DHCP is enable. The system will allocate the IP address, the subnet mask, the gateway, and the DNS parameters automatically.
   - If disable DHCP, you should enter the IP address, the subnet mask, the gateway, and the DNS parameters manually.
   - Tap the connected Wi-Fi, and tap **Forgot This Network** and tap **OK** to disconnect with and forgot the Wi-Fi.

8.6.3 Set Bluetooth

If the environment is noisy, you can connect an external bluetooth loudspeaker to enhance the prompt volume.

Note

The external bluetooth loudspeaker should be purchased by yourself.

Long tap the initial page for 3 s and slide to the left/right by following the gesture. Select **Administrator**, and enter the password to enter the menu page. Tap **Communication** on the menu page to enter the Communication page.

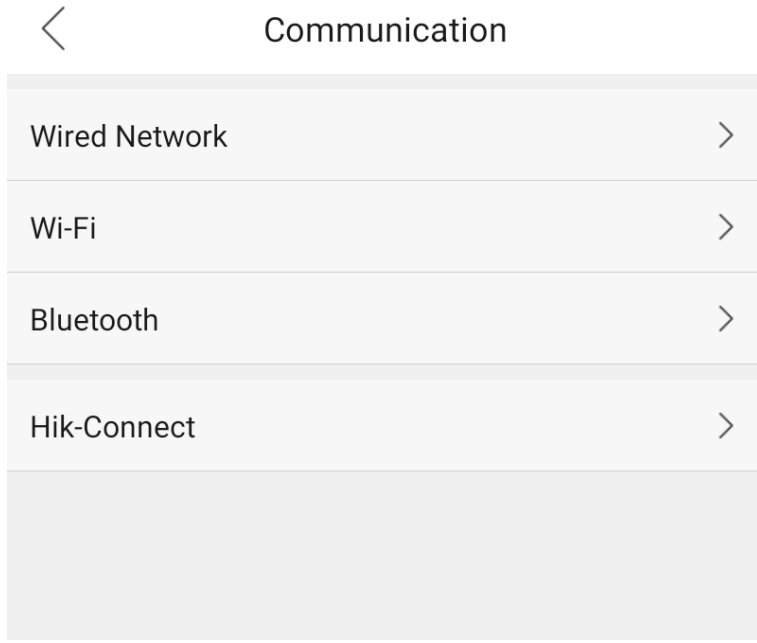


Figure 8-10 Communication Page

On the Communication page, tap **Bluetooth**.

Select a bluetooth from the list to pair.

After pairing completed. The Device's sound will be played via the bluetooth loudspeaker.

8.6.4 Platform Access

You can change the device verification code 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. Long tap the initial page for 3 s and slide to the left/right by following the gesture. Select **Administrator**, and enter the password to enter the menu page.
2. Tap **Communication** on the menu page to enter the Communication page.

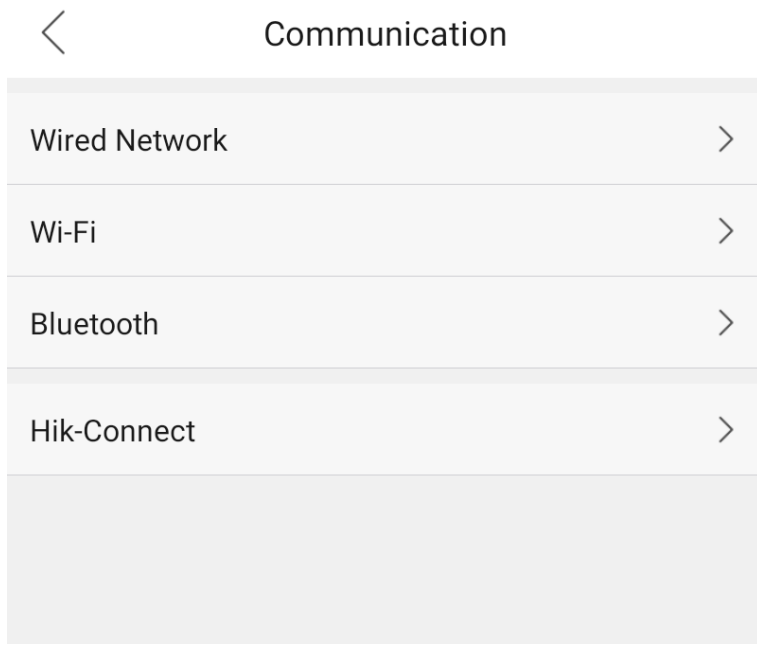


Figure 8-11 Communication Page

3. On the Communication page, tap **Hik-Connect**.
4. Enable **Hik-Connect**
5. Create the **Verification Code**, and you need to enter the verification code when you manage the devices via **Hik-Connect** mobile client.

8.7 Basic Settings

You can set the device sound, time, card, wake-up distance, language, IR light parameters.

Long tap the initial page for 3 s and slide to the left/right by following the gesture. Select **Administrator**, and enter the password to enter the menu page. Tap **Basic** on the menu page to enter the Basic page.

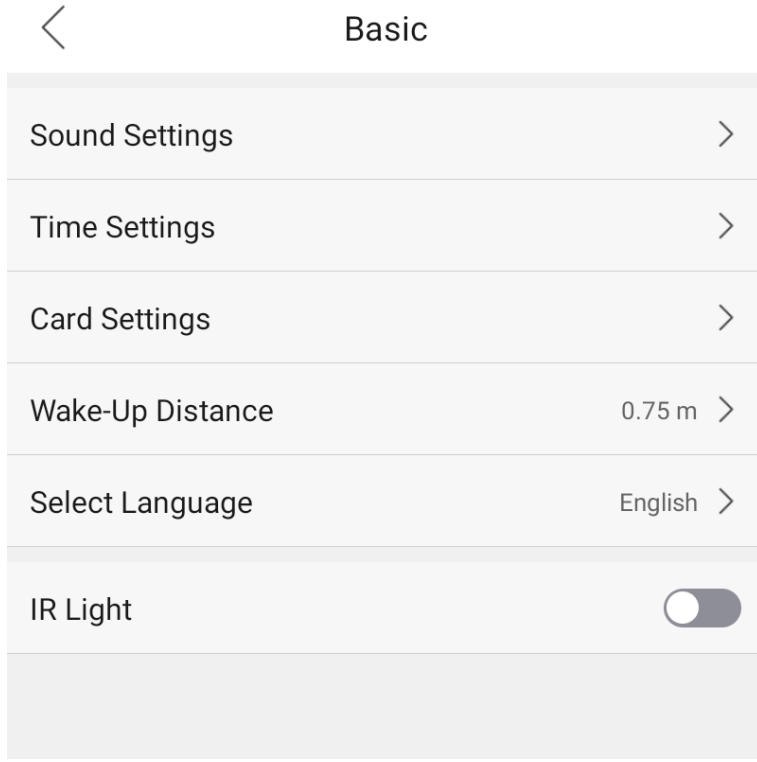


Figure 8-12 Basic Page

Sound Settings

You can enable/disable the voice prompt function. If enabling the function, you can set payment result voice prompt, custom prompt for successful/failed payment, and the voice volume.

Payment Result Voice Prompt

If enabling the function, a result voice prompt will be played when the payment is completed.

Custom Prompt for Successful/Failed Payment

Enter the successful or failed text and the text will be changed to voice prompt, which will be played when the payment is successful or failed.

Voice Volume

Drag the block to control the voice volume.

Note

You can set the voice volume between 0 and 10. 0 means silent.

Time Settings

Set the device time, date, date format, and time zone.

Card Settings

Enable/disable M1 card, NFC card, DESFire card, and FeliCa card. After enabling the cards, consumer can use those cards during the payment.

M1 Card Encryption Reading

M1 card encryption can improve the security level of authentication.

DESFire Card Content Reading

If enabling the item, the system will read the DESFire card content when authentication.

Wake-Up Distance

Select a distance, and the device initial page will be lightened up when a person within the configured distance.

Select Language

Change a language. The new language will be applied immediately after the new language settings is saved.

IR Light

Set the IR light brightness by dragging the block.

8.8 Set Biometric Parameters

You can customize the face parameters to improve the face recognition performance. The configurable parameters includes face liveness level, face recognition interval, authentication interval, wide dynamic range, face 1:N security level, and mask settings.

Long tap the initial page for 3 s and slide to the left/right by following the gesture. Select **Administrator**, and enter the password to enter the menu page. Tap **Biometrics** on the menu page to enter the Biometrics page.

Face Liveness Level

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

Face Recognition Interval

The time interval between two continuous face recognitions when authenticating.

Note

You can input the number from 1 to 10.

Authentication Interval

Set the device's authentication interval of the same person when authenticating.

Wide Dynamic Range

It is suggested to enable the WDR function if installing the device outdoors.

When there are both very bright and very dark areas simultaneously in the view, you can enable the WDR function to balance the brightness of the whole image and provide clear images with details.

Make Settings

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

Face with Mask 1:N Security Level

Drag the block to set the face with mask 1:N security level.

Strategy

None

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

Must Wear

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

8.9 Data Management

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

8.9.1 Delete Data

Delete consumer data.

Long tap the initial page for 3 s and slide to the left/right by following the gesture. Select **Administrator**, and enter the password to enter the menu page. Tap **Data** on the menu page to enter the Data page.

Tap **Data → Delete Data → Consumer Data** . All consumer's data added in the device will be deleted.

8.9.2 Export Data

Steps

1. Plug a USB flash drive in the device.
2. Long tap the initial page for 3 s and slide to the left/right by following the gesture. Select **Administrator**, and enter the password to enter the menu page. Tap **Data** on the menu page to enter the Data page.
3. Tap **Export Data**.
4. **Optional:** Create a password for exporting. When you import those data to another device, you should enter the password.

Note

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

8.9.3 Import Data

Steps

1. Plug a USB flash drive in the device.
2. Long tap the initial page for 3 s and slide to the left/right by following the gesture. Select **Administrator**, and enter the password to enter the menu page. Tap **Data** on the menu page to enter the Data page.
3. Tap **Import Data**.
4. Enter the password you created when exported the data. If you do not create a password when you exported the data, leave a blank in the input box and tap **OK**.

Note

- If you want to transfer all user information from one device (Device A) to another (Device B), you should export the information from Device A to the USB flash drive and then import from the USB flash drive to Device B. In this case, you should import the user data before importing the profile photo.
- The supported USB flash drive format is FAT32.
- The imported pictures should be saved in the folder (named enroll_pic) of the root directory and the picture's name should be follow the rule below:
  Card No._Name_Department_Employee ID_Gender.jpg
- If the folder enroll_pic cannot save all imported pictures, you can create another folders, named enroll_pic1, enroll_pic2, enroll_pic3, enroll_pic4, under the root directory.
- The employee ID should be less than 32 characters. It can be a combination of lower letters, upper letters, and numbers. It should not be duplicated, and should not start with 0.

8.10 System Maintenance

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

Long tap the initial page for 3 s and slide to the left/right by following the gesture. Select **Administrator**, and enter the password to enter the menu page. Tap **Maintenance** on the menu page to enter the Maintenance page.

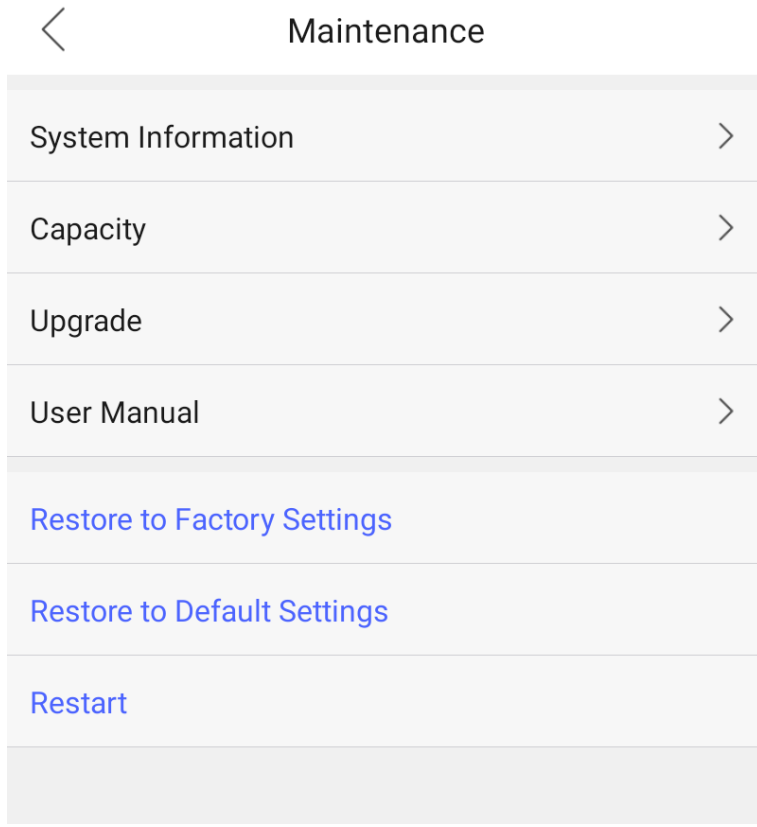


Figure 8-13 Maintenance Page

System Information

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

Hold the **?** on the upper-right corner of the page and enter the password to view the version of the device.

Note

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

Capacity

You can view the capacity of users, transactions, operators, face pictures, cards, and events.

Upgrade

You can view the current version and upgrade the device.

Online Update

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

Update via USB

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

User Manual

Scan the QR code to view the user manual.

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.

Restart

Restart the device.

Chapter 9 Quick Operation via Web Browser

9.1 Language Settings

You can select a language for the device system.

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

By default, the system language is English.

Click **Next** to complete the settings.

9.2 Time Settings

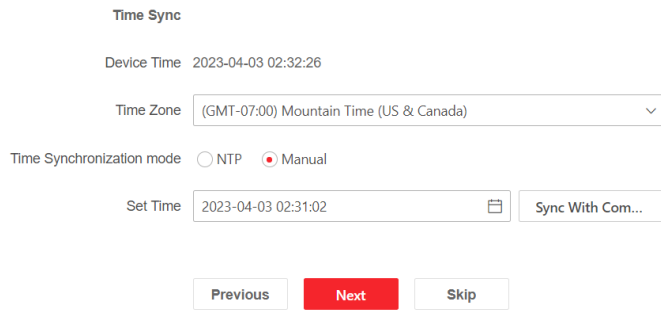


Figure 9-1 Set Time and DST

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

Time Zone

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

Time Sync.

NTP

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

Manual

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

Server Address/NTP Port/Interval

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

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

9.3 Privacy Settings

Set the picture uploading and storage parameters.

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

Picture Uploading and Storage

Save Picture When Auth.

Save picture when authenticating automatically.

Upload Picture When Auth.

Upload the pictures when authenticating to the platform automatically.

Save Registered Picture

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

Click **Complete** to save the settings and go to the next parameters. Or click **Skip** to skip privacy settings.

Chapter 10 Operation via Web Browser

10.1 Login

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

Note

Make sure the device is activated. For detailed information about activation, see ***Activate via Web Browser*** .

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

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

10.2 Overview

You can view the transaction statistics, set payment mode, view network status, basic information, and device capacity.

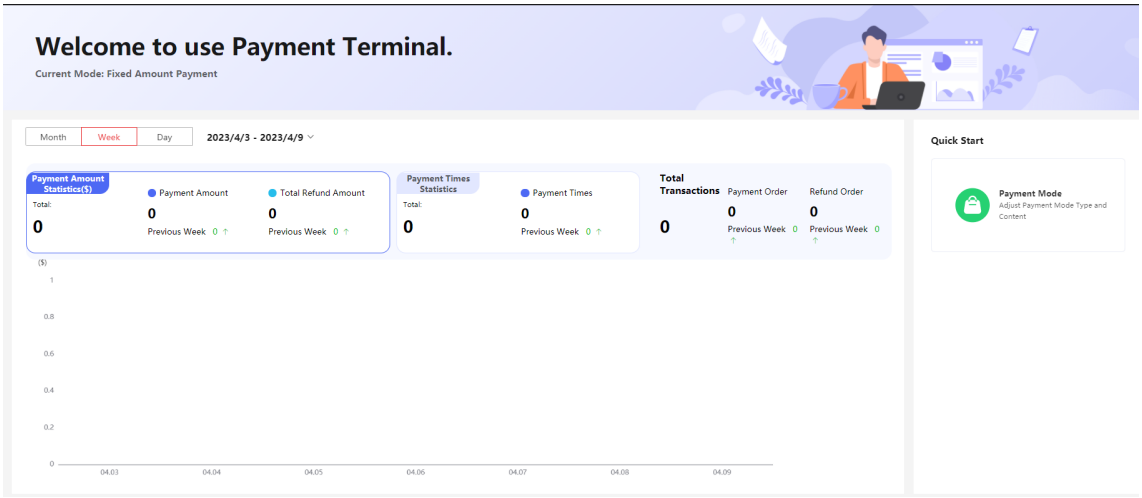


Figure 10-1 Overview Page

Function Descriptions:

Statistics

Click **Month**, **Week**, or **Daytime** to view the statistics.

Click **Payment Amount Statistics**, **Payment Times Statistics** to view different chats.

Quick Start

Click **Payment Mode** to quick enter the payment mode settings page to configure. For details, see ***Set Payment*** .

Network Status

View the device network connection type and status.

Basic Information

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

Device Capacity

You can view the person (operator), face, card, consumer, and event capacity.

View More

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

10.3 Check Transaction

You can search and view transaction records of different operators, including transaction type, payment mode, transaction amount, balance after payment, payment/remaining attempts, transaction center, etc.

Click **Check Transaction** to enter the interface.

Enter **Employee ID** and **Card No.**, check filter type, select the currency type, set **Start Time**, and **End Time** according to actual needs, and click **Search**. All transaction records will be listed, including transaction type, payment mode, transaction amount, balance after payment, payment/remaining attempts, transaction center, etc.

Note

Due to the existence of offline transaction records, payment statistics are subject to the server (client or web) data.

10.4 Search Event

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

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

The results will be displayed on the right panel.

10.5 Configuration

10.5.1 View Device Information

View the device name, language, model, serial No., version, number of camera, and device capacity.

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

You can view and edit the device name and the device language.

You can also view the device model, serial No., version, number of camera, and device capacity.

10.5.2 Set Time

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

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

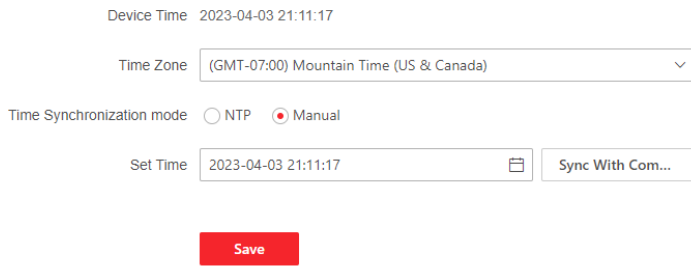


Figure 10-2 Time Settings

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

Device Time

View the current device time.

Time Zone

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

Time Synchronization Mode

NTP

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

Manual

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

Server Address Type/Server Address/NTP Port/Interval

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

10.5.3 Change Administrator's Password

Steps

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

Caution

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

10.5.4 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.

10.5.5 View Device Arming/Disarming Information

View device arming type and arming IP address.

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

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

10.5.6 Network Settings

Set TCP/IP, Wi-Fi parameters, bluetooth, HTTP, HTTPS, RTSP, and platform access.

Set Basic Network Parameters

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

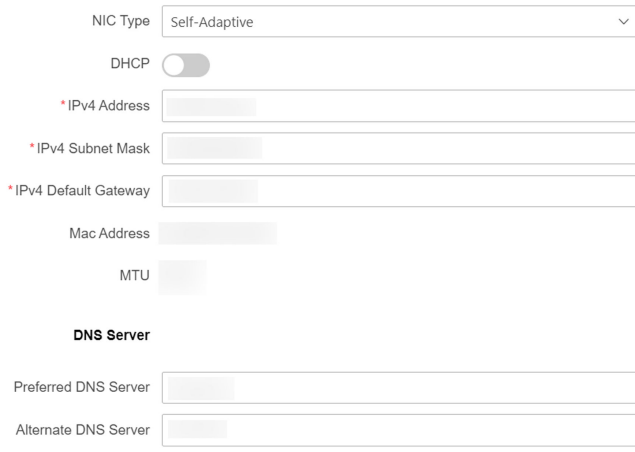


Figure 10-3 TCP/IP Settings Page

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

NIC Type

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

DHCP

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

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

DNS Server

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

Set Wi-Fi Parameters

Set the Wi-Fi parameters for device wireless connection.

Steps

Note

The function should be supported by the device.

1. Click **Configuration → Network → Network Settings → Wi-Fi** .

Figure 10-4 Wi-Fi Settings Page

2. Check **Wi-Fi**.
3. Select a Wi-Fi
   - Click of a Wi-Fi in the list and enter the Wi-Fi password.
   - Click **Manual Add** and enter a Wi-Fi's name (SSID), security mode, password (WPA). Click **OK**.
4. **Optional:** Set the WLAN parameters.
   1) Set the IP address, subnet mask, and default gateway. Or enable **DHCP** and the system will allocate the IP address, subnet mask, default gateway, and DNS server automatically.
5. Click **Save**.

Bluetooth Settings

You can enable bluetooth function.

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

Open

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

Device Name

You can edit the device name connected to the bluetooth.

Connection Status

You can view the connection status.

Set Port Parameters

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

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

HTTP

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

HTTPS

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

HTTP Listening

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

You can also click **Default** to reset the HTTP parameters.

Note

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

RTSP

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

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

Platform Access

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

Steps

1. Click **Configuration → Network → Device Access → Hik-Connect** to enter the settings page.

Note

Hik-Connect is an application for mobile devices. With the App, you can view live image of the device, receive alarm notification and so on.

2. Check **Enable** to enable the function.
3. **Optional:** Check the checkbox of **Custom**, and you can set the server address by yourself.
4. Enter the server IP address, and create a verification code.

Note

- 6 to 12 letters (a to z, A to Z) or numbers (0 to 9), case sensitive. You are recommended to use a combination of no less than 8 letters or numbers.
- The verification code cannot be ***123456*** or ***abcdef*** (case non-sensitive0).

5. Click **Save** to enable the settings.
6. Click **View** to view the device QR code. Use the Hik-Connect mobile client's adding function and scan the QR code to add. Use the App to operate the device.

10.5.7 Set Video and Audio Parameters

Set the image quality and resolution.

Set Video Parameters

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

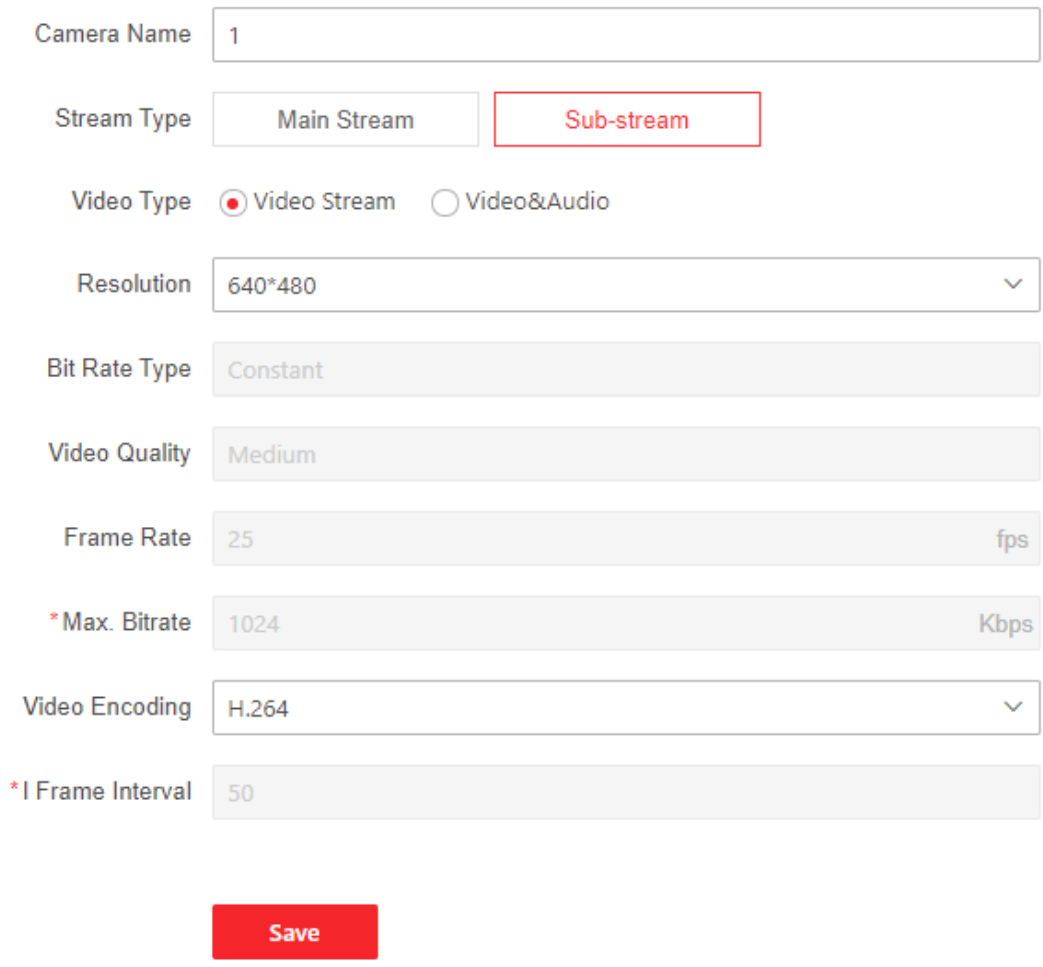


Figure 10-5 Video Settings Page

Set camera name, the stream type, the video type, the resolution, the video encoding.
Click **Save** to save the settings after the configuration.

Note

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

Audio

Click **Configuration → Video/Audio → Audio** .
Set the audio stream type, input volume, and output volume.

10.5.8 Set Image Parameters

You can adjust the image parameters, LED light, backlight and video adjustment.

Steps

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

   Image Adjustment

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

   LED Light

   Set the supplement light type, mode, LED light brightness.

   Backlight

   Enable or disable the WDR function.

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

   Video Adjust(Video Standard)

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

   PAL

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

   NTSC

   30 frames per second. Suitable for the USA, Canada, Japan, Taiwan (China), Korea, the Philippines, etc.
3. **Optional:** Click **Restore Default Settings** to restore the parameters to the default settings.

10.5.9 Set Payment

Set payment parameters, including payment auth. method, balance, payment mode, fixed amount settings, allowed time period of viewing payment data.

Steps

1. Click **Configuration → Payment Settings** .
2. Set the parameters.

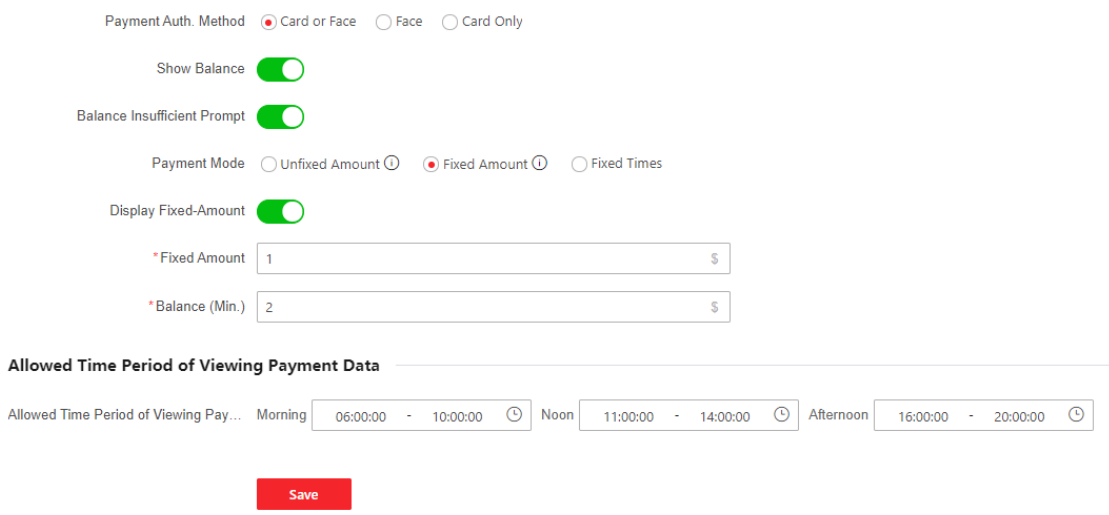


Figure 10-6 Payment Parameters

Payment Auth. Method

Card or Face

Supports authentication via face or card.

Face

Only supports authentication via face.

Card Only

Only supports authentication via card.

Show Balance

The balance will be displayed on the payment page.

Insufficient Balance Prompt

If you enable the function, the system will pop up a prompt if the consumer's balance is not enough. You should set the balance threshold to complete the settings.

Payment Mode

Unfixed Amount

You can set **Payment Mode** as **Unfixed Amount** if the payment amount varies. Set **Upper Limit of Single Payment** of the amount.

Max. Amount

By default, the Max. amount is 999,999.99

Custom Amount

You can set a Max. amount of upper limit.

Fixed Amount

If every payment requires the same amount of money, you can set **Payment Mode** as **Fixed Amount**. **Fixed Amount** should be set for each payment between 0.00~9999.99. 0 means no limits.

Enable **Show Fixed Amount**, the amount will be displayed during the payment.

Fixed Times

Pay once when use fixed times payment mode.

When the time reaches the upper limit, the system will issue prompt.

Balance (Min.)

When the balance of the consumer is less than the configured amount, the balance insufficient prompt will be displayed on payment page.

Allowed Time Period of Viewing Payment Data

Set time periods that the operators can view the payment data. For other time durations, operators cannot check the payment data.

3. Click **Save**.

10.5.10 Set Authentication Parameters

Click **Configuration → Payment Settings → 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.

Continuous Face Recognition Interval

The time interval between two continuous face recognitions when authenticating.

Note

You can input the number from 1 to 10.

Authentication Interval

Set the device's authentication interval of the same person when authenticating.

10.5.11 Set Card Security

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

Set the parameters and click **Save**.

Enable NFC Card

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

Enable M1 Card

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

M1 Card Encryption

Sector

M1 card encryption can improve the security level of authentication.

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

Enable DESFire Card

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

DESFire Card Read Content

The device can read the DESFire card content.

Enable FeliCa Card

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

10.5.12 Set Privacy Parameters

Set the authentication result, picture upload and storage parameters, and the picture clearing parameters.

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

Authentication Result Settings

Display Authentication Result

You can check **Face Picture**, **Name**, and **Employee ID**. The checked item will be displayed in the authentication result.

Picture Uploading and Storage

Save Picture When Auth.

Save picture when authenticating automatically.

Upload Picture When Auth.

Upload the pictures when authenticating to the platform automatically.

Save Registered Picture

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

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.

10.5.13 Set Biometric Parameters

Set Basic Parameters

Click **Configuration → Smart → Smart** .

Note

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

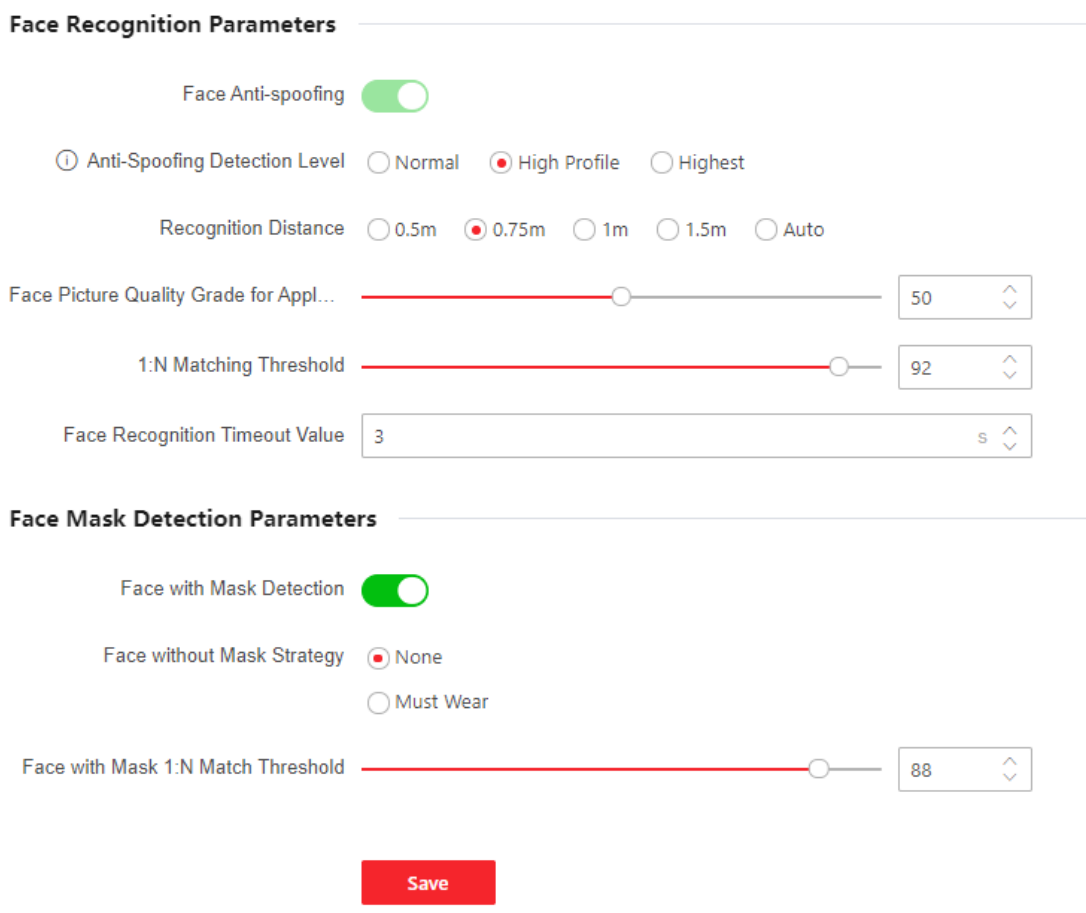


Figure 10-7 Smart Settings Page

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

Face Anti-spoofing

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

Note

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

Anti-spoofing Detection Level

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

Recognition Distance

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

Face Picture Quality Grade for Applying

Set the face pictrue's grade.

1:N Matching Threshold

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

Face Recognition Timeout Value

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

Face without Mask Detection

After enabling the face without mask detection, the system will recognize the captured face with mask picture or not. You can set face with mask1:N matching threshold and the strategy.

None

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

Must Wear

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

Face with Mask 1:N Matching Threshold

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

Set Recognition Area

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

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

Or drag the block of each parameter to set the area.
Click **Save**.
Click or , or to capture pictures, record videos, and view full screen live video.

10.5.14 Set Screen Sleep Time

You can set the screen saver and the sleep time for the device.

Click **Configuration → Preference → Screen Display** .

Sleep

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

Click **Save**.

10.5.15 Set Theme

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

Set Theme

Click **Configuration → Preference → Notice Publication** .
Click **Media Library Management**, and click **+** to add media.
Back to the Notice Publication page, and click **+Add Program** and create a name for the program.
Click **Save**.
Click **+** in Picture area, you can add the picture from the media library that will display on the device screen saver.
Set the slide show interval and the schedule.
Click **Save**.

10.5.16 Set Payment Prompt

You can enable payment amount prompt and payment result prompt, and customize prompt for successful payment and failed payment.

Steps

1. Click **Configuration → Preference → Payment Prompt** .
2. Enable **Enable Voice Prompt** and **Payment Result Prompt** according to your actual needs.
3. Enter text in the textboxes to customize prompt for successful payment and failed payment.
4. Click **Save**.

10.5.17 Customize Audio Content

Customize the output audio content when authentication succeeded and failed.

Steps

1. Click **Configuration → Preference → Prompt Schedule** .

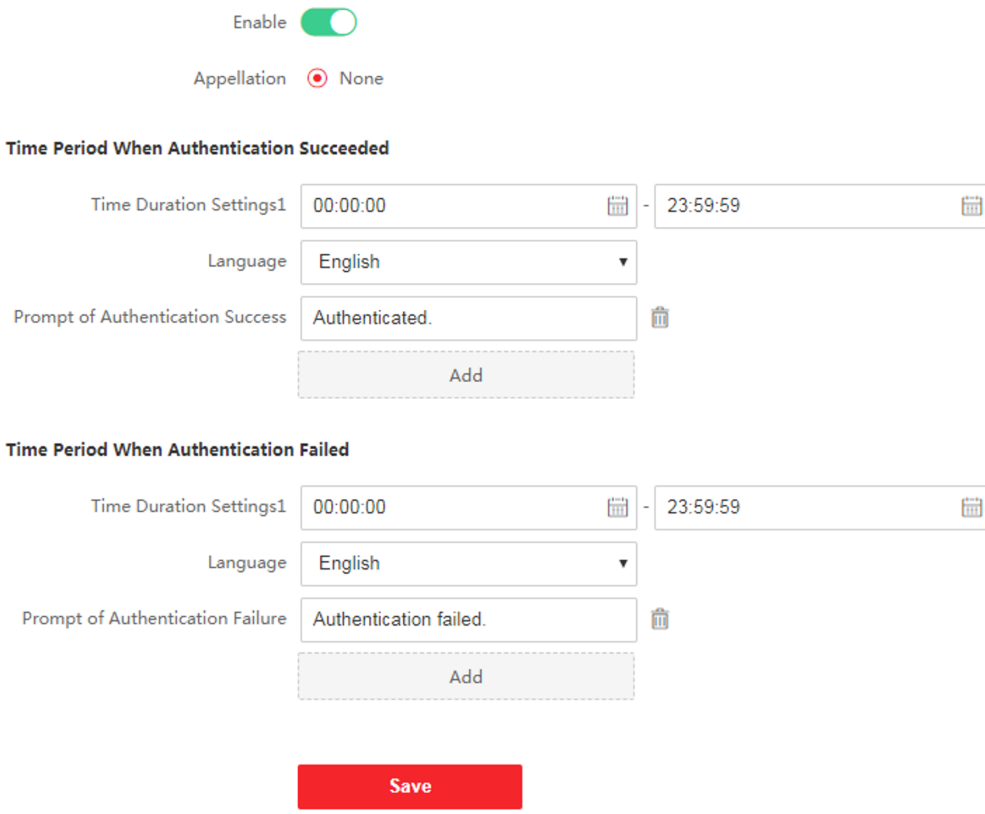


Figure 10-8 Customize Audio Content

2. Enable the function.
3. Set the time period when authentication succeeded.
   1) Click **Add Time Duration**.
   2) Set the time duration and the language.

   Note

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

2) Set the time duration and the language.

Note

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

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

5. Click **Save**.

10.5.18 Upgrade and Maintenance

Reboot device, restore device parameters, and upgrade device.

Reboot Device

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

Upgrade

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

Local Upgrade

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

Online Upgrade

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

Note

Do not power off during the upgrading.

Restore

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

Restore to Default Settings

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

Restore to Factory Settings

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

Import and Export Parameters

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

Export

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

Note

You can import the exported device parameters to another device.

Import Config File

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

10.5.19 Device Debugging

You can set device debugging parameters.

Steps

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

   Enable SSH

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

   ADB

   Enable **ADB Remote Control** for actual needs.

   Print Log

   You can click **Export** to export log.
3. Click **Save**.

10.5.20 Log Query

You can search and view the device logs.

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

Set the major and minor type of the log type. Set the start time and end time for searching, and click **Search**.

The results will be displayed below, which including the No., time, the major type the minor type, the channel No., the local/remote user information, the remote host IP, etc.

10.5.21 Certificate Management

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

Note

The function is only supported by certain device models.

Create and Import HTTPS Certificate

Steps

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

Create and Import SYSLOG Certificate

Steps

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

Import CA Certificate

Before You Start

Prepare a CA certificate in advance.

Steps

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

Note

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

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

10.5.22 View Open Source Software Statement and Help

View Open Source Software Statement

On the web browser page, click → **Open Source Software Statement** to view the open source software statement.

View Help

On the web browser page, click → **Online Document** to view the open source software statement.

Chapter 11 Operation via HikCentral Professional

You can use the HikCentral Professional to add merchant and do other operations.

11.1 Login

You can access and configure the platform via web browser directly, without installing any client software on the your computer.

Note

The login session of the Web Client will expire and a prompt with countdown will appear after the configured time period in which there is no action. For setting the time period, refer to *System Security Settings*.

11.1.1 First Time Login

If this is the first time for you to login, you can choose to login as admin or normal user according to your user role.

Login for First Time for admin User

By default, the platform predefined the administrator user named admin. When you login via the Web Client for the first time, you are required to create a password for the admin user before you can properly configure and operate the system.

Steps

1. In the address bar of the web browser, enter the address of the PC running SYS service and press **Enter** key.

   Example

   If the IP address of PC running SYS is 172.6.21.96, and you should enter http://172.6.21.96 or https://172.6.21.96 in the address bar.
2. Enter the password and confirm password for the admin user in the pop-up Create Password window.

   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.

3. Click **OK**.

   The Home page of Web Client will be displayed after you successfully creating the admin password.

First Time Login for Normal User

When you log in to the system as normal user via Web Client for the first time, you should change the initial password and set a new password for login.

Steps

1. In the address bar of the web browser, input the address of the PC running SYS service and press the **Enter** key.

   Example

   If the IP address of PC running SYS is 172.6.21.96, and you should enter http://172.6.21.96 or https://172.6.21.96 in the address bar.

   Note

   You should configure the SYS's IP address in WAN Access of System Configuration before accessing the SYS via WAN. For details, refer to *Set WAN Access*.

2. Enter the user name and password.

   Note

   Contact the administrator for the user name and initial password.

3. Click **Log In** and the **Change Password** window opens.
4. Set a new password and confirm the password.

   Note

   The password strength can be checked by the system and should meet the system requirements. If password strength is lower than the required minimum strength, you will be asked to change your password. For setting minimum password strength, refer to .

   Caution

   The password strength of the device can be checked by the system. 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 reset your password regularly, especially in the high security system, resetting 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. Click **OK** to change the password.

Result

Web Client home page displays after you successfully logging in.

11.1.2 Login via Web Client (Administrator)

You can access the system via web browser and configure the system.

Steps

1. In the address bar of the web browser, input the address of the PC running SYS service and press **Enter** key.

   Example

   If the IP address of PC running SYS is 172.6.21.96, and you should enter http://172.6.21.96 or https://172.6.21.96 in the address bar.

   Note

   You should configure the SYS's IP address in WAN Access of System Configuration before accessing the SYS via WAN. For details, refer to .

2. Select the **Management** tab.
3. Enter the user name and password.
4. Click **Log In** to log in to the system.

   Note

   - If failed password attempt of current user is detected, you are required to input the verification code. The failed password attempts from current client, other client, and other address will all require the verification code.
   - The failed password attempt and verification code attempt from current client, other client (e.g., Control Client), and other address will all be accumulated. Your IP address will be locked for a specified period of time after specific number of failed password or verification code attempts detected. For setting failed login attempts and locking duration, refer to *System Security Settings*.
   - The account will be frozen for 30 minutes after 5 failed password attempts. The failed password attempts from current client, other clients (e.g., Control Client), and other addresses will all be accumulated.
   - The password strength can be checked by the system and should meet the system requirements. If password strength is lower than the required minimum strength, you will be

asked to change your password. For setting minimum password strength, refer to *System Security Settings*.

- If your password is expired, you will be asked to change your password when login. For setting maximum password age, refer to *System Security Settings*.

Result

Web Client home page displays after you successfully logging in to the system.

11.1.3 Login via Web Client (Employee)

Employees can access the system via web browser.

Before You Start

The administrator should enable self-service login (enabled by default) and set the login password (employee ID by default) for employees.

Steps

1. In the address bar of the web browser, input the address of the PC running SYS service and press the **Enter** key.

   Example

   If the IP address of the PC running SYS is 172.6.21.96, and you should enter http://172.6.21.96 or https://172.6.21.96 in the address bar.

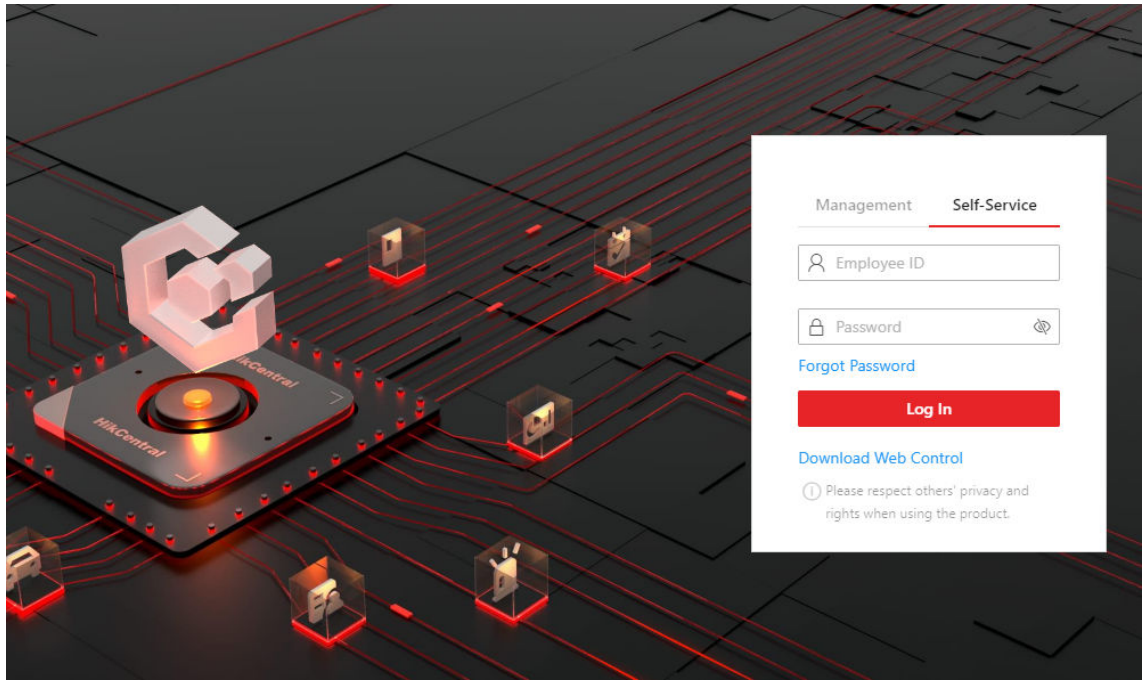


Figure 11-1 Login Page

2. Select the **Self-Service** tab.

3. Enter the employee ID and password.
4. Click **Log In** to log in to the system.

Note

- Employees are required to change the password upon the first login.
- If employees forget the password, they can reset new password in **Forgot Password**.
- If the password is expired, employees will be asked to change the password upon login. For setting the maximum password age, refer to *System Security Settings*.

Result

Web Client home page displays after employees successfully log in to the system.

11.1.4 Change Password for Reset User

When the normal user's password is reset by admin user, he/she should change the initial password and set a new password when logging into HikCentral Professional via the Web Client.

Steps

1. In the address bar of the web browser, enter the address of the PC running SYS service and press **Enter** key.

   Example

   If the IP address of PC running SYS is 172.6.21.96, and you should enter http://172.6.21.96 or https://172.6.21.96 in the address bar.

   Note

   You should configure the SYS's IP address in WAN Access of System Configuration before accessing the SYS via WAN. For details, refer to *Set WAN Access*.
2. Enter the user name and initial password set by the administrator.
3. Click **Log In** and a **Change Password** window opens.
4. Set a new password and confirm the password.

   Note

   The password strength can be checked by the system and should meet the system requirements. If password strength is lower than the required minimum strength, you will be asked to change your password. For setting minimum password strength, refer to *System Security Settings*.

   Caution

   The password strength of the device can be checked by the system. 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 reset your password regularly, especially in the high security system, resetting 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. Click **OK**.

Result

Web Client home page displays after you successfully changing the password.

11.1.5 Forgot Password

If you forgot the your account's password, you can reset the password and set a new password.

Before You Start

- Make sure the normal user has been configured with an available email address.
- Make sure the email server is tested successfully.

Steps

1. On the login page, enter a user name in the User Name field.
2. Click **Forgot Password**.

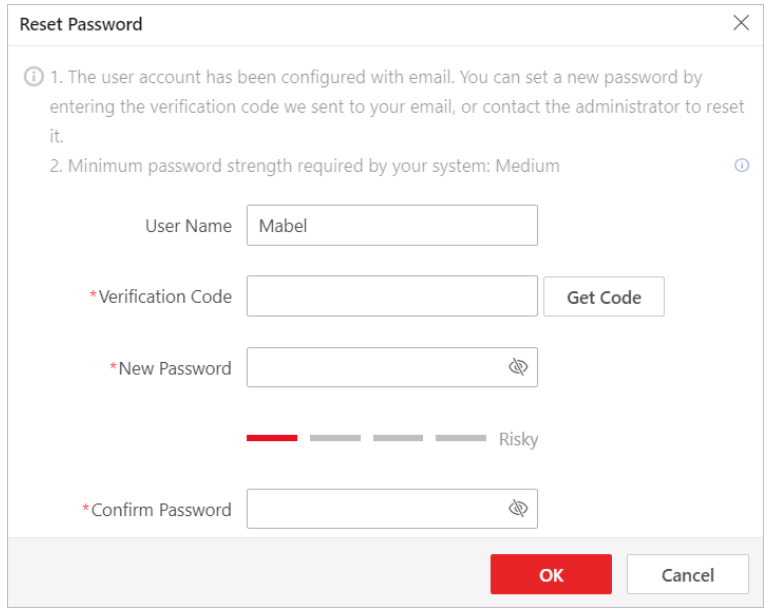


Figure 11-2 Reset Password for Normal User

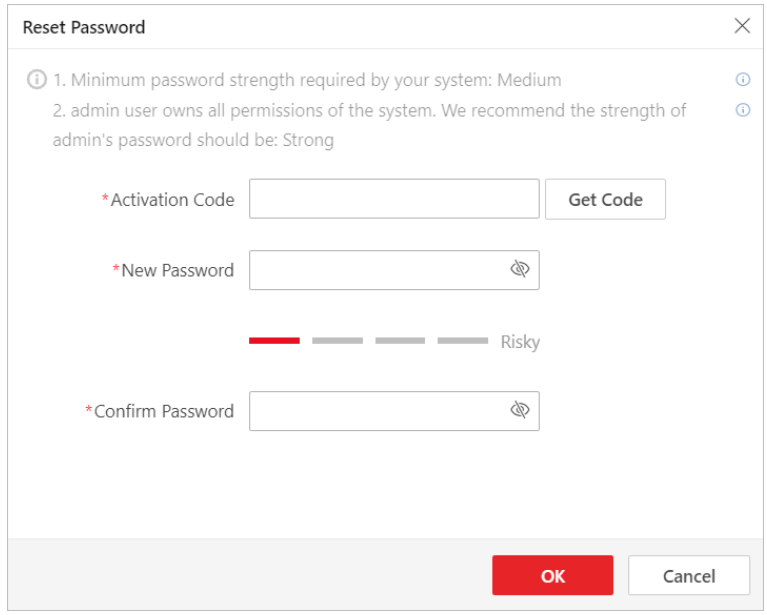


Figure 11-3 Reset Password for admin User

3. Enter the required information on the Reset Password pane.
   - For the admin user, enter the License activation code, new password, and confirm password.

     Note

     If you forget the License activation code, you can click **Get Code** to send the activation code to the email address configured when activating the License in online mode. For setting an email for the admin user, refer to ***Activate License - Online*** .
   - For normal users, click **Get Code** to send the verification code to the email address configured when adding the user. And then enter the received verification code, new password, and confirm password within 10 minutes.

     Note

     If the email address is not set for the normal user, contact the admin user to reset the password and change the password when login.
   - For domain user, contact the admin user to reset the password.

Note

The password strength can be checked by the system and should meet the system requirements. If password strength is lower than the required minimum strength, you will be asked to change your password. For setting minimum password strength, refer to *System Security Settings*.

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.

4. Click **OK**.

11.2 Download Mobile Client

On the login page of Web Client, you can scan the QR code to download the Mobile Client that is used for accessing the system via mobile terminal (e.g., mobile phone).

Perform this task when you need to download the Mobile Client.

Note

You can also search and download the Mobile Client in the App Store.

Steps

1. In the address bar of the web browser, enter the address of the PC running SYS service and press **Enter** key.

   Example

   If the IP address of PC running SYS is 172.6.21.96, and you should enter http://172.6.21.96 in the address bar.

   Note

   You should configure the SYS's IP address in WAN Access of System Configuration before accessing the SYS via WAN. For details, refer to *Set WAN Access*.

2. Scan the corresponding QR code with your mobile terminal to download the Mobile Client.

11.3 Web Control

For accessing the Web Client via web browser, you must install a web control on the PC on which you access the Web Client when performing some functions. Web Client automatically asks you to install the web control when you want to access the corresponding functions, and you can follow the prompts to install it on the PC, or download it on the login page.

11.4 Home Page Overview

The default Home page of the Web Client provides a visual overview of function modules on the platform. You can access specific modules quickly and conveniently via the Home page.

Note

After you entered the modules, tabs will appear on the top of the Web Client, you can click tabs to quickly switch modules. You can also click in the tab area to refreshthe module.

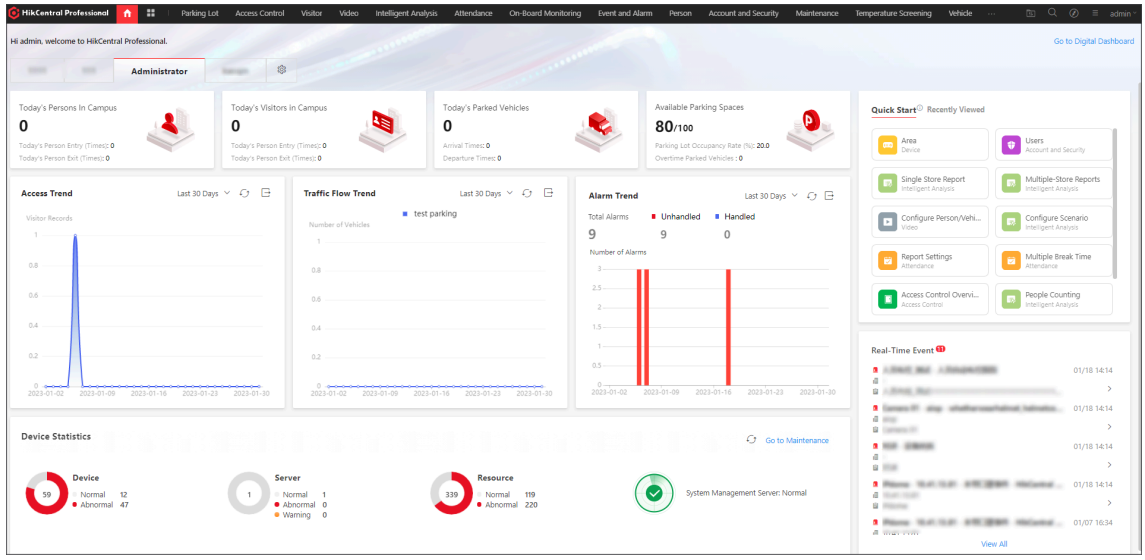


Figure 11-4 Home Page Overview

Table 11-1 Home Page Description

Section	Module	Description
Top Navigation Bar	Navigation Icon	The navigation bar shows the available functions determined by the Licenses you purchased. You can add some frequently used or important modules to the navigation bar for convenient access. See details in *Customize Navigation Bar*.
	Download Center	You can view and manage all of the downloading and downloaded tasks on the Web Client.
	Search Module	You can search for a specific function module and view the recently viewed pages.
	Real-Time Event	View the list of real-time events. Also, you can click an event, go to the Alarm Details page to view details and acknowledge the alarm.
	Wizard	**Video** A wizard which guides you through the management and applications of video. You can also view the flow

Section	Module	Description
		chart which introduces the video resource management, recording configurations, and video application in *Video Management*. **Access Control** A wizard which guides you through the basic configurations of access control. You can also view the flow chart which introduces the configurations and operations of access control and elevator control in *Flow Chart of Door Access Control*. **Visitor** A wizard which guides you through the basic configurations and applications of visitor management. You can also view the flow chart which introduces the process of visitor management from reserving visitors to checking out visitors and viewing visitor information/records (see *Flow Chart of Visitor Management*. **On-Board Monitoring** A wizard which guides you through the configuration and applications of on-board monitoring. You can also view the flow chart which introduces the management of on-board devices and vehicles, the configuration of GIS map and driving rules, driving monitoring, vehicle route and driving event search, and the report management in *On-Board Monitoring and Search*. **Vehicle and Parking** A wizard which guides you through the management and applications of vehicle and parking. You can also view the flow chart which introduces the management of parking lots, vehicles, and entry & exit rules, parking fee rules, parking guidance, and vehicle & record search in *Flow Chart of Parking Management*. **Alarm Detection** A wizard which guides you through the management and configurations of alarm detection. You can also view the flow chart which introduces the management

Section	Module	Description
		of security control panels and alarm inputs, arming schedule configuration, and event & alarm management in *Flow Chart of Alarm Detection*. **Digital Signage** A wizard which guides you through the management and configurations of digital signage. You can also view the flow chart which introduces the management of digital signage terminals, materials, programs, and schedules, program approval, and program release in *Flow Chart of Digital Signage*. **Attendance** A wizard which guides you through the management and configurations of attendance. You can also view the flow chart which introduces the management of devices, person groups, and persons, basic attendance configuration, attendance rule configuration, and record search and handling in *Flow Chart of Time and Attendance*. **Patrol** A wizard which guides you through the management and configurations of patrol. You can also view the flow chart which introduces the process of patrol management from adding patrol points to real-time patrol monitoring and records/statistics search (see *Flow Chart of Patrol Management*).
	Maintenance and Management	**License** You can view the License details, activate, upgrade, and deactivate the License if needed. For more details, refer to *License Management*. **Back Up and Restore System Data** You can manually back up the data in the system, or configure a schedule to run the backup task regularly. When an exception occurs, you can restore the database if you have backed up the database. For more details, refer to *Set System Data Backup* and *Restore System Data*.

Section	Module	Description
		Export Configuration Data You can export and save configuration data to your local PC. For more details, refer to *Export Configuration File*. **Download Installation Package** Download the installation package of other clients, such as Control Client. **About** Check the version information of the Web Client. View the License Agreement and Open-Source License Agreement.
	Account	**Change Password** Change the password of the current user. For more details, refer to *Change Password of Current User*. **Logout** Log out of the system and back to the login page.
Workbench / Digital Dashboard	Workbench	You can configure the available workbenches (including the preset workbench) and customize personal workbench by adding the frequently used components. For more details, refer to *Customize Preset Workbench* and *Customize Personal Workbench*. You can check the default and the added workbenches to display on the Home page for convenient use.
	Digital Dashboard	Click **Go to Digital Dashboard** to view statistical information about digital campus overview, security control and management, persons, and vehicles. For more details, refer to *View Digital Dashbaord*.

11.4.1 Customize Navigation Bar

To conveniently access some frequently used or important modules, you can customize the navigation bar.

Steps

1. On the top left, select to display the navigation bar.

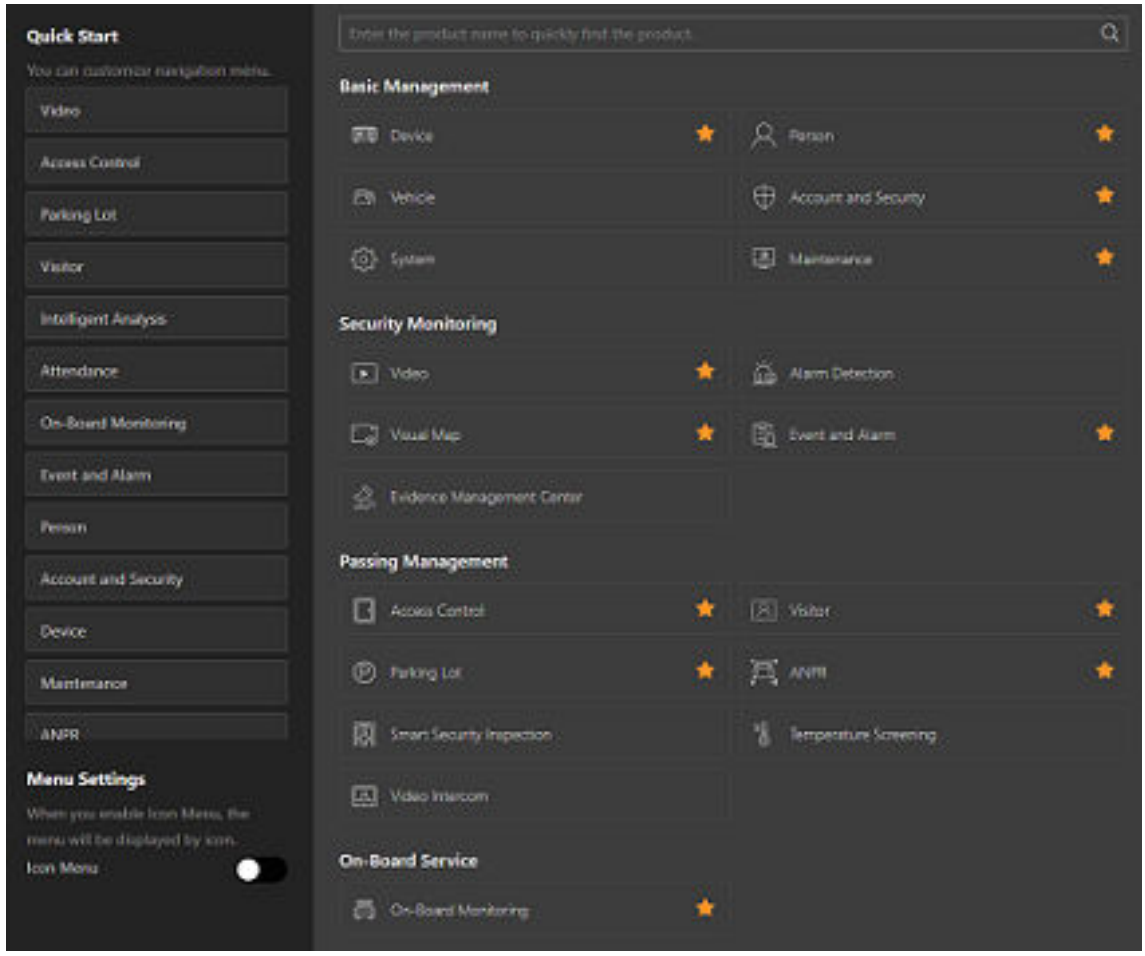


Figure 11-5 Navigation Bar

Note

On the All Modules panel, the icon beside the module name indicates that this module has been added to the left navigation bar.

2. **Optional:** Click to remove the module from the navigation bar.
3. **Optional:** In the Quick Start area, drag a module up or down to adjust the module order on the top navigation bar.
4. **Optional:** In Menu Settings area, switch on **Icon Menu**, the module name turns to be an icon displayed on the top navigation bar.

11.4.2 View Digital Dashboard

The platform provides visualized statistics about the digital campus information, including overview, persons, vehicles, and security control and management.

Click to enter the Home page. On the upper-right corner, click **Go to Digital Dashboard** to enter the Digital Campus page.

Note

- Click to select the time period (today, last 7 days, or last 30 days) to display the statistics.
- Click to refresh the real-time statistics.

Overview

- On the left, you can view today's person statistics, access trend, and vehicle parking trend of parking lots.
- On the right, you can view the alarm trend (including the number of total alarms, handled alarms, and unhandled alarms), and device statistics, and you can set cameras auto-switch.

Figure 11-6 Digital Campus Overview

Person

- On the left, you can view the total number of persons (including employees and visitors), today's person employee entry trend, and today's visitor entry trend.
- On the right, you can view the historical employee entry trend and historical visitor entry trend.

Vehicle

- On the left, you can view the vehicle statistics, internal and external vehicle passing trend, and vehicle parking trend of parking lots.
- On the right, you can view the parking space statistics, parking space occupancy trend, and parking duration distribution.

Security

- On the left, you can view the alarm trend (including the number of total alarms, handled alarms, and unhandled alarms), top 5 events, and top 5 areas with alarms.
- In the middle, you can select to view the live view of events.
- On the right, you can view the device statistics and device status.

11.4.3 Customize Preset Workbench

As an administrator, you can link users with the default preset workbench. Also, you can customize preset workbenches.

Note

Make sure you have logged in to the Client by the administrator account. For details, refer to ***Login via Web Client (Administrator)*** .

You can customize a preset workbench by going to one of the two following entries.

- Click to enter the Home page. Then click to expand the workbench configuration pane. In the personal workbench area, click **Preset Workbench Configuration**.
- On the top left, select → **Basic Management** → **System** . Select **Workbench Management** on the left.

Note

- You can filter the preset workbenches by conditions, such as workbench name, linked users, and unlinked users.
- You can hover the cursor on the preset workbench, click **Preview** to preview the preset workbench.

Configure Default Preset Workbench

Hover the cursor on the default preset workbench, including Administrator, Time and Attendance, Visitor Management. Click **Edit**, select users to link with the workbench, so the workbench will be displayed on the user's Home page.

Note

The default preset workbench name and remark cannot be edited.

Add Preset Workbench

1. Click **Add Workbench** in the upper-right corner.
2. Click to edit the workbench name. Also, you can select an existing workbench as the template from the Copy From drop-down list, link users with the workbench, and add remark.
3. Click **OK**
4. (Optional) Set the display size of the component.
5. Click **Save**. The added preset workbench will be displayed in the Preset Workbench pane on the Home page.

11.4.4 Customize Personal Workbench

You can customize personal workbench by adding the frequently used components for overview and quick access to modules, including person, time and attendance, security control and management, and vehicle.

Steps

1. Click to enter the Home page.
2. Click to expand the workbench configuration pane.
3. In the personal workbench area, click **Personal Workbench** to enter the Create Personal Workbench page.
4. Click to edit the workbench name.
5. **Optional:** Select an existing workbench as the template from the Copy From drop-down list.
6. Click **OK**.
7. Click + on the right side of the component.

   The component will be displayed on the right.
8. **Optional:** Drag in the lower right corner of a single component or set the display ratio (e.g., 100%, 60%, or 50%) to adjust the display size of the component.
9. Click **Save**.

   The added personal workbench will be displayed in the Personal Workbench pane on the Home page.

11.5 Getting Started

The following content describes the tasks typically involved in setting a working system.

Verify Initial Configuration of Devices and Other Servers

Before doing anything on the platform, make sure the devices (encoding devices, access control devices, recording server, and so on) you are going to use are correctly mounted and connected to the network as specified by the manufacturers. Such initial configurations are required in order to connect the devices to the platform via network.

Log In to Web Client

Refer to ***Login for First Time for admin User*** .

Activate License

Refer to ***Activate License - Online*** or ***Activate License - Offline*** .

Add Devices to Platform and Configure Area

The platform can quickly scan your network for relevant devices, and add them. Or you can add the devices by inputting the required information manually. The devices added should be organized into areas for convenient management. Refer to *Resource Management* and *Area Management*.

Configure Recording Settings

You can record the video files of the cameras on the storage device according to the configured recording schedule. The schedule can be set as continuous, alarm triggered, or command triggered as desired. Refer to *Configure Storage and Recording*.

Configure Event and Alarm

The camera exception, device exception, server exception, alarm input, and so on, can trigger linkage actions in the platform. Refer to *Event and Alarm*.

Configure Users

Specify who should be able to access the platform, and how. You can set different permissions for the users to limit their operations. Refer to *Role and User Management*.

View How-to Videos

On the lower left of the log-in page, click **Scan QR Code for Help**, and then scan the QR Code by your smart phone to view the how-to videos of the platform.

11.6 License Management

After installing HikCentral Professional, you have a temporary License for a specified number of devices and limited functions. To ensure the proper use of HikCentral Professional, you can activate the SYS to access more functions and manage more devices. If you do not want to activate the SYS now, you can skip this chapter and activate the system later.

Two types of License are available for HikCentral Professional:

- **Base:** You need to purchase at least one basic License to activate the HikCentral Professional.
- **Expansion:** If you want to increase the capability of your system, you can purchase an expanded License to get additional features.

Note

- Only the admin user can perform the activation, update, and deactivation operation.
- If you encounter any problems during activation, update, and deactivation, please send the server logs to our technical support engineers.

11.6.1 Activate License - Online

If the SYS server to be activated can properly connect to the Internet, you can activate the SYS server in online mode.

Steps

1. Log in to HikCentral Professional via the Web Client. Refer to ***Login via Web Client (Administrator)*** .
2. On the Home page, click **Activate** to open the Activate License panel.
3. Click **Online Activation** to activate the License in online mode.

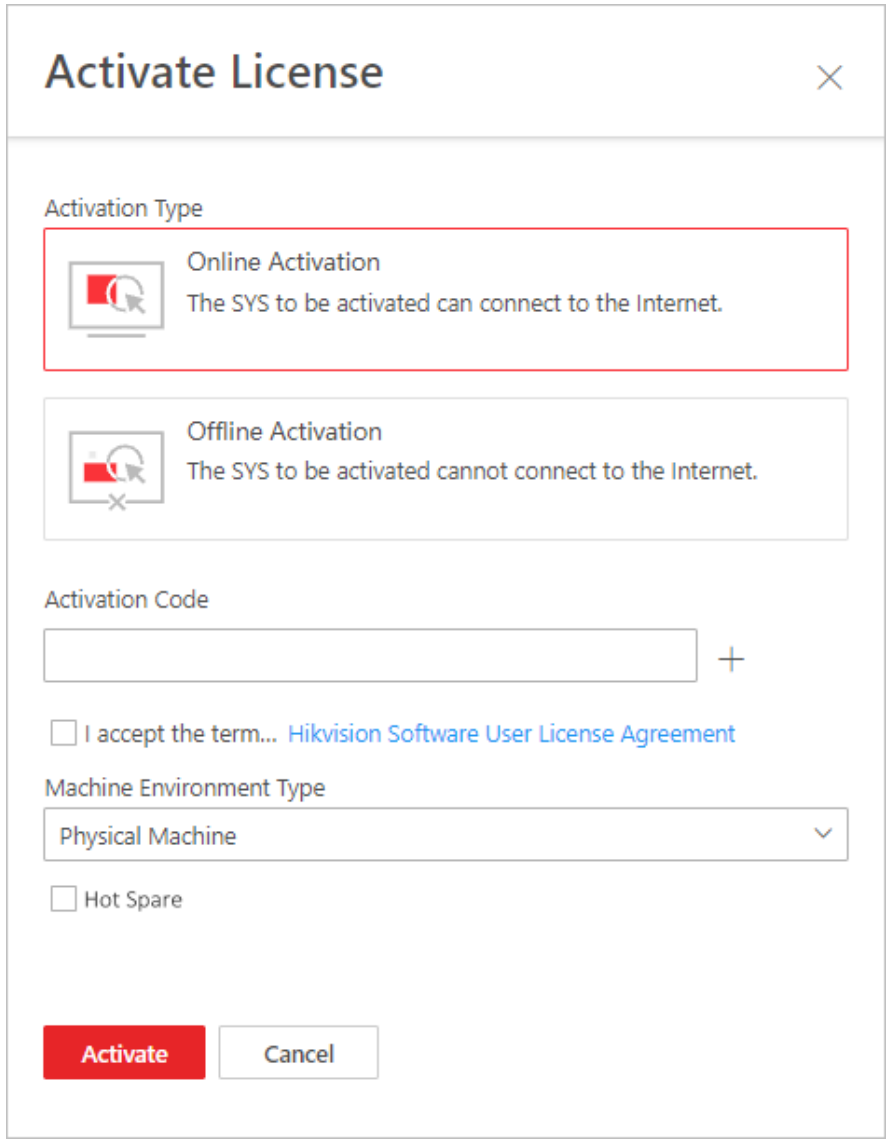


Figure 11-7 Activate License in Online Mode

4. Enter the activation code received when you purchased your License.

Note

- If you have purchased more than one Licenses, you can click + and enter other activation codes.
- The activation code should contain 16 characters or 32 characters (except dashes).

5. Check **I accept the terms of the agreement** to open the License Agreement panel and click **OK**.
6. **Optional:** Select the machine environment type.

   Physical Machine (Default)

   A physical computer that contains hardware specifications and is used for running the SYS. If the hardware changed, the License will be invalid, and the SYS may not run normally.

   AWS (Amazon® Web Services)

   A virtual machine that provides the cloud computing services for running the SYS.

   Azure (Microsoft® Azure)

   A virtual machine that provides the cloud computing services for running the SYS.

Note

If you select the AWS or Azure as the machine environment type, the pStor server, Streaming Server, and other external servers cannot access the platform. And the Rose hot spare system is also not supported.

7. **Optional:** Check the **Hot Spare**, select type, and enter the IP address if you want to build a hot spare system.

Note

- You must select Hot Spare mode when you install the system.
- For how to build the hot spare system, please contact our technical support engineers.

8. Click **Activate**.

   The email settings pane will appear after you activated the License.
9. Enter an email address for the admin user.

Note

This email is used to receive the License activation code when the admin user forgets the password for logging in to the platform and the activation code at the same time.

10. Set the email server parameters. See details in *Configure Email Account*.
11. Click **OK** to save the email settings.

11.6.2 Activate License - Offline

If the SYS to be activated cannot connect to the Internet, you can activate the License in offline mode.

Steps

1. Log in to HikCentral Professional via the Web Client.
2. On the Home page, click **Activate** to open the Activate License panel.
3. Click **Offline Activation** to activate the License in offline mode.

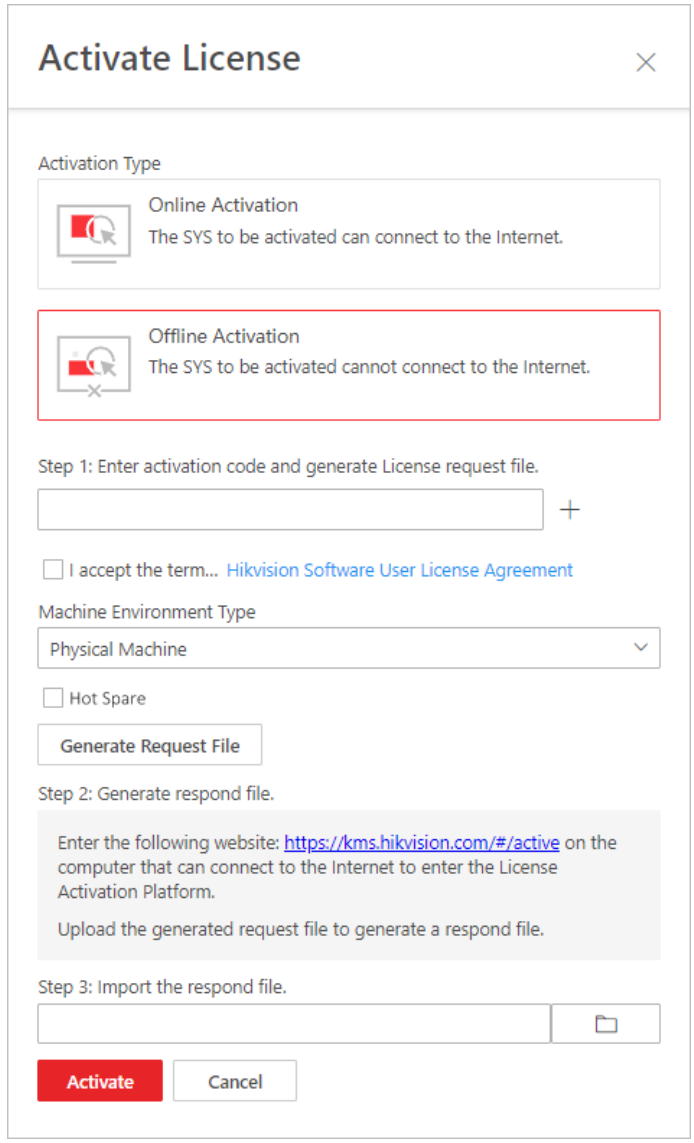


Figure 11-8 Activate License in Offline Mode

4. Enter the activation code received when you purchased your License.

Note

- If you have purchased more than one Licenses, you can click + and enter other activation codes.
- The activation code should contain 16 characters or 32 characters (except dashes).

5. Check **I accept the terms of the agreement** to open the License Agreement panel and click **OK**.

6. **Optional:** Select the machine environment type.

   Physical Machine (Default)

   A physical computer that contains hardware specifications and is used for running the SYS. If the hardware changed, the License will be invalid, and the SYS may not run normally.

   AWS (Amazon® Web Services)

   A virtual machine that provides the cloud computing services for running the SYS.

   Azure (Microsoft® Azure)

   A virtual machine that provides the cloud computing services for running the SYS.

   Note

   If you select the AWS or Azure as the machine environment type, the pStor server, Streaming Server, and other external servers cannot access the platform. And the Rose hot spare system is also not supported.

7. **Optional:** Check the **Hot Spare**, select type, and enter the IP address if you want to build a hot spare system.

   Note

   - You must select Hot Spare mode when you install the system.
   - For how to build the hot spare system, please contact our technical support engineers.

8. Click **Generate Request File**.

   A request file named "ActivationRequestFile.bin" will be downloaded. Save the request file to the proper directory or the removable storage medium (e.g., USB flash disk).

9. Copy the request file to the computer that can connect to the Internet.
10. On the computer which can connect to the Internet, enter the following website: ***https://kms.hikvision.com/#/active*** .
11. Click ↑ and then select the downloaded request file.

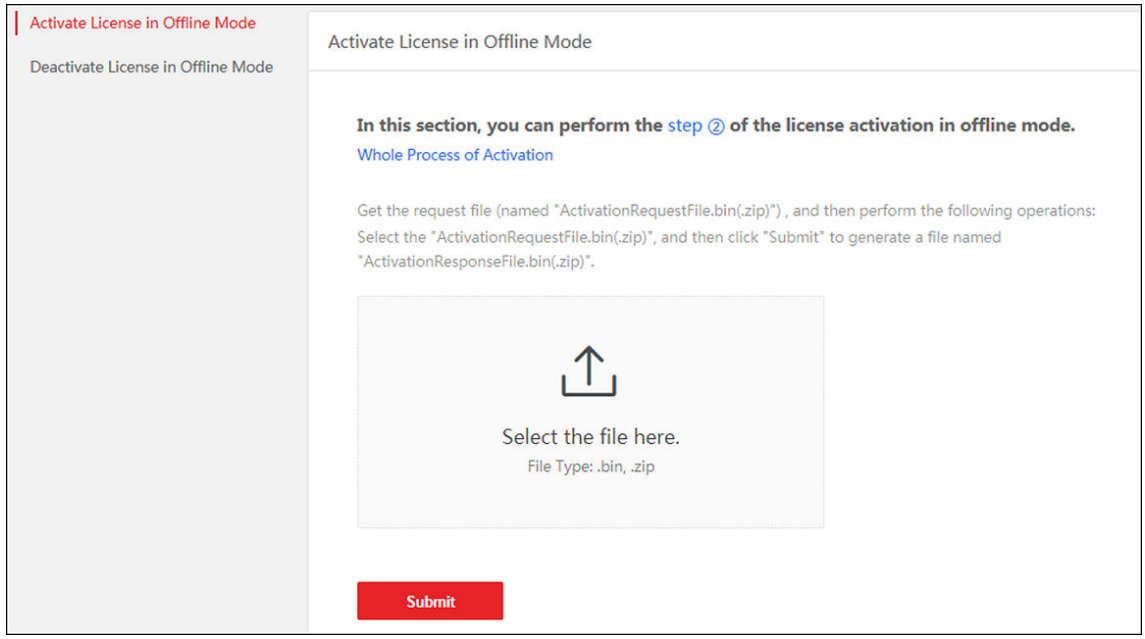


Figure 11-9 Select Request File

12. Click **Submit**.

    A respond file named "ActivationResponseFile.bin" will be downloaded. Save the respond file to the proper directory or the removable storage medium (e.g., USB flash disk).
13. Copy the respond file to the proper directory of the computer that accesses HikCentral Professional via the Web Client.
14. In the Offline Activation panel, click and select the downloaded respond file.
15. Click **Activate**.

    The email settings pane will appear after you activated the License.
16. Enter an email address for the admin user.

    Note

    This email is used to receive the License activation code when the admin user forgets the password for logging in to the platform and the activation code at the same time.
17. Set the email server parameters. See details in *Configure Email Account*.
18. Click **OK** to save the email settings.

11.6.3 Update License - Online

As your project grows, you may need to increase the connectable number of resources (e.g., cameras) for your HikCentral Professional. If the SYS to be updated can properly connect to the Internet, you can update the License in online mode.

Before You Start

Contact your dealer or our sales team to purchase a License for additional features.

Steps

1. Log in to HikCentral Professional via the Web Client. Refer to ***Login via Web Client (Administrator)*** for details.
2. In the top right corner of Home page, move the cursor to the **Maintenance and Management** to show the drop-down menu.
3. Click **Update License** in the drop-down menu to open the Update License panel.
4. Click **Online Update** to update the License in online mode.
5. Enter the activation code received when you purchase your License.

Note

- If you have purchased more than one Licenses, you can click + and enter other activation codes.
- The activation code should contain 16 characters or 32 characters (except dashes).

6. Check **I accept the terms of the agreement** to open the License Agreement panel and click **OK**.
7. Click **Update**.

11.6.4 Update License - Offline

As your project grows, you may need to increase the connectable number of cameras for your HikCentral Professional. If the SYS to be updated cannot connect to the Internet, you can update the system in offline mode.

Before You Start

Contact your dealer or our sales team to purchase a License for additional features.

Steps

1. Log in to HikCentral Professional via the Web Client.
2. In the top right corner of Home page, move the cursor to **Maintenance and Management** to show the drop-down menu.
3. Click **Update License** in the drop-down menu to open the Update License pane.
4. Click **Offline Update** to update the License in the offline mode.

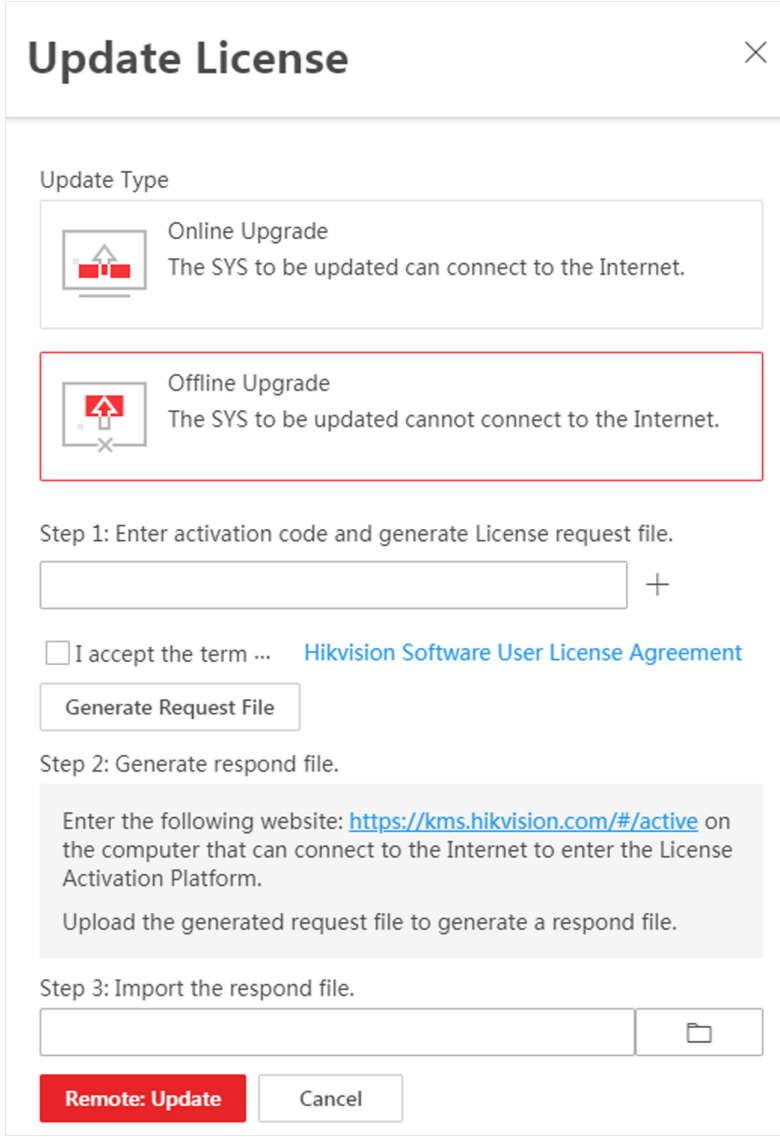


Figure 11-10 Update License in Offline Mode

5. Enter the activation code of your additional License.

Note

- If you have purchased more than one License, you can click + and enter other activation codes.
- The activation code should contain 16 characters or 32 characters (except dashes).

6. Check **I accept the terms of the agreement** to open the License Agreement panel and click **OK**.
7. Click **Generate Request File**.

   A request file named "ActivationRequestFile.bin" will be downloaded. Save the request file to the proper directory or the removable storage medium (e.g., USB flash disk).
8. Copy the request file to the computer that can connect to the Internet.

9. On the computer which can connect to the Internet, enter the following website: ***https://kms.hikvision.com/#/active*** .
10. Click and then select the downloaded request file.

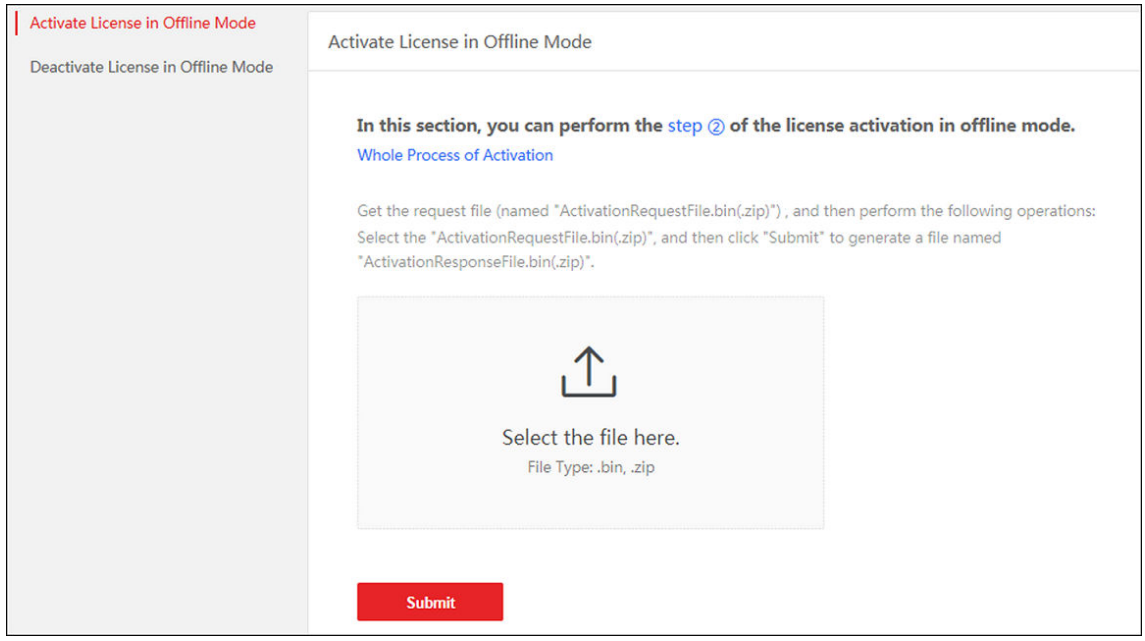


Figure 11-11 Select Request File

11. Click **Submit**.

    A respond file named "ActivationResponseFile.bin" will be downloaded. Save the respond file to the proper directory or the removable storage medium (e.g., USB flash disk).
12. Copy the respond file to the proper directory of the computer that accesses HikCentral Professional via the Web Client.
13. In the offline update panel, click and select the downloaded respond file.
14. Click **Update**.

11.6.5 Deactivate License - Online

If you want to run the SYS on another PC or server, you should deactivate the SYS first and then activate it again. If the computer or server on which the SYSrunning can properly connect to the Internet, you can deactivate the License in online mode.

Steps

1. Log in to HikCentral Professional via the Web Client. Refer to ***Login via Web Client (Administrator)*** .
2. In the top right corner of Home page, move the cursor to the **Maintenance and Management** to show the drop-down menu.
3. Click **Deactivate License** in the drop-down menu to open the Deactivate License panel.
4. Click **Online Deactivation** to deactivate the License in online mode.

5. Check the activation code(s) to be deactivated.
6. Click **Deactivate**.

11.6.6 Deactivate License - Offline

If you want to run the SYS on another computer or server, you should deactivate the SYS first and then activate the SYS again. If the SYS to be deactivated cannot connect to the Internet, you can deactivate the License in offline mode.

Steps

1. Log in to the HikCentral Professional via Web Client.
2. In the top right corner of the Client, move the cursor to the **Maintenance and Management** to show the drop-down menu.
3. Click **Deactivate License** in the drop-down menu to open the Deactivate License pane.
4. Click **Offline Deactivation** to deactivate the License in offline mode.

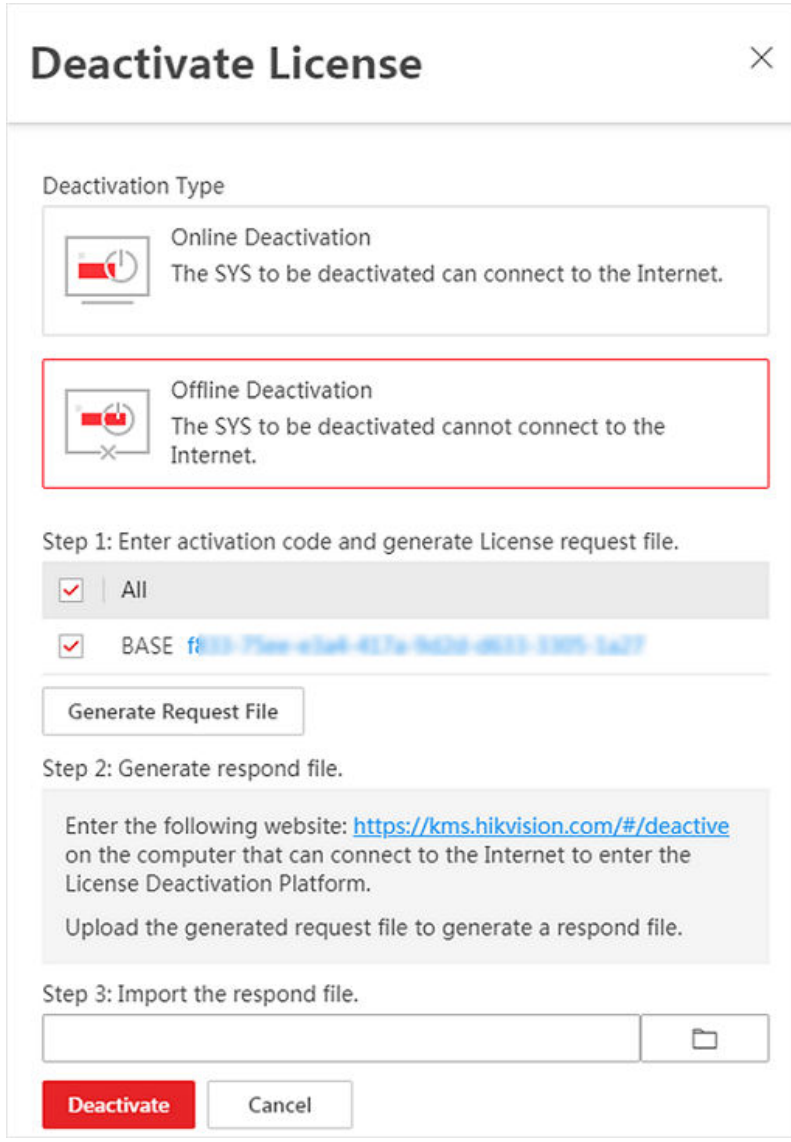


Figure 11-12 Deactivate License in Offline Mode

5. Check the activation code(s) to be deactivated.
6. Click **Generate Request File**.

Note

After the request file is generated, the selected activation code(s) will be unavailable.

A request file named "ActivationRequestFile.bin" will be downloaded. Save the request file to the proper directory or the removable storage medium (e.g., USB flash disk).

7. Copy the request file to the computer that can connect to the Internet.
8. On the computer which can connect to the Internet, enter the following website: ***https://kms.hikvision.com/#/deactive*** .

9. Click and then select the downloaded request file.

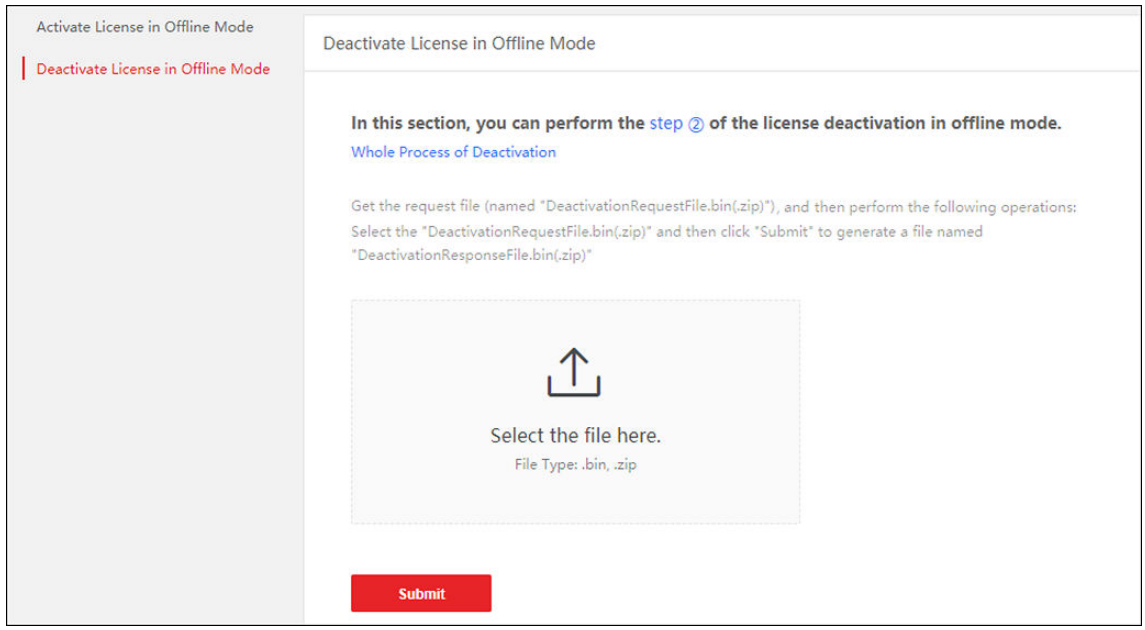


Figure 11-13 Select Request File

10. Click **Submit**.

    A respond file named "DectivationResponseFile.bin" will be downloaded. Save the respond file to the proper directory or the removable storage medium (e.g., USB flash disk).
11. Copy the respond file to the proper directory of the computer that accesses HikCentral Professional via the Web Client.
12. In the Offline Deactivation pane, click and select the downloaded respond file.
13. Click **Deactivate**.

11.6.7 View License Details

You can check the authorization details of the License you purchased and view the number of manageable devices and function of your platform. If the License is not activated, you can also view the trial period.

Steps

1. Log in to the HikCentral Professional via Web Client. See ***Login via Web Client (Administrator)*** for details.
2. In the top right corner of Home page, click **Maintenance and Management** to show the drop-down menu.
3. Click **License Details** in the drop-down menu to open the License Details panel.

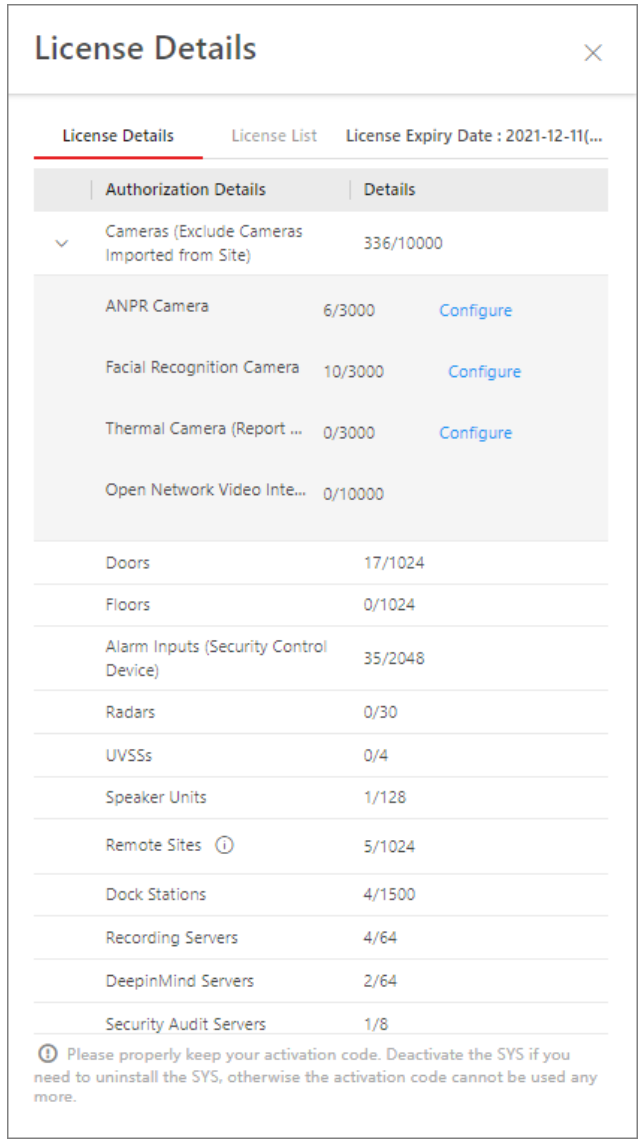


Figure 11-14 License Details Page

You can view the authorization details and check the expiry date of the trial License or the License you purchased.

4. **Optional:** Click › besides the Cameras(Exclude Cameras Imported from Site) to show the number of facial recognition cameras/ANPR cameras/thermal cameras (report supported)/Open Network Video Interface cameras and click **Configuration** to select the added cameras as these types of cameras, respectively.

Note

- Configuration of Open Network Video Interface cameras is not supported.
- If you do not configure the facial recognition camera/ANPR camera/thermal camera, these cameras' functions (facial recognition, plate recognition, and temperature report) cannot be performed normally in the platform.

5. **Optional:** Click **License List** to check all the activated License(s) of your platform and click an activation code to view the related authorization details.

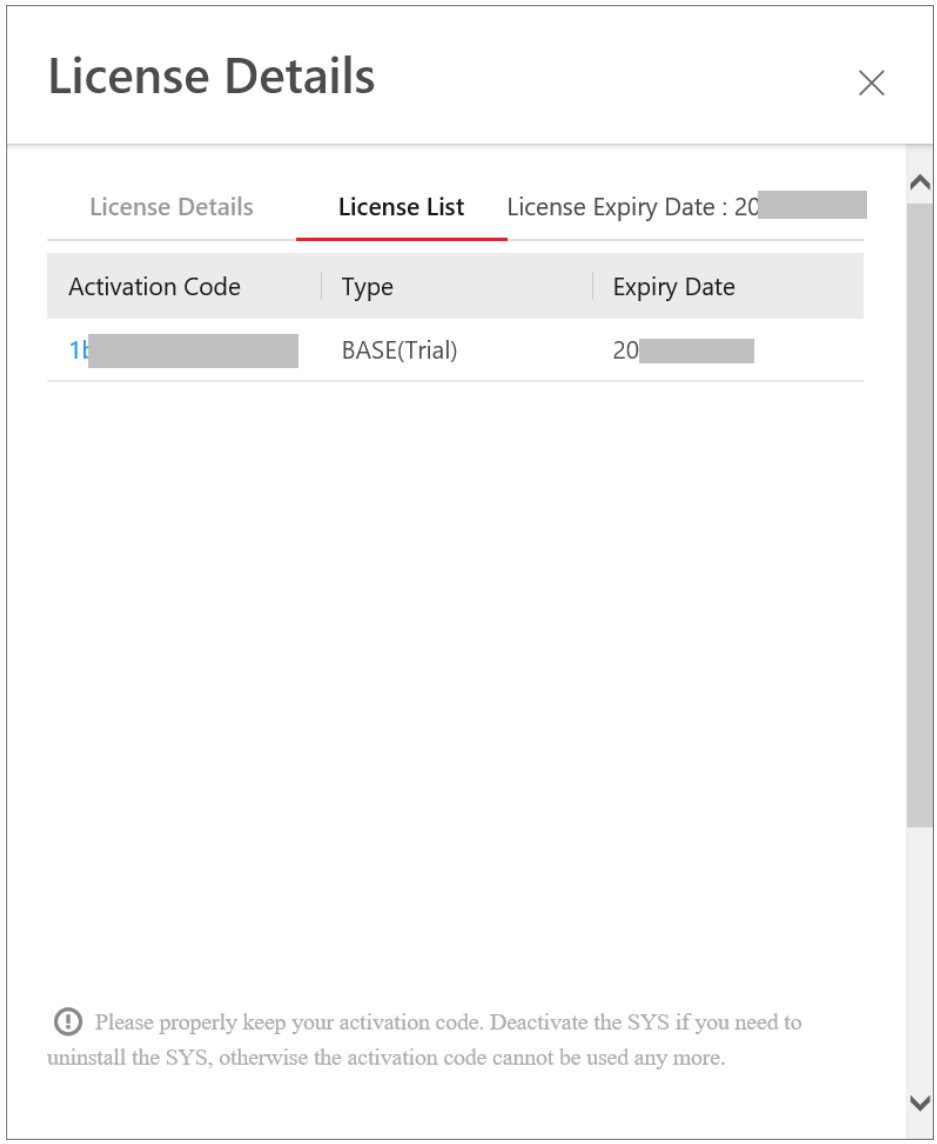


Figure 11-15 License List Page

11.6.8 Set SSP Expiration Prompt

SSP (Software Service Program) refers to the platform's maintenance service, which has an expire date and needs to be upgraded before expiration. You can set SSP expiration prompt on the platform. After that, when the SSP is going to expire, you can receive an email reminding the expiration every day during the configured period.

Steps

1. In the top right corner of the client, select **Maintenance and Management → License Details** to open the License Details panel.
2. Go to the bottom of details list and click ⚙ to enter the SSP Expiration Prompt Settings panel.
3. Set the **Overdue Reminder** switch to ON.
4. Set the days when you will receive the prompt email before expiration.

   Note

   - You should enter an integer between 1 to 365.
   - By default, the platform will send a prompt email 30 days before expiration.
5. Click **Add User** to add user(s) who can receive upgrade prompt.

   Note

   - You should configure the users' email addresses before adding them as recipients. The added users can receive upgrade prompt via the bound email addresses.
   - Up to 64 recipients can be added.
   - You can click × to delete the added user(s).
6. Click **Add Email** to add email address(es).

   Note

   You can add email of both the platform user(s) and other user(s). The platform will send expiration prompt to the added email address(es).
7. Click **Save**.

11.7 Consumption Management

The Consumption Management module is mainly used for payments at a dining hall. You can add consumption devices to the platform and configure related parameters according to your needs, so that you can search for consumption records and generate consumption reports in different dimensions.

In the top left corner of Home page, select ⊞ → **All Modules → Consumption → Consumption Overview** to enter the Consumption Overview page. On the Consumption Overview page, you can go to different pages quickly, view consumption statistics today, and distribution reports.

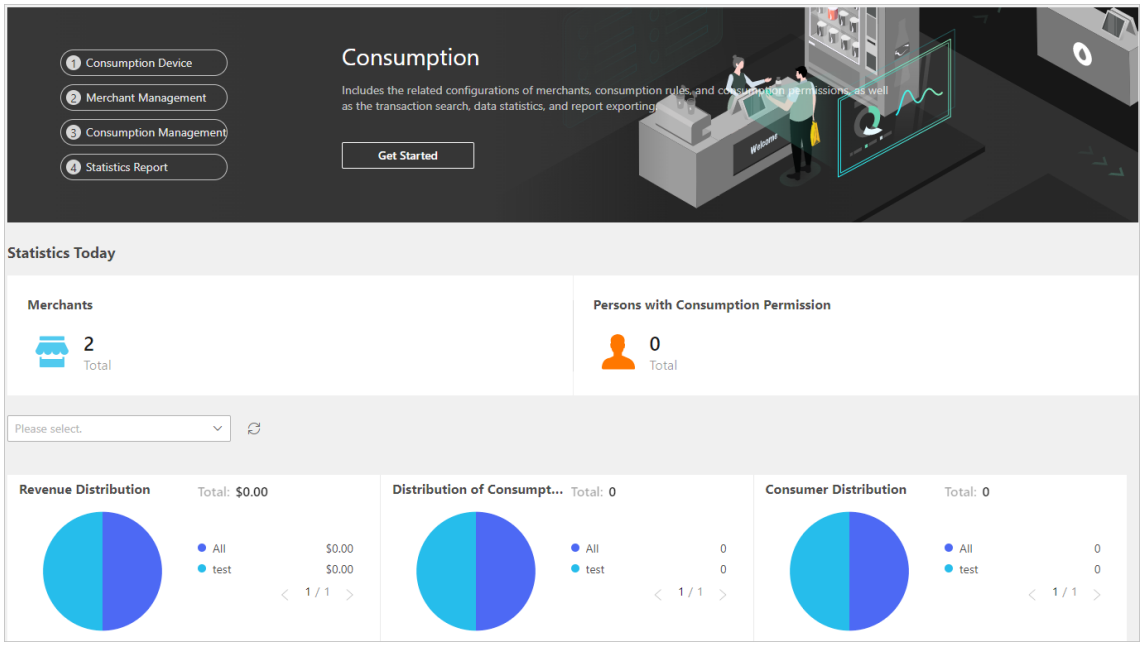


Figure 11-16 Consumption Overview

11.7.1 Flow Chart of Consumption Management

The following flow chart shows the process of the configurations and operations of consumption module.

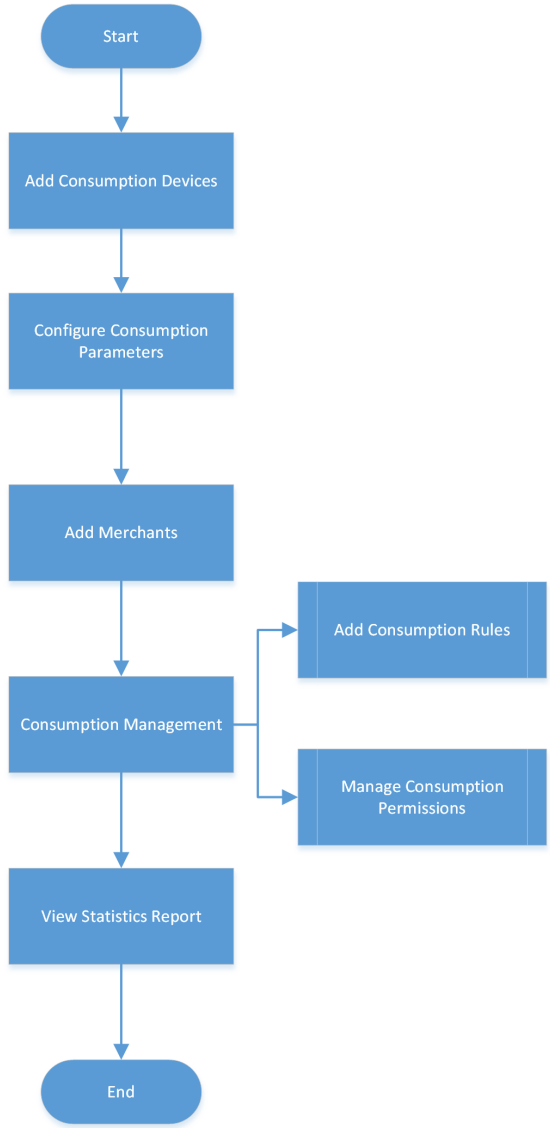


Figure 11-17 Flow Chart of Consumption Management

- Add Consumption Devices: at first, you should add consumption devices to the platform by different ways. See *Manage Consumption Devices*.
- Configure Consumption Parameters: configure related parameters according to your needs, including general parameters, meal types, and schedule templates. If your scenario changes, you can edit the parameters. See ***Set General Parameters*** .
- Add Merchants: the platform supports managing merchants of different levels. You can add different merchants to the platform and link consumption devices to them. See ***Manage Merchants*** .

- Consumption Management: configure consumption rules for consumption devices and manage consumption permissions. See ***Add a Consumption Rule*** and ***Manage Consumption Permissions*** .
- View Statistics Report: search consumption records and generate different consumption reports. See ***Search for Consumption Records*** and ***Manage Consumption Report*** .

11.7.2 Configure Consumption Parameters

You can configure the consumption parameters, including the general parameters, meal types, and schedule templates.

Set General Parameters

You can configure the general parameters including the threshold for consumption times, currency unit, auto applying parameters, and auto calculating parameters.

In the top left corner of the client, select → **All Modules → Consumption → Basic Configuration → General Configuration** .

Threshold for Consumption Times

You can enable the **Threshold for Consumption Times** to set the maximum consumption times per person for a specific meal type.

Note

The **Threshold for Consumption Times** are applicable only when the device is set to charge according to the consumption times of a person. For details about consumption rules, refer to ***Add a Consumption Rule*** .

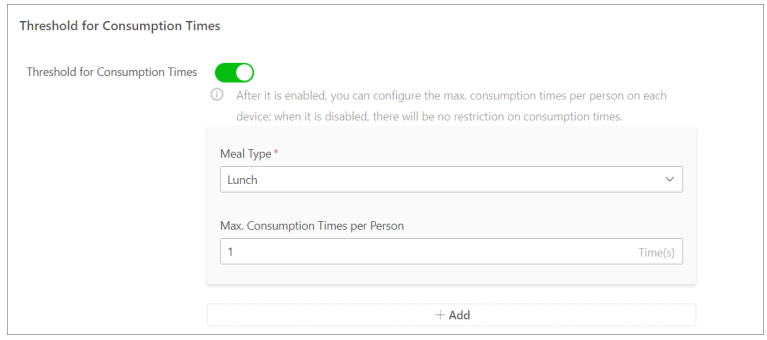


Figure 11-18 Set Threshold for Consumption Times

Meal Type

You need to select the meal type in the drop-down list. For adding more meal types, refer to ***Manage Meal Type*** .

Max. Consumption Times per Person

The maximum consumption times per person need to be set between 1 to 100.

You can click **Add** to add more time thresholds.

Currency Unit

You can select the currency unit in consumption, including Renminbi Yuan, U.S Dollar, Euro, Pound, etc.

Figure 11-19 Set Currency Unit

Auto Apply

You can enable **Auto Apply** and set a fixed time to automatically apply the consumption permissions. For applying consumption permissions, refer to ***Apply Consumption Permissions to Devices*** .

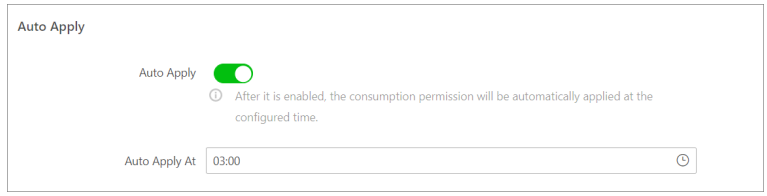


Figure 11-20 Set Auto Applying Parameters

Auto Apply

After it is enabled, the consumption permission will be automatically applied at the configured time.

Auto Apply At

The time when the consumption permission will be applied automatically.

Auto Calculate

You can enable **Auto Calculate** for automatically calculating the consumption amount at the fixed time.

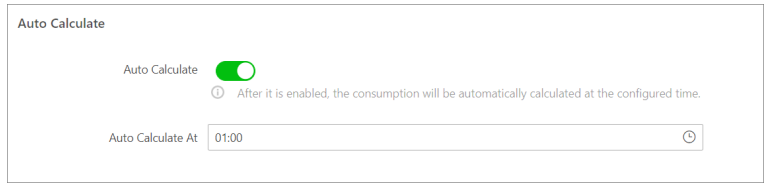


Figure 11-21 Set Auto Calculating Parameters

Auto Calculate

After it is enabled, the consumption revenue will be automatically calculated at the configured time.

Auto Calculate At

The time when the consumption revenue will be calculated automatically.

Manage Meal Type

You can manage the meal types including adding meal types, editing meal type information, and deleting the added meal types.

Steps

1. In the top left corner of the client, select → **All Modules → Consumption → Basic Configuration → Meal Type Management** .

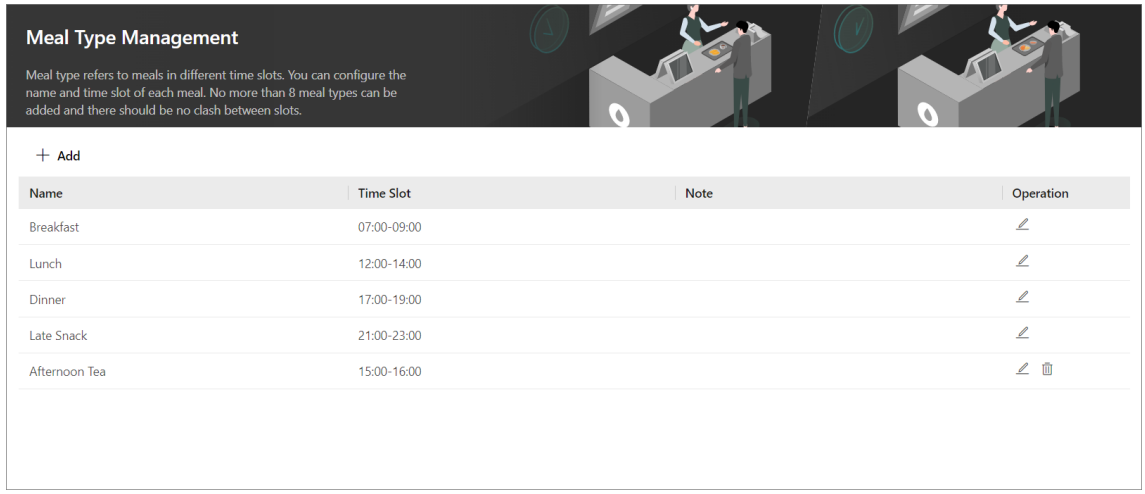


Figure 11-22 Manage Meal Type

2. Click **Add** to open the adding meal type pane.
3. Specify the meal type name and the time slot, and enter the note if needed.
4. Click **Add** in the pane to add the new meal type to the list.

Note

No more than 8 meal types can be added and there should be no clash between slots.

5. **Optional:** Click in the Operation column of a meal type to edit the information.
6. **Optional:** Click in the Operation column to delete the meal type.

The default meal types (Breakfast, Lunch, Dinner, and Late Snack) cannot be deleted.

Add Consumption Schedule Template

Consumption schedules define the start/end time of valid consumption slots for assigning consumption permissions. You can create consumption schedules in advance and use them as templates when configuring consumption schedules.

Steps

1. In the upper-left corner of Home page, select → **All Modules → Consumption → Basic Configuration → Schedule Template** .
2. Click + to open the Add Consumption Schedule Template pane.

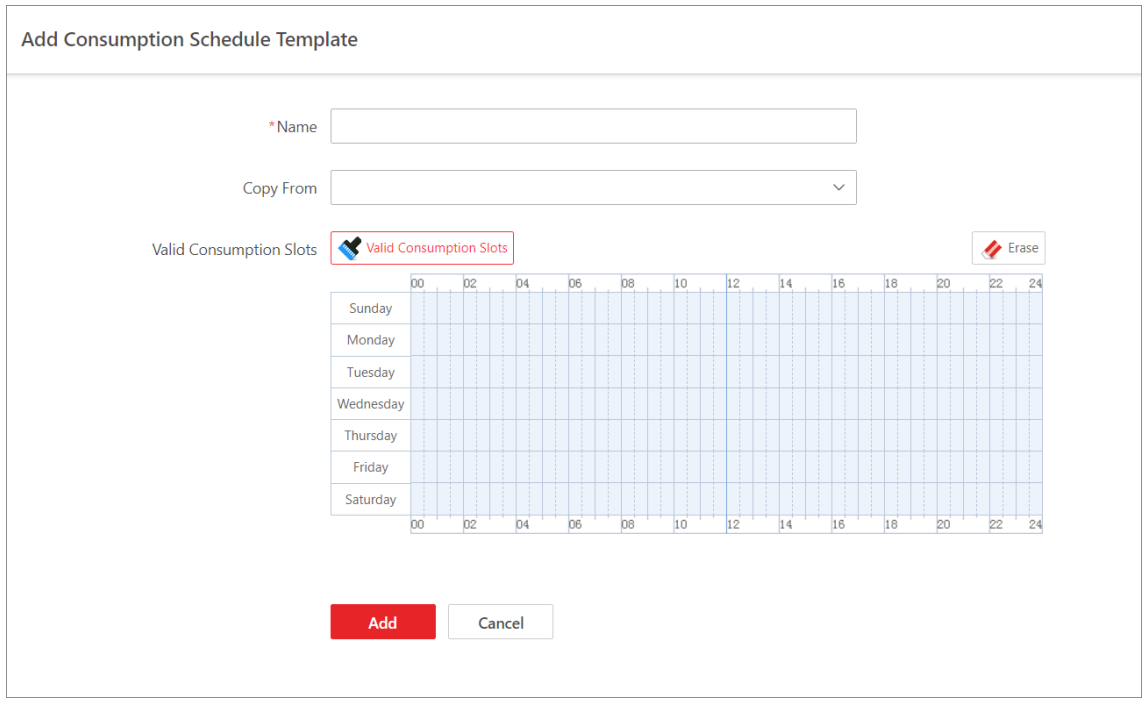


Figure 11-23 Add a Consumption Schedule Template

3. Set parameters for the consumption schedule template.

   Name

   The name created for the consumption schedule template, such as "All-Day Consumption Schedule Template".

   Copy Form

   You can select a template in the drop-down list, and the following table will be covered by the form of the selected template.
4. Adjust the valid consumption slots.
   - Move the cursor to the program bar on the timeline and drag the right and left edges to adjust the beginning time and end time of the valid consumption.
   - Click the valid consumption bar on the timeline, and adjust the beginning time and end time of the program in the input box.

- Click **Erase** to delete the valid consumption in this time period.

5. Click **Add** to save the current template.
6. **Optional:** After creating schedule templates, perform the following operations as needed.

Edit Schedule Template	Click the name of the schedule template to enter the editing page and you can edit the schedule template information.
Delete Schedule Template	Select the schedule template, click to delete the selected schedule templates.
Search for Schedule Template	Enter keywords on the upper right corner of the page, and click the Enter to quickly find the target schedule templates.

11.7.3 Manage Merchants

The platform supports managing merchants of different levels. You can add different merchants to the platform and link consumption devices to them.

Steps

1. In the top left corner of Home page, select → **All Modules** → **Consumption** → **Merchant Management** .
2. Click + on the top left, or select an existing merchant and then click + .
3. Enter the basic information about the merchant, including name, upper-level merchant, address, contact, etc.
4. In the Consumption Device area, check consumption devices and click › .
5. Click **Add** to add the merchant and go back to the merchant list page; or click **Add and Continue** to add the current merchant and continue to add a new merchant.
6. **Optional:** Perform the following operations.

Edit a Merchant	Select a merchant on the left, and then click to edit its information.
Clear Consumption Devices Linked to a Merchant	Select a merchant on the left, and then click **Clear** on the right to clear all consumption devices linked to the merchant.
Unlink a Consumption Device from a Merchant	Select a merchant on the left to show the linked consumption devices. Hover the cursor on a device and click to unlink the device from the merchant.

11.7.4 Add a Consumption Rule

By adding a consumption rule, you can select different charging rules for different consumption devices.

Steps

1. In the top left corner of Home page, select → **All Modules** → **Consumption** → **Consumption Management** .
2. Select **Consumption Rule** on the left.
3. Click **Add Consumption Rule**.
4. In the Consumption Device area, check available devices and then click › .
5. **Optional:** In the Copy From drop-down list, select a device which has been configured with a consumption rule, so as to copy the device's consumption rule to the selected devices.
6. Enter the rule name.
7. Select a consumption rule graph, and then draw the timetable.
8. Select a consumption verification mode.
9. Select a charging mode in the Charge By (Default) drop down list.

   Fixed Amount

   The platform charges a fixed amount when the person pays.

   Consumption Times

   The platform charges according to the consumption times of a person. For example, you can set a threshold of consumption times for different meal types of a factory. Workers at the factory can verify for a meal type no more than the threshold of consumption times. See ***Set General Parameters*** for details about how to set the threshold of consumption times.
10. Click **Show More Device Advanced Configuration** and then select a consumption verification mode.
11. **Optional:** Enable **Offline Consumption**.

    Offline Consumption

    If the consumption device is offline, the platform will record the consumption without charging. After the consumption device turns online, the platform will charge according to the consumption records.
12. Click **Add** to add the consumption rule and go back to the consumption rule list; or click **Add and Continue** to add the current consumption rule and continue to add a new consumption rule.
13. **Optional:** Click to apply a consumption rule to a device.

11.7.5 Manage Consumption Permissions

Consumption permissions define during which time periods the persons or person groups can consume in which merchants. After assigning consumption permissions to persons or person groups, you need to apply the permissions to devices to make them take effect.

Consumption Permission Overview

The Consumption Permission page shows the consumption permission and its applying status of each person in the person group. You can also perform operations such as applying permissions to devices and batch replacing consumption schedule template on this page.

In the top left corner of Home page, select → **All Modules → Consumption → Consumption Management** , and click **Consumption Permission** on the left panel.

Select a person group, and have an overview of consumption permissions in this group.

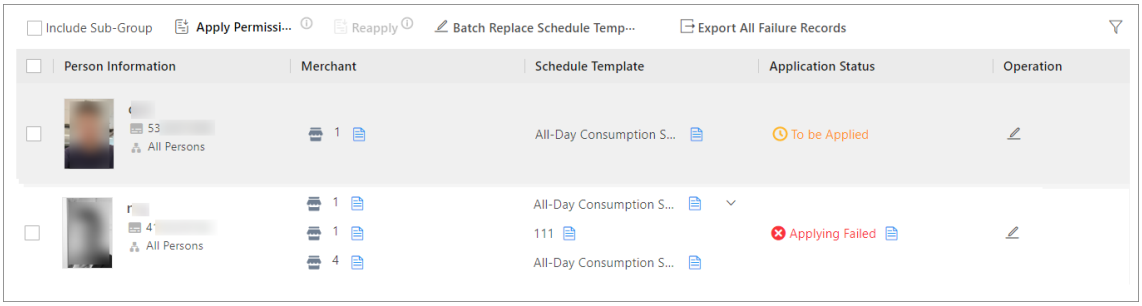


Figure 11-24 Consumption Permission Overview

You can perform the following operations on this page.

Include Sub-Group	Check **Include Sub-Group** to display the persons' consumption permissions of the sub-groups of the selected person group.
Apply Permissions to Device	Click **Apply Permissions to Device**to apply persons' consumption permissions to devices. For details, refer to ***Apply Consumption Permissions to Devices*** .
Reapply Permission	Check one or more persons whose application status is **Applying Failed**, click **Reapply** to reapply consumption permissions of the selected persons to devices.
Batch Replace Schedule Template	Click **Batch Replace Schedule Template**, select the template to be replaced, select the person(s) or person group(s) to be replaced, and select the new template to batch replace schedule template for the selected person(s) or person group(s).
Export All Failure Records	Click **Export All Failure Records** to export all the applying failed records.
Edit Permission	Click in the Operation column to edit the consumption permission of the selected person.

Filter Persons	Click in the upper right corner, and set conditions to filter persons.
View Failure Reason	For applying failed records, click in the Application Status column to view the failure details.
View Details	Hover on in the Merchant column and Schedule Template column to view the details of merchant(s) and the schedule template.

Assign Consumption Permissions by Person

You can assign consumption permissions by person to specify during which time period(s) the person(s) can consume in which merchant(s).

Steps

1. In the top left corner of Home page, select → **All Modules** → **Consumption** → **Consumption Management** .
2. Click **Assign Permission by Person** on the left panel.
3. Click **Assign Permission**.

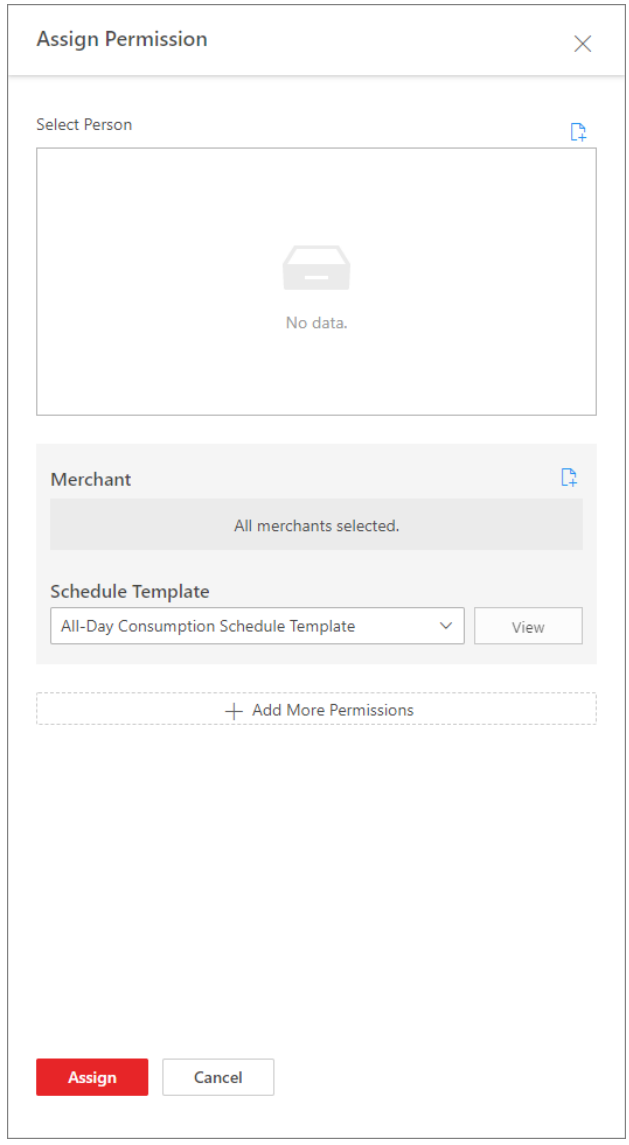


Figure 11-25 Assign Permission Pane

4. In the Assign Permission pane, click to select person(s) to assign consumption permissions to.
5. Click below to select merchant(s).

Note

By default, all merchants are selected.

6. Click to select a schedule template from the drop-down list.

Note

- You can click **View** to view the details of the selected template.
- You can click **Add Schedule Template** to add a new schedule template. For details, refer to ***Add Consumption Schedule Template*** .

7. **Optional:** Click **Add More Permissions** to add more permissions.

Note

Refer to the previous two steps for details.

8. Click **Assign**.

   The corresponding permissions are assigned to the selected person(s).

9. **Optional:** Perform more operations after assigning permissions.

Edit Permissions	Click to edit the consumption permissions of the selected person.
Unassign Permissions	• Cancel Selected Permissions: Select a person, click **Unassign → Cancel Selected Permissions** , select the permissions to be canceled, and click **OK**. • Cancel All Permissions: Select a person, click **Unassign → Cancel All Permissions** , and click **OK**.
Filter Persons	Click in the upper right corner, and set conditions to filter persons.
View Details	Hover on in the Merchant column and Schedule Template column to view the details of merchant(s) and the schedule template.

Assign Consumption Permissions by Person Group

You can assign consumption permissions by person group to specify during which time period(s) the person group(s) can consume in which merchant(s).

Steps

1. In the top left corner of Home page, select → **All Modules → Consumption → Consumption Management** .
2. Click **Assign Permission by Person Group** on the left panel.
3. Assign permissions to one or multiple person groups.
   - Select a person group and click **Assign Permission**.
   - Hover on beside **Assign Permission**, and click **Batch Assign Permissions**.
4. **Optional:** If you select **Batch Assign Permissions**, select the person groups to assign the permissions to.

Note

You can check **Select Sub-Groups**, then the sub-groups of the selected person groups will also be selected.

5. Click to select merchant(s).

Note

By default, all merchants are selected.

6. Click ⌄ to select a schedule template from the drop-down list.

Note

- You can click **View** to view the details of the selected template.
- You can click **Add Schedule Template** to add a new schedule template. For details, refer to ***Add Consumption Schedule Template*** .

7. **Optional:** Click **Add More Permissions** to add more permissions.

Note

Refer to the previous two steps for details.

8. Click **Assign**.

   The corresponding permissions are assigned to the selected person group(s).

9. **Optional:** Perform more operations after assigning permissions.

Edit Permissions	Select a person group, and click ✎ in the operation column to edit the consumption permissions.
Unassign Permissions	Select a person group to view all its permissions on the right side, select one or more permissions, and click **Cancel Permission** to cancel the selected permissions. Select a person group, move the mouse cursor to ⌄ , and click **Clear All Permissions** to clear all permissions of the selected person group.
Filter Permissions	Click ▽ in the upper right corner, and set conditions to filter consumption permissions.
View Details	Select a person group, click › to view the details of merchant(s) and the schedule template.

Apply Consumption Permissions to Devices

After assigning consumption permissions to persons or person groups, you need to apply the permissions to devices to make it take effect.

Before You Start

Make sure you have applied consumption permissions to persons or person groups. Refer to ***Assign Consumption Permissions by Person*** and ***Assign Consumption Permissions by Person Group*** for details.

Steps

1. In the top left corner of Home page, select ⊞ → **All Modules** → **Consumption** → **Consumption Management** .
2. Click **Consumption Permission** on the left panel.

3. Click **Apply Permissions to Device**.

Note

Only consumption permissions of persons whose application status is **To be Applied** can be applied to devices.

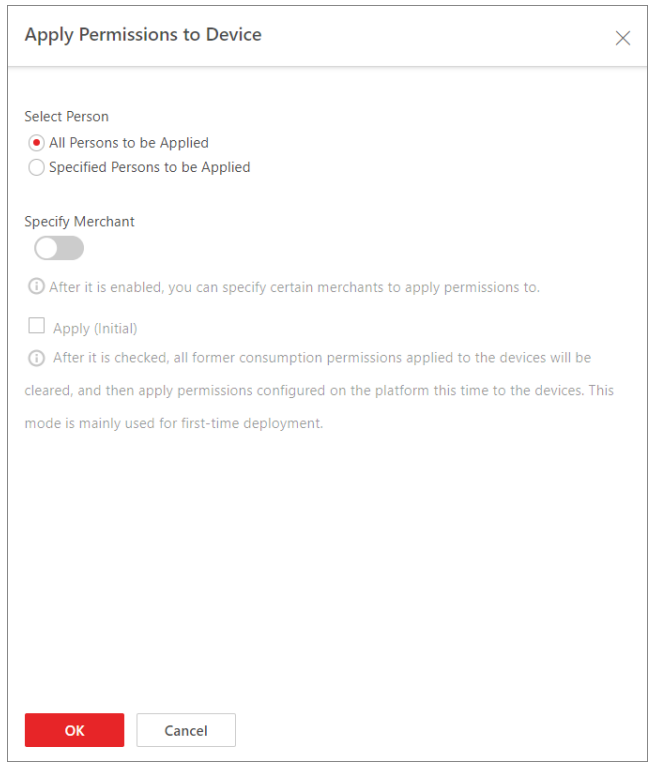


Figure 11-26 Apply Permissions to Device

4. Select person(s).
   - Click **All Persons to be Applied** to select all persons to be applied.
   - Click **Specified Persons to be Applied**, click , and select specified person(s) to be applied.
5. **Optional:** Switch on **Specify Merchant** and specify certain merchant(s) to apply permissions to.

Note

By default, all merchants are selected.

6. **Optional:** Check **Apply (Initial)**.

Note

If you check this, all former consumption permissions applied to the devices will be cleared, and permissions configured on the platform this time will be applied to the devices. This mode is mainly used for first-time deployment.

7. Click **OK** to start applying permissions to the devices.

11.7.6 Search for Consumption Records

You can set conditions to search for normal and abnormal consumption records.

1. In the top left corner of Home page, select → **All Modules** → **Consumption** → **Transaction Search** , and click **Consumption Record**.
2. Click **Normal Consumption Record** or **Abnormal Consumption Record** on the top side.

Note

Consumption records without person information (person name, ID, and person group) are abnormal consumption records. Also, consumption records will be generated when a person's consumption times for a certain type of meal exceed the configured value, or the consumption permission of a person dose not match with that is configured on the platform.

3. Set the needed conditions, including person name, person ID, person group, etc., and click **Search**. The consumption records that meet the conditions are displayed on the right side. The explanations of some parameters are as follows:

Consumption Device

Select consumption device(s) to be searched for consumption records.

Handling Status

Note

This condition is for abnormal consumption records only.

Not Handled

Search for the consumption records that are not handled.

Handled

Search for the consumption records that have been handled.

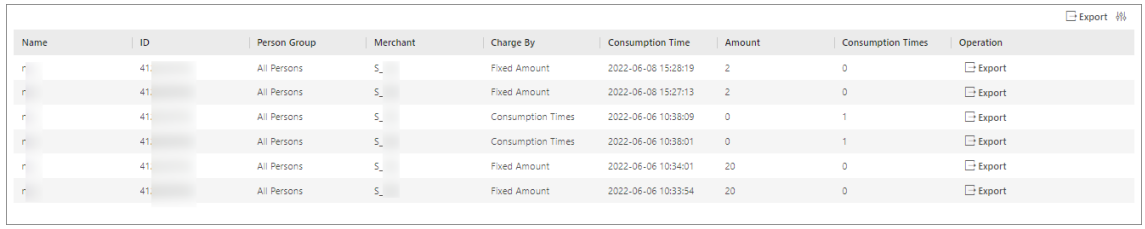


Figure 11-27 Normal Consumption Records

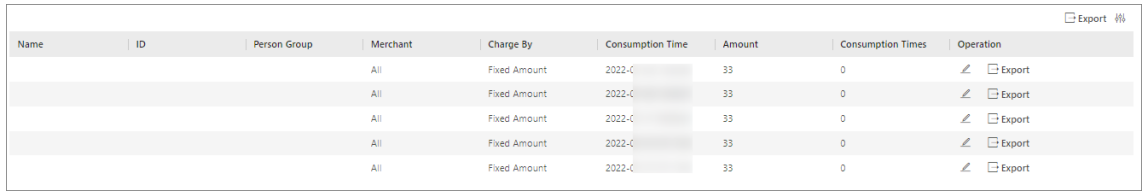


Figure 11-28 Abnormal Consumption Records

Note

in the Operation column represents that the record is not handled.

4. You can do more of the following for the searched consumption records.
   - **Export Single Record**: Click **Export** in the Operation column to export the current consumption record.
   - **Export All Records**: Click **Export** in the upper right corner, select the file type (only Excel is supported currently), and click **Export** to export all the consumption records.
   - **Customize List Items**: Click and select the items to be displayed in the list.
   - **Handle Abnormal Record**: For an abnormal consumption record, click in the Operation column, enter the description, and click **OK** to handle this record.

11.7.7 Manage Consumption Report

There are four types of reports including personal consumption report, person group consumption report, revenue reports of merchant, and revenue reports of device. You can customize reports by setting conditions such as report target, meal type, and time. You can also export reports in Excel and PDF.

View Person Consumption Report

You cam view consumption reports of a specified person or specified persons.

In the top left corner of the Client, select → **All Modules → Consumption → Statistics Report → Personal Consumption Report** .

- Select target person(s), meal type, and time to generate a report.
- Click **Calculate Again** and select target person(s), meal type, and time to generate a report.

In a personal consumption report, you can view total consumption amount, total consumption times, and total records of consumption charged by times of the specified person(s) in pie charts.

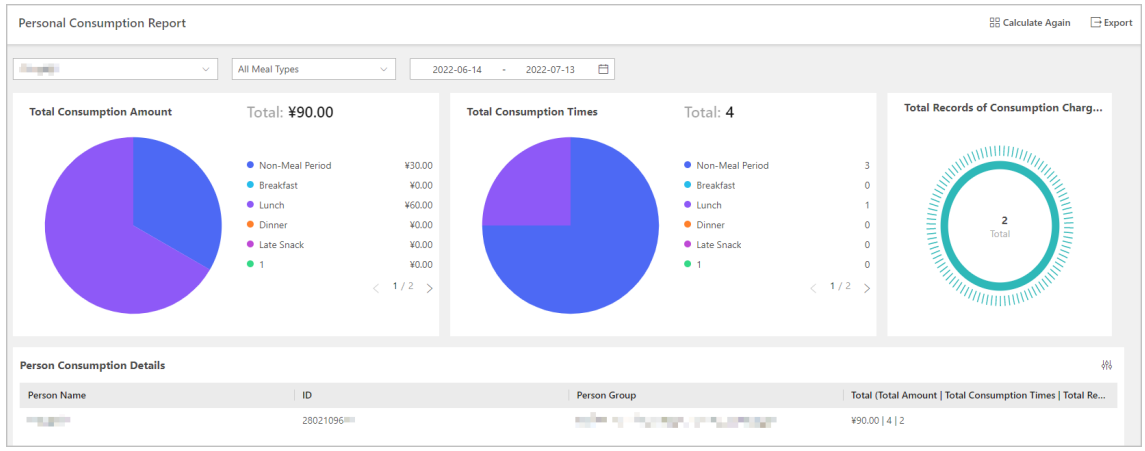


Figure 11-29 Person Consumption Report

Note

- Total Consumption Times = Total Records of Consumption Charged by Fixed Amount + Total Records of Consumption Charged by Times.
- The item **Total Records of Consumption Charged by Times** refers to the number of consumptions that are charged by times. In other words, it refers to how many times did all report targets consume.

You can also click to set what you want to display in the **Person Consumption Details** table.

You can click **Export** to export the report in Excel or PDF.

View Person Group Consumption Report

You cam view consumption reports of a specified person group or specified person groups.

In the top left corner of the Client, select → **All Modules** → **Consumption** → **Statistics Report** → **Person Group Consumption Report** .

- Select target person group(s), meal type, and time to generate a report.
- Click **Calculate Again** in the upper-right corner, select target person group(s) and time, and click **OK** to generate a report.

In a person group consumption report, you can view total consumption amount, total consumption times, total number of consumers, and total records of consumption charged by times of the specified person group(s) in pie charts.

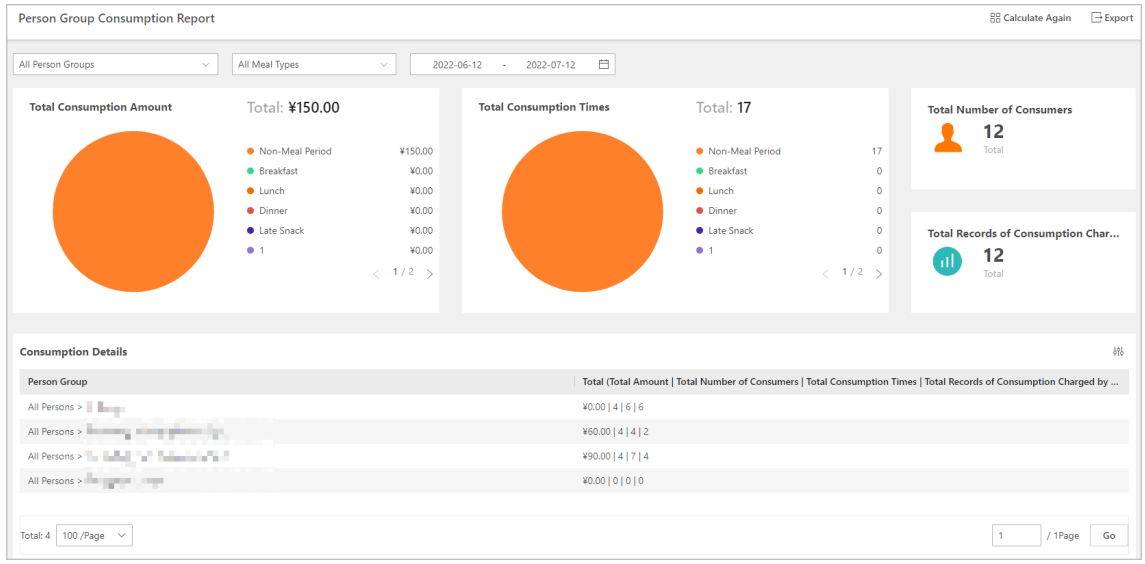


Figure 11-30 Person Group Consumption Report

Note

- Total Consumption Times = Total Records of Consumption Charged by Fixed Amount + Total Records of Consumption Charged by Times.
- The item **Total Records of Consumption Charged by Times** refers to the number of consumptions that are charged by times. In other words, it refers to how many times did all report targets consume.

You can also click to set what you want to display in the **Consumption Details** table.

You can click **Export** to export the report in Excel or PDF.

View Revenue Report of Merchants

You cam view daily and monthly revenue reports of a specified merchant or specified merchants.

In the top left corner of the Client, select → **All Modules → Consumption → Statistics Report → Revenue Report of Merchant → Daily Revenue Report of Merchant** .

Select target person merchant(s), meal type, and time to generate a report.

In a revenue report of merchant(s), you can view revenue, consumption times, number of consumers, and total records of consumption charged by times of the store(s) in pie charts. Also, you can view Monthly Revenue Report of Merchant by clicking **Monthly Revenue Report of Merchant**.

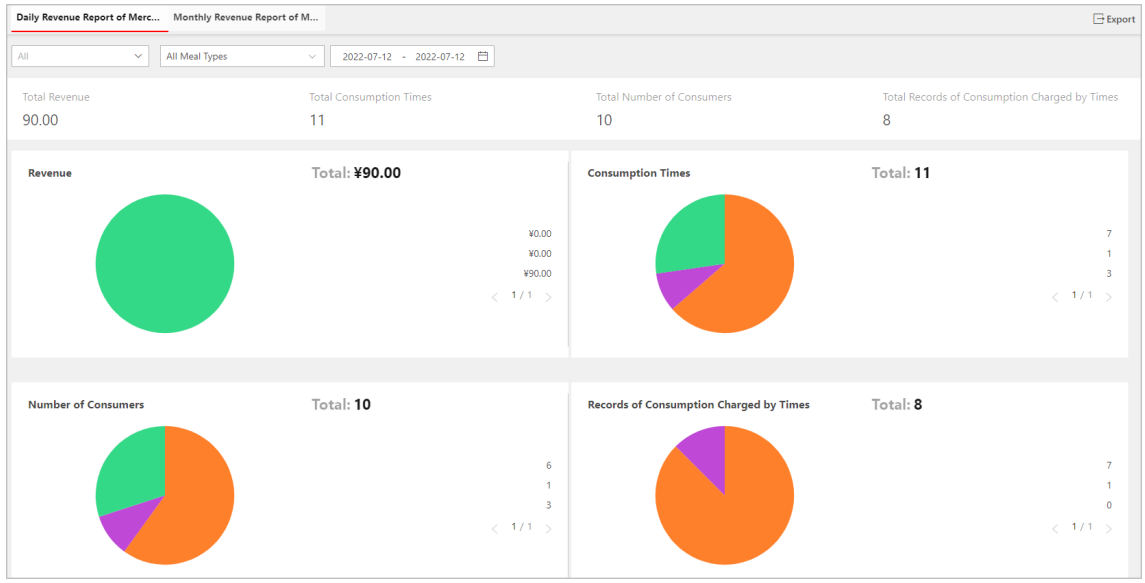


Figure 11-31 Revenue Report of Merchants

Note

- Total Consumption Times = Total Records of Consumption Charged by Fixed Amount + Total Records of Consumption Charged by Times.
- The item **Total Records of Consumption Charged by Times** refers to the number of consumptions that are charged by time.

You can also click to set what you want to display in the **Daily Revenue Details of Merchants** / **Monthly Revenue Details of Merchants** table.

You can click **Export** to export the report in Excel or PDF.

View Revenue Report of Devices

You cam view daily and monthly revenue reports of a specified device or specified devices.

In the top left corner of the Client, select → **All Modules** → **Consumption** → **Statistics Report** → **Revenue Report of Device** .

- Select target device(s), meal type, and time to generate a report.
- Click **Calculate Again** in the upper-right corner, select target device(s) and time, and click **OK** to generate a report.

In a revenue report of device(s), you can view total revenue, total consumption times, total number of consumers, and total records of consumption charged by times of the device(s) in pie charts.

Note

- Total Consumption Times = Total Records of Consumption Charged by Fixed Amount + Total Records of Consumption Charged by Times.
- The item **Total Records of Consumption Charged by Times** refers to the number of consumptions that are charged by times. In other words, it refers to how many times did all report targets consume.

You can also click to set what you want to display in the **Revenue Details of Devices** table.

You can click **Export** to export the report in Excel or PDF.

Appendix A. Tips When Collecting/Comparing Face Picture

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

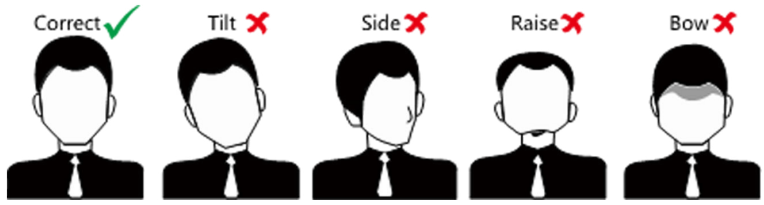
Expression

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

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

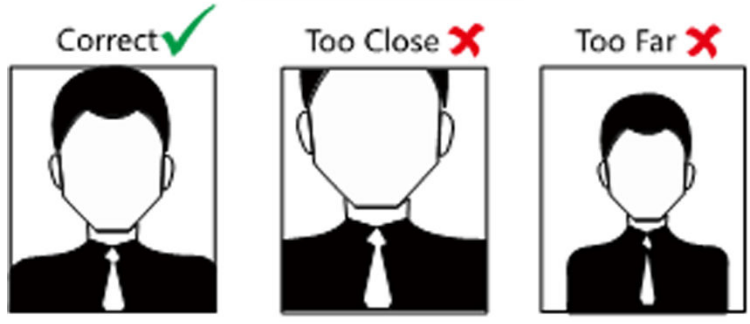
Posture

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



Size

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



Appendix B. Tips for Installation Environment

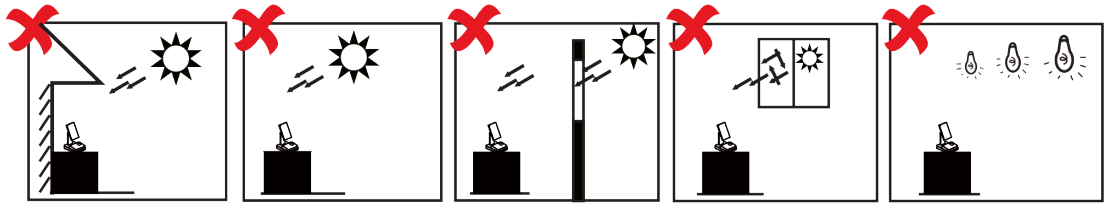
1. Light Source Illumination Reference Value

Candle: 10Lux

Bulb: 100~850Lux

Sunlight: More than 1200Lux

2. Avoid backlight, direct and indirect sunlight



Appendix C. Dimension

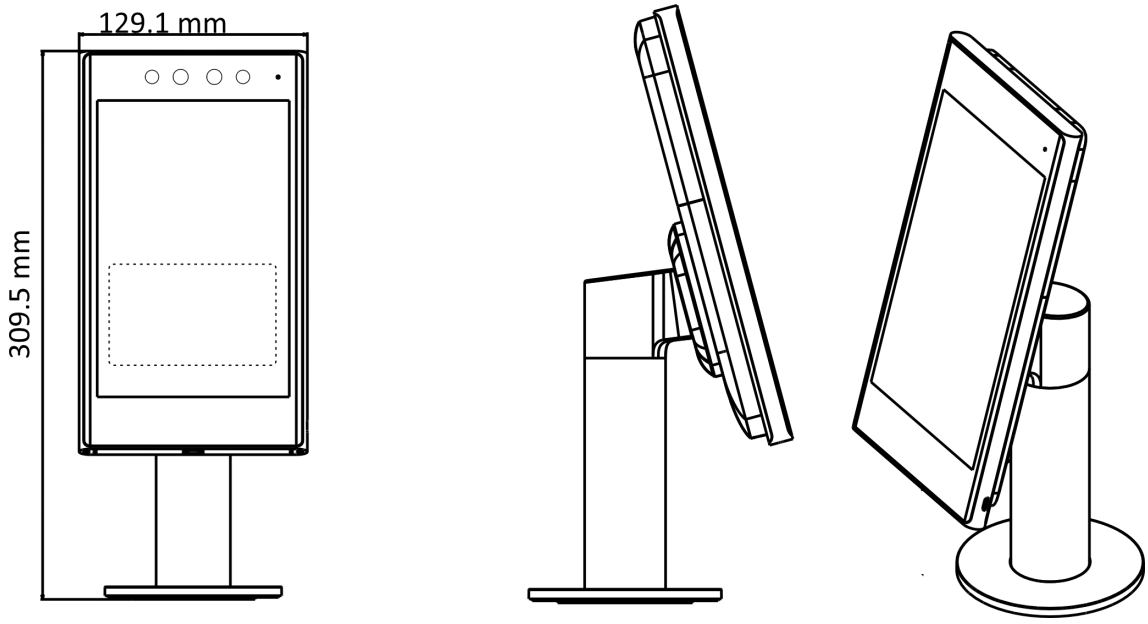


Figure C-1 Dimension of Device with Turnstile Bracket

Note

Take single screen as an example.

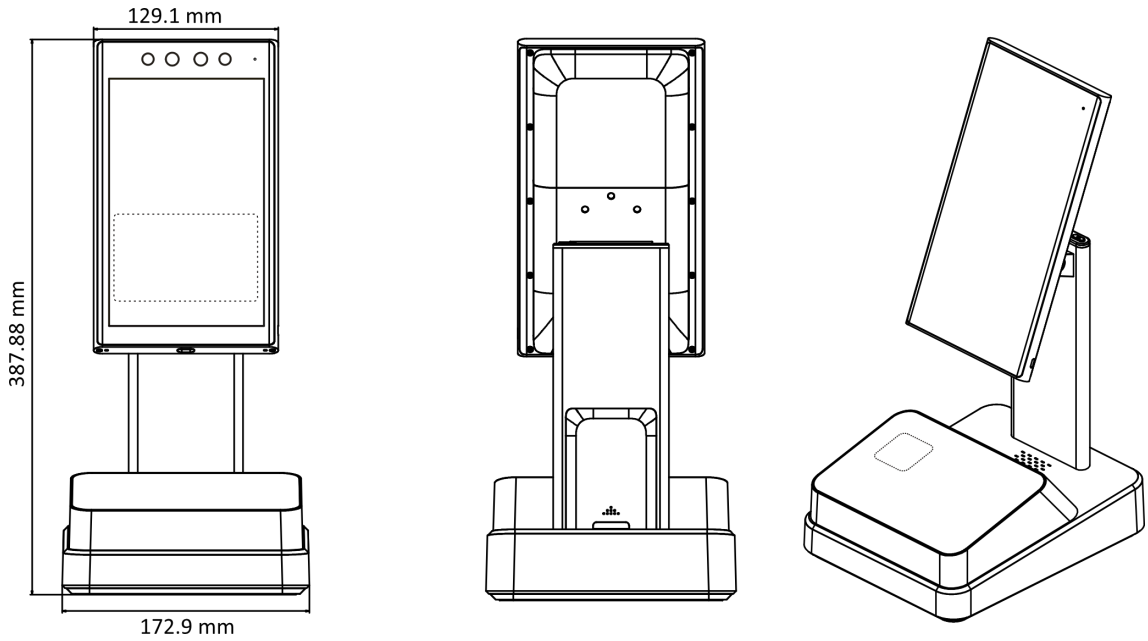


Figure C-2 Dimension of Device on Base (Single Screen)


See Far, Go Further