DS-K5033 Series Visitor Terminal

User Manual

Regulatory Information

FCC Information

Please take attention that changes or modification not expressly approved by the party responsible for compliance could void the user’s authority to operate the equipment.

FCC compliance: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

—Reorient or relocate the receiving antenna.

—Increase the separation between the equipment and receiver.

—Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

—Consult the dealer or an experienced radio/TV technician for help

This equipment should be installed and operated with a minimum distance 20cm between the radiator and your body.

FCC Conditions

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

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

EU Conformity Statement

This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed under the EMC Directive 2014/30/EU, RE Directive 2014/53/EU,the RoHS Directive 2011/65/EU

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

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

Safety Instruction

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

The precaution measure is divided into Dangers and Cautions:

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

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

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

⚠ Danger:

- All the electronic operation should be strictly compliance with the electrical safety regulations, fire prevention regulations and other related regulations in your local region.
- Do not connect several devices to one power adapter as adapter overload may cause over-heat or fire hazard.
- Please make sure that the power has been disconnected before you wire, install or dismantle the device.
- When the product is installed on wall or ceiling, the device shall be firmly fixed.
- If smoke, odors or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service center.
- Do not ingest battery, Chemical Burn Hazard.
  This product contains a coin/button cell battery. If the coin/button cell battery is swallowed, it can cause severe internal burns in just 2 hours and can lead to death.
  Keep new and used batteries away from children. If the battery compartment does not close securely, stop using the product and keep it away from children. If you think batteries might have been swallowed or placed inside any part of the body, seek immediate medical attention.
- If the product does not work properly, please contact your dealer or the nearest service center. Never attempt to disassemble the device yourself. (We shall not assume any responsibility for problems caused by unauthorized repair or maintenance.)

⚠ Cautions:

- Do not drop the device or subject it to physical shock, and do not expose it to high electromagnetism radiation. Avoid the equipment installation on vibrations surface or places subject to shock (ignorance can cause equipment damage).
- Do not place the device in extremely hot (refer to the specification of the device for the detailed operating temperature), cold, dusty or damp locations, and do not expose it to high electromagnetic radiation.
- The device cover for indoor use shall be kept from rain and moisture.

- Exposing the equipment to direct sun light, low ventilation or heat source such as heater or radiator is forbidden (ignorance can cause fire danger).
- Do not aim the device at the sun or extra bright places. A blooming or smear may occur otherwise (which is not a malfunction however), and affecting the endurance of sensor at the same time.
- Please use the provided glove when open up the device cover, avoid direct contact with the device cover, because the acidic sweat of the fingers may erode the surface coating of the device cover.
- Please use a soft and dry cloth when clean inside and outside surfaces of the device cover, do not use alkaline detergents.
- Please keep all wrappers after unpack them for future use. In case of any failure occurred, you need to return the device to the factory with the original wrapper. Transportation without the original wrapper may result in damage on the device and lead to additional costs.
- Improper use or replacement of the battery may result in hazard of explosion. Replace with the same or equivalent type only. Dispose of used batteries according to the instructions provided by the battery manufacturer.
- Biometric recognition products are not completely applicable to anti-spoofing environments. If you require a higher security level, use multiple authentication modes.

Available Models

Product Name	Model
Visitor Terminal	DS-K5033MW, DS-K5033MW-D, DS-K5033TMW-D

Contents

Chapter 1 Appearance

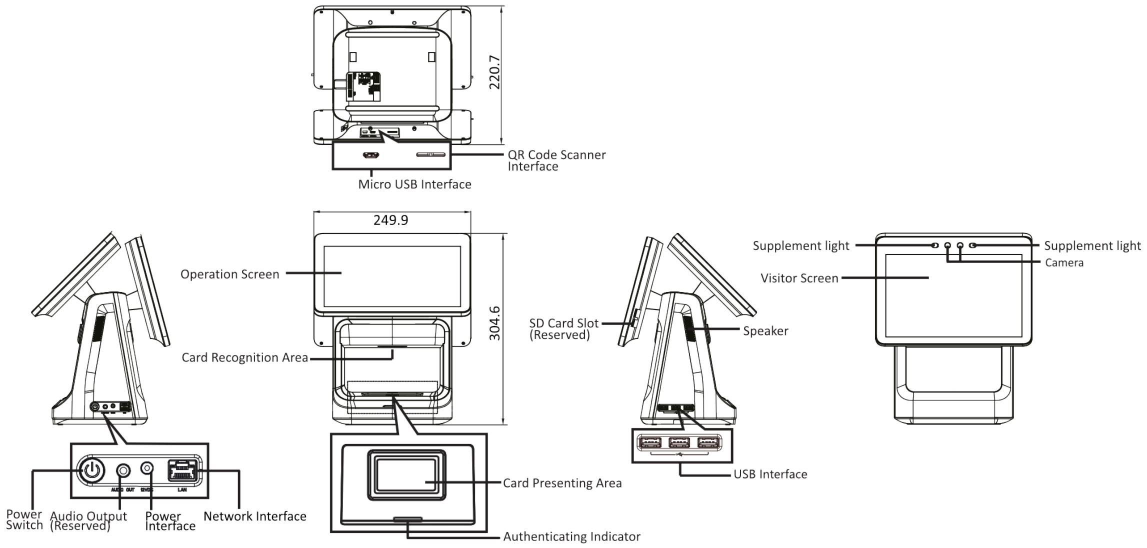


Figure 1-1 Dual Small Screens Device

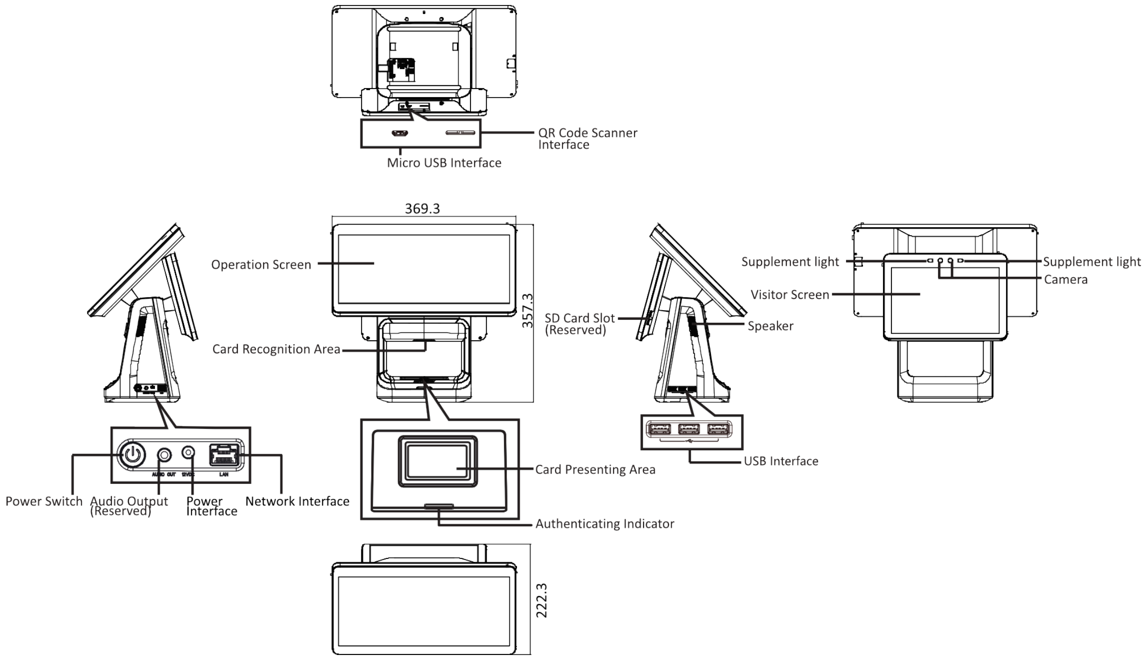


Figure 1-2 Large and Small Screens Device

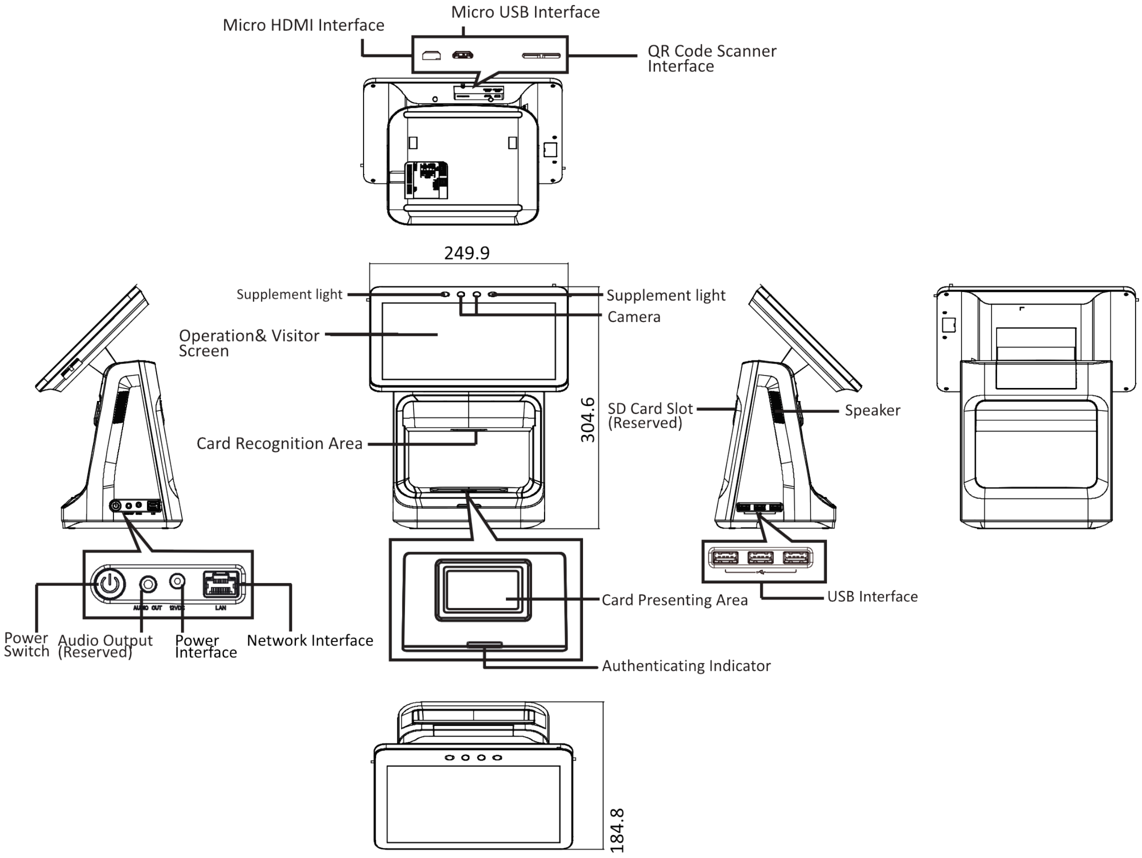


Figure 1-3 Single Screen Device

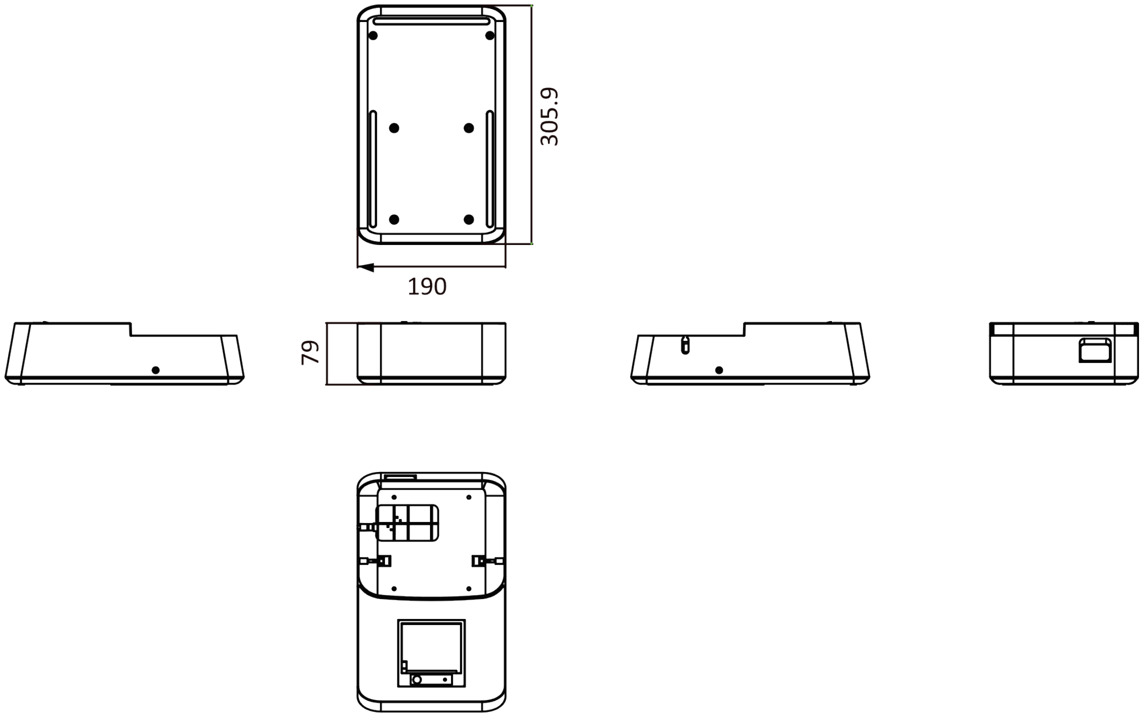


Figure 1-4 Base of Device

Note

The base can be used to print receipt and scan visitor QR code.

Chapter 2 Installation

2.1 Installation Environment

- Avoid backlight, direct sunlight, and indirect sunlight.

Note

- The device doesn't support outdoor use.
- For details about installation environment, see *Tips for Installation Environment*.

2.2 Install Device

Steps

1. Put the device on the surface.

   Note

   This equipment is suitable for mounting on concrete or other non-combustible surface only.
2. Plug the power supply in the power interface.
3. Press the power switch to power on the device. The device will enter the main page after powering on.

2.3 Install Base

Steps

1. According to the direction shown, turn the sheet metal hook outward, load it into the corresponding slot on the printer, and pay attention to the elastic position along the shrapnel.

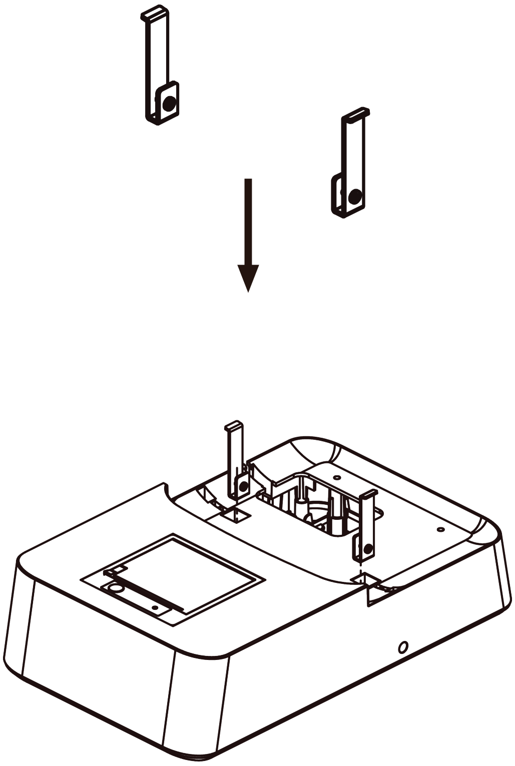


Figure 2-1 Load Sheet Metal Hook

2. Plug the printer's exposed cable into the designated position for silk screen printing at the bottom of the base, and then place the base vertically down on the concave surface of the printer fit.

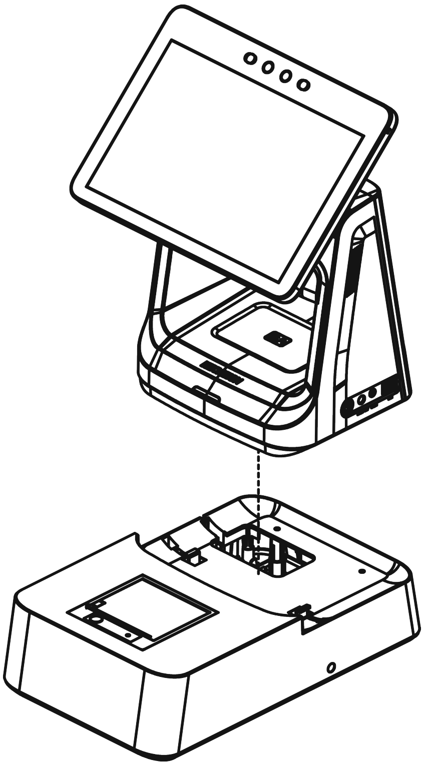


Figure 2-2 Place Base

3. Take out 2 long screws, insert into the corresponding round hole channel in the direction shown in the figure, and screw them in until they are tightened.

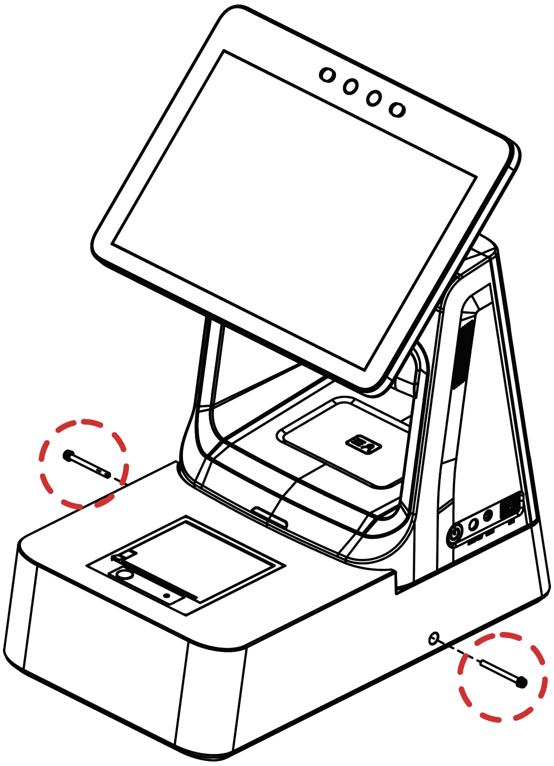


Figure 2-3 Secure Device

Note

If you need to use the device with a base, please use the adapter that comes standard with the base for power.

2.4 Install Temperature Measurement Module

Steps

1. Use a screwdriver from the accessory kit to remove the two screws in Figure 1 and remove the temperature measurement module shield.

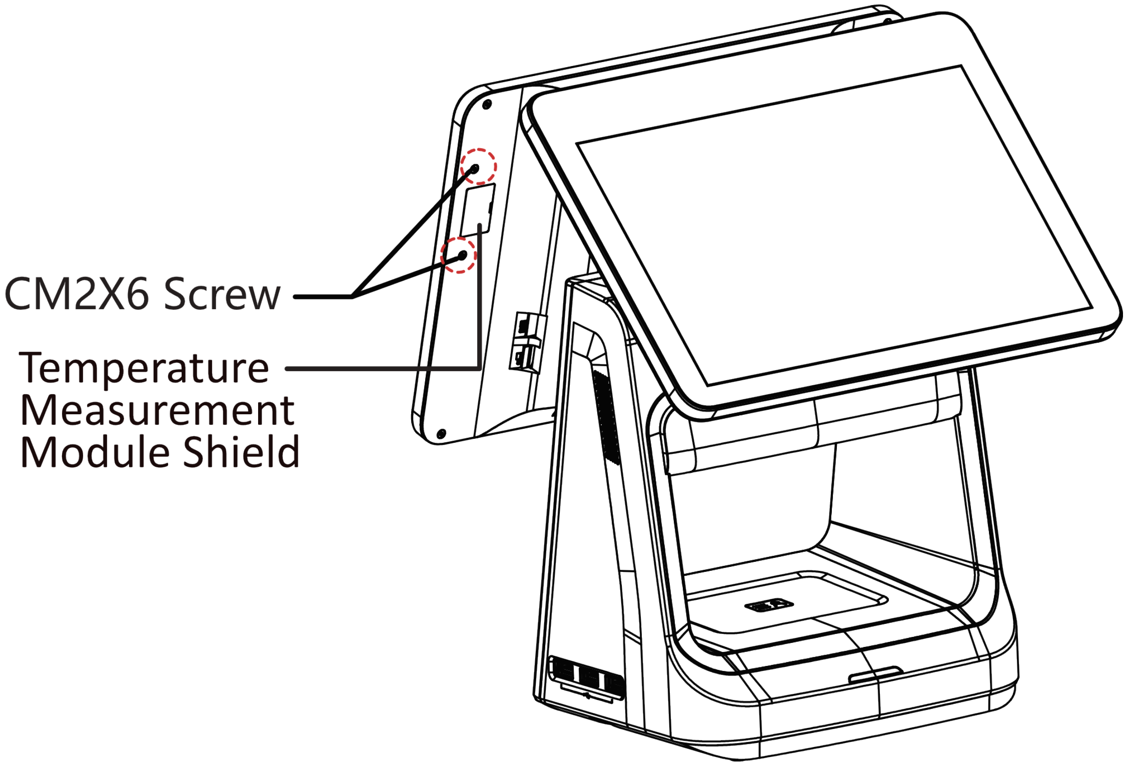


Figure 2-4 Remove Screw

2. Using the SC-SM2X8L4.5 screws in the accessory kit, secure the temperature measurement module to the two removed screw holes.

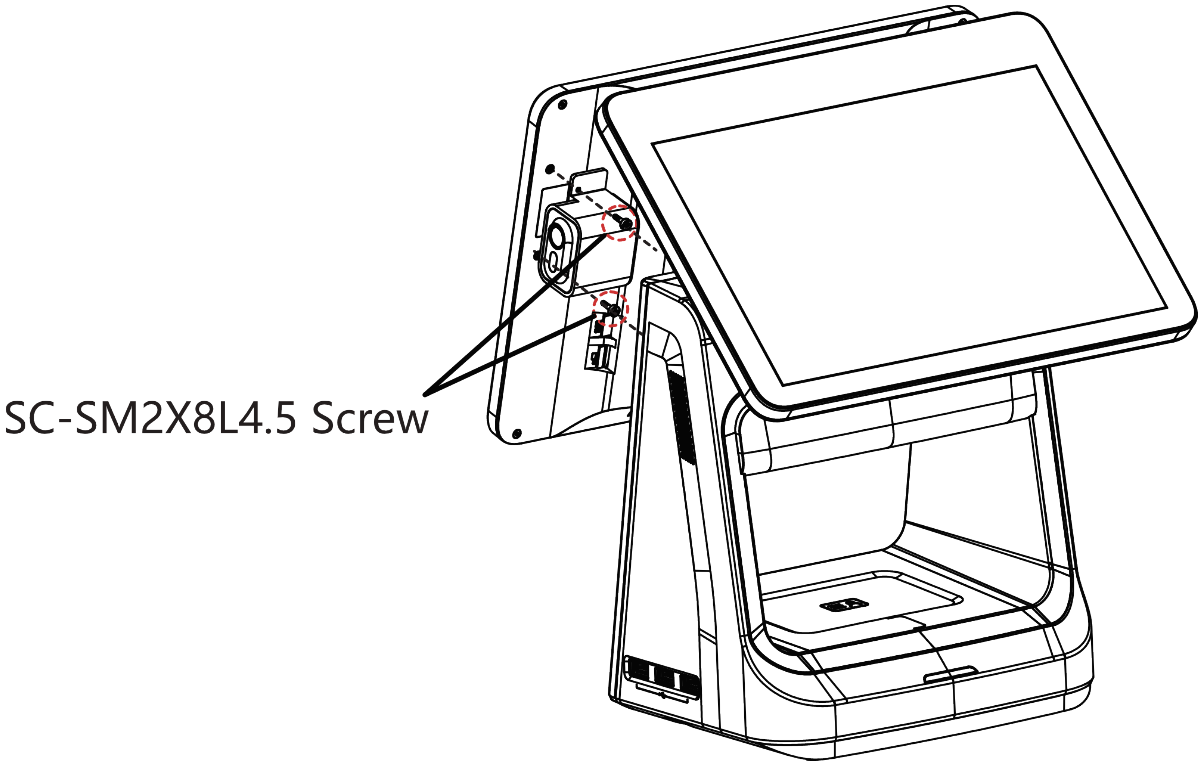


Figure 2-5 Secure Screw

Chapter 3 Wiring

The device supports connecting to the RS-485 terminal, the door lock, the exit button, the alarm output/input devices, the Wiegand card reader, the access controller, and the power supply. You can wire the peripherals according to the descriptions below.

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

Note

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

3.1 Wire Normal Device

You can connect the terminal with normal peripherals.

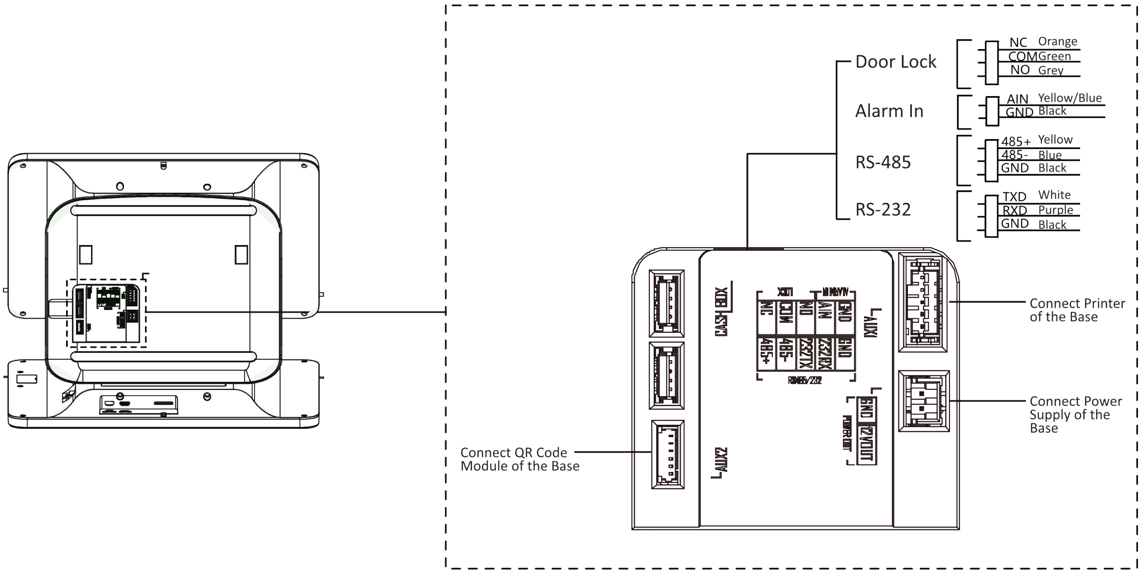


Figure 3-1 Device Wiring

Note

Do not wire the device to the electric supply directly.

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.

Caution

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

After activation, you should follow the wizard for a quick start.

4.2 Activate via Web Browser

You can activate the device via the web browser.

Steps

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

   Note

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

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

⚠ **Caution**

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

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

4.3 Activate via SADP

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

Before You Start

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

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

Steps

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

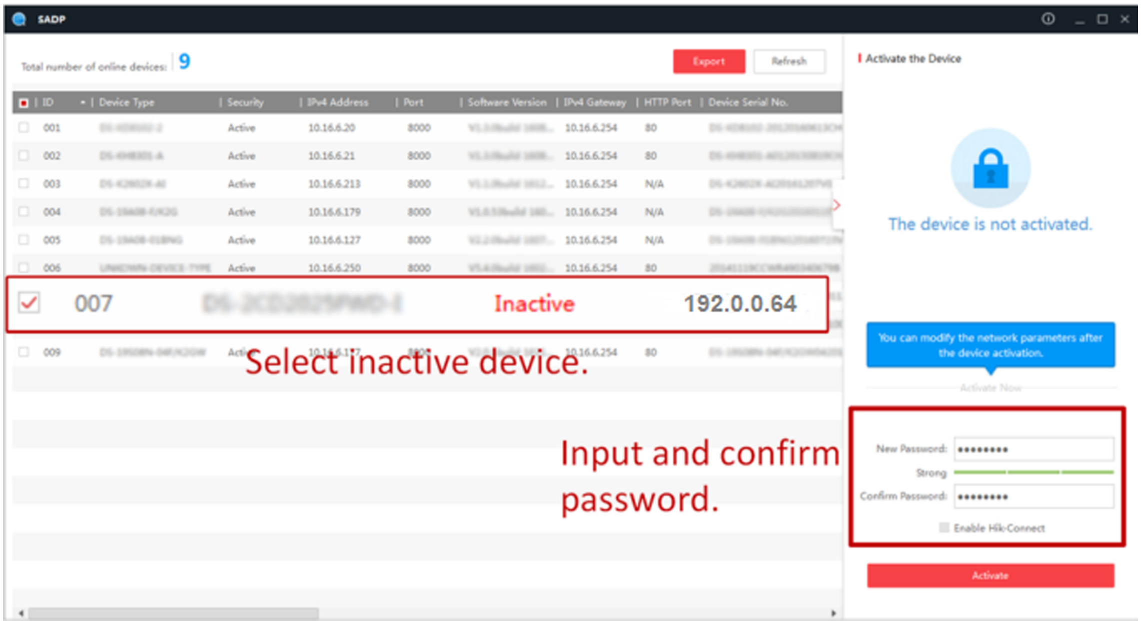
⚠ **Caution**

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

Note

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

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



SADP

Total number of online devices: 9

ID	Device Type	Security	IPv4 Address	Port	Software Version	IPv4 Gateway	HTTP Port	Device Serial No.
□ 001	[illegible]	Active	10.16.6.20	8000	[illegible]	10.16.6.254	80	[illegible]
□ 002	[illegible]	Active	10.16.6.21	8000	[illegible]	10.16.6.254	80	[illegible]
□ 003	[illegible]	Active	10.16.6.213	8000	[illegible]	10.16.6.254	N/A	[illegible]
□ 004	[illegible]	Active	10.16.6.179	8000	[illegible]	10.16.6.254	N/A	[illegible]
□ 005	[illegible]	Active	10.16.6.127	8000	[illegible]	10.16.6.254	N/A	[illegible]
□ 006	UNKOWN-DEVICE-TYPE	Active	10.16.6.250	8000	[illegible]	10.16.6.254	80	[illegible]
☑ 007	[illegible]	Inactive	192.0.0.64					
□ 009	[illegible]	Active	10.16.6.177	8000	[illegible]	10.16.6.254	80	[illegible]

Select inactive device.

Input and confirm password.

Activate the Device

The device is not activated.

You can modify the network parameters after the device activation.

New Password: ••••••••

Strong

Confirm Password: ••••••••

□ Enable Hik-Connect

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

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

4.4 Activate Device via iVMS-4200 Client Software

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

Steps

Note

This function should be supported by the device.

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

   The searched online devices are displayed in the list.
4. Check the device status (shown on **Security Level** column) and select an inactive device.

5. Click **Activate** to open the Activation dialog.
6. Create a password in the password field, and confirm the password.

⚠ **Caution**

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

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

ℹ **Note**

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

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

Chapter 5 Quick Operation

5.1 Select Language

You can select a language for the device system.

After the device activation, you can select a language for the device system.
By default, the system language is English.

Note

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

5.2 Set Password Change Type

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

Change Password via Email Address

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

Change via Security Questions

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

Note

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

5.3 Set Time Zone

You can set a time zone for the device system.

Steps

1. Select a time zone according to your actual needs.

   Note

   The time zone will affect the device time.

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

5.4 Set Network Parameters

You can set the network for the device.

Steps

1. Tap **Wired Network** or **Wireless** for your actual needs.
2. Tap **Next**.
3. **Optional:** Tap **Skip** to skip network settings.

5.5 Privacy Settings

Select parameters according to your actual needs.

Select All

If you enable this function, **Upload Picture When Authenticating** and **Save Picture When Authenticating** will be enabled automatically.

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

Upload the pictures captured when authenticating to the platform automatically.

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

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

Chapter 6 Basic Operation

6.1 Visitor Check In

6.1.1 Reserved Visitor Check In

Visitors can make appointments on the platform in advance and check in by phone number or the visitor code generated for successful reservation.

Before You Start

Fill in the visitor information on the platform in advance.

Steps

1. Tap on the right side of the home page to enter the visitor code or the last 4 digits of the visitor's phone number.
2. Present the card on the card presenting area.

   When authentication is completed, you will enter the visitor check-in information page.
3. **Optional:** If authentication fails, tap ⇦ to retry authentication, or tap 📷 to capture face picture.
4. Fill in the rest of the visitor information.

   Note

   Go to ***Visitor Information Settings*** and set the visitor information to be filled in.
5. Click **Check In** on the visitor check-in information page.

What to do next

Print visitor receipt and visitors can scan the QR code on the receipt to check out.

6.1.2 Non-Reserved Visitor Check In

Check-in for unreserved visitors.

Before You Start

Complete the basic settings and visitor parameter settings. Refer to ***Set System Parameters*** , and ***Visitor Information Settings*** for details.

Steps

1. Enroll visitor information.
   1) Tap **Unreserved Check In** in the lower right corner of the home page to enter the visitor check-in page.
   2) Present the card on the card presenting area for authentication.

      When authentication is completed, you will enter the visitor check-in information page.

Note

If authentication fails, tap ← to retry authentication, or tap 📷 to capture face picture.

3) Add face picture according to the instruction on the visitor screen.

Note

- Refer to ***Set System Parameters*** for details.
- The page and instructions are based on dual-screen devices and are referable for single-screen devices.
- Go to ***Visitor Information Settings*** and set the visitor information to be displayed.

4) Fill in the visitor information.

Note

Go to ***Visitor Information Settings*** and set the visitor information to be filled in.

2. Tap **Check In** to check in the visitor.

What to do next

Print visitor receipt and visitors can scan the QR code on the receipt to check out.

6.1.3 Offline Check In

Check-in for visitors when the device is unconnected to network.

Before You Start

Complete the basic settings and visitor parameter settings. Refer to ***Set System Parameters*** and ***Visitor Information Settings*** for details.

Steps

1. Enroll visitor information.

1) Tap **Offline Check In** in the right corner of the home page to enter the visitor check-in page.

2) Add face picture according to the instruction on the visitor screen.

Note

- Refer to ***Set System Parameters*** for details.
- The page and instructions are based on dual-screen devices and are referable for single-screen devices.
- Go to ***Visitor Information Settings*** and set the visitor information to be displayed.

3) Fill in the visitor information.

Note

Go to ***Visitor Information Settings*** and set the visitor information to be filled in.

2. Tap **Check In** to check in the visitor.

What to do next

Print visitor receipt and visitors can scan the QR code on the receipt to check out.

6.2 Visitor Check Out

6.2.1 Check Out via QR Code

Scan scan the QR code on the receipt to check out.

Steps

1. Scan the QR code on the visitor receipt.

   Note

   Visitors should scan the QR code on the receipt. Refer to ***Printing Receipt Settings*** for receipt content details. Refer to ***Visitor Information Settings*** for receipt print steps.

   The check-out window will pop up on the operator screen.
2. Tap **Check Out**.

6.2.2 Check Out via Card

Check out via card.

Steps

1. Present the card.

   The check-out window will pop up on the operator screen.
2. Tap **Check Out**.

6.2.3 Check Out via Search Record

You can search and view the visitor record and check out the visitors.

Steps

1. Tap ▤ in the top right corner to enter the visitor record page.
2. **Optional:** Filter visitors by conditions.
3. Tap on the selected visitor to enter the detailed information page.
4. Tap **Check Out**.

6.2.4 Auto Check Out

System will check out all visitors at 24 o'clock every day.

6.3 Visitor System

6.3.1 View and Search Visitor Information

After the visitor is checked in, the administrator can view and search the visitor information.

View Visitor Information

Tap **Today's Visitor**, **Leave**, or **Not Checked Out** to view the visitor number of today's, already leaves, and not checked out. By default, it displays today's visitor information.
Tap at the upper right corner of the page to enter the visitor records page. Select **Name**, **ID No.**, or **Last Digits of Phone Number**, enter key words in the search box, the list below will display the search result.

Note

The phone last No. is the last 4 digits of the phone No.

Or tap at the upper right corner of the page. Filter the records according to the **Visitor Status**, **Visiting Purpose**, or **Visiting Time**. Tap ✓ to start filtering.

6.3.2 Login

Steps

1. Tap ⚙ in the top right corner of the home page. The login window will pop up.
2. Enter the activation password.
3. **Optional:** Tap to display the password.
4. Tap **OK** to enter the settings page.

   Note

   5 failed attempts with incorrect password will lock the device for 30 minutes.

6.3.3 System Settings

Set Network Parameters

You can set wired network or Wi-Fi for the device.

Steps

1. Tap ⚙ in the top right corner of the home page and enter admin password. Tap **Communication → Wired Network** or **Communication → Wi-Fi** according to your actual needs.
2. Set network.

Wired Network

Note

Make sure the device has connected to a network.

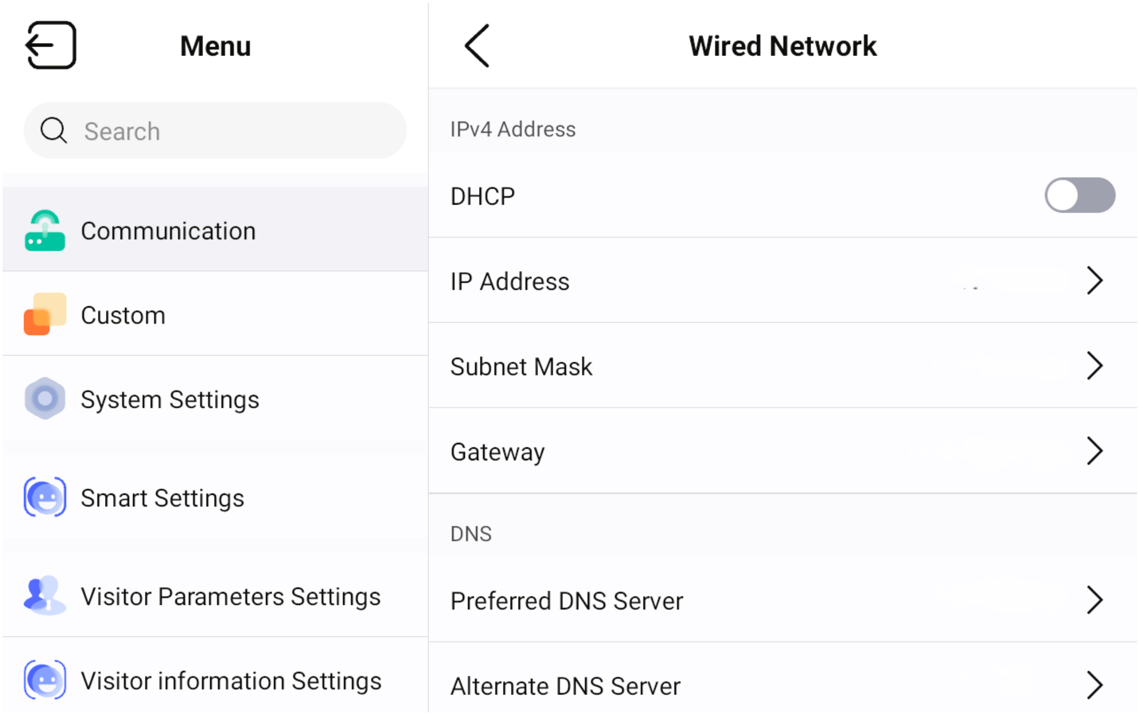


Figure 6-1 Wired Network

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 default gateway, DNS1 and DNS2.

Tap ☑ to save the settings.

Wi-Fi

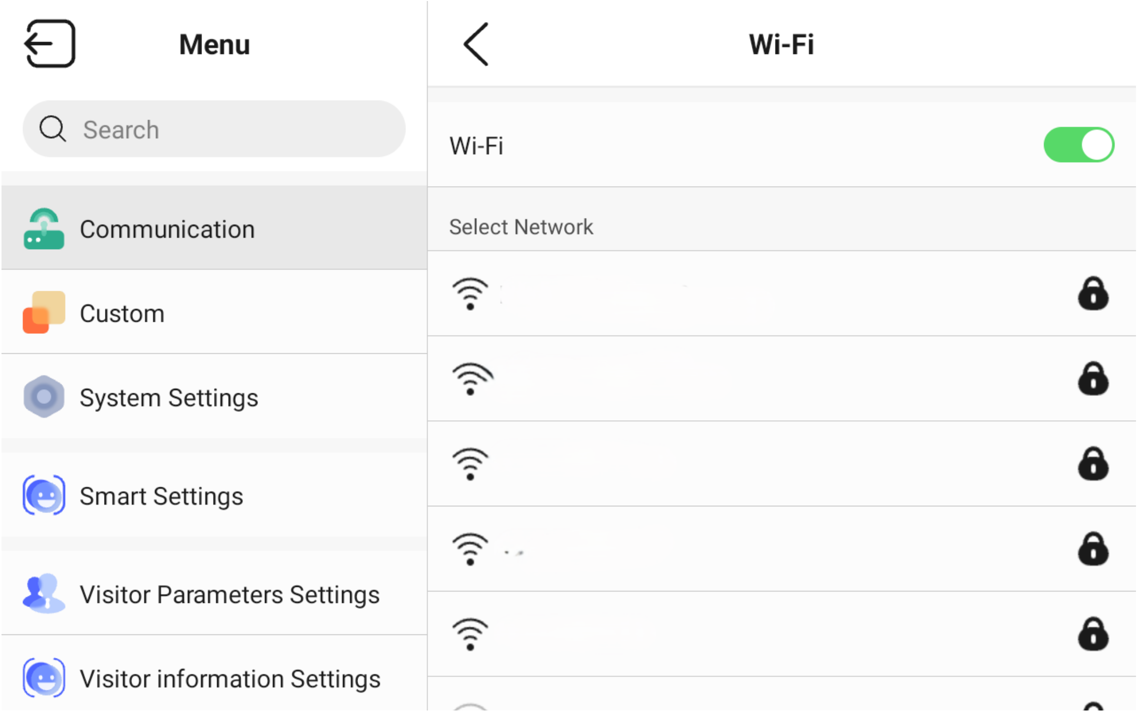


Figure 6-2 Wi-Fi

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

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

Set ISUP Parameters

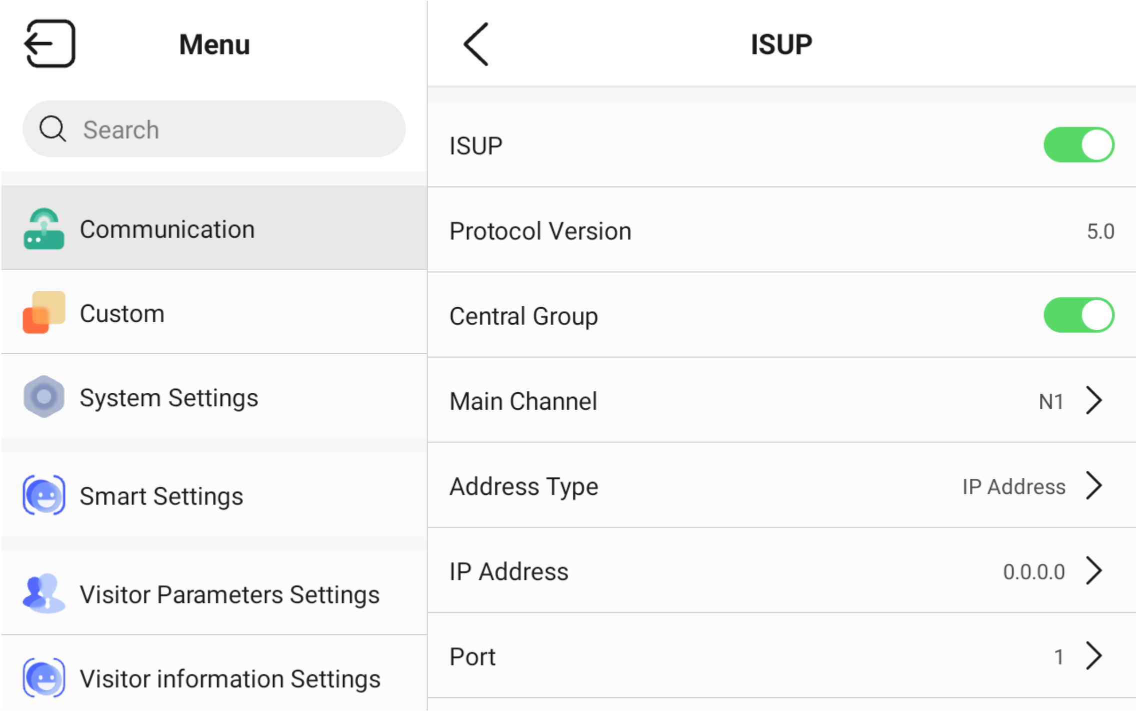
Set ISUP parameters and the device can upload data via ISUP protocol.

Before You Start

Make sure your device has connect to a network.

Steps

1. Tap ⚙ in the top right corner of the home page and enter admin password. Tap **Communication** → **ISUP** on the Home page to enter the settings page.



ISUP

Protocol Version 5.0

Central Group

Main Channel N1

Address Type IP Address

IP Address 0.0.0.0

Port 1

Figure 6-3 ISUP Settings

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

   ISUP Version

   Set the ISUP version according to your actual needs.

   Central Group

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

   Main Channel

   Support N1 or None.

   Address Type

   Select an address type according to your actual needs.

   IP Address

   Set the ISUP server's IP address.

   Port No.

   Set the ISUP server's port No.

   Note

   Port No. Range: 0 to 65535.

   Device ID

   Set device serial no.

Password

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

Note

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

Platform Access

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

Before You Start

Make sure your device has connected to a network.

Steps

1. Tap ⚙ in the top right corner of the home page and enter admin password. Tap **Communication → Hik-Connect** on the Home page to enter the settings page.
2. Enable **Hik-Connect**
3. You can view the connection status.
4. Enter **Server IP**.
5. Create the **Verification Code**, and you need to enter the verification code when you manage the devices via **Hik-Connect**.

Switch Mode

You can select switch mode.

Steps

1. Tap ⚙ in the top right corner of the home page and enter admin password. Tap **Custom → Switch Mode** .
2. You can select **Normal Mode** or **Advert. Mode**.

   Normal Mode

   Display welcome interface with time information.

   Advert. Mode

   Play media information applied by Web.

Set System Parameters

You can set system parameters for the device.

Tap ⚙ in the top right corner of the home page and enter admin password. Tap **System Settings**.

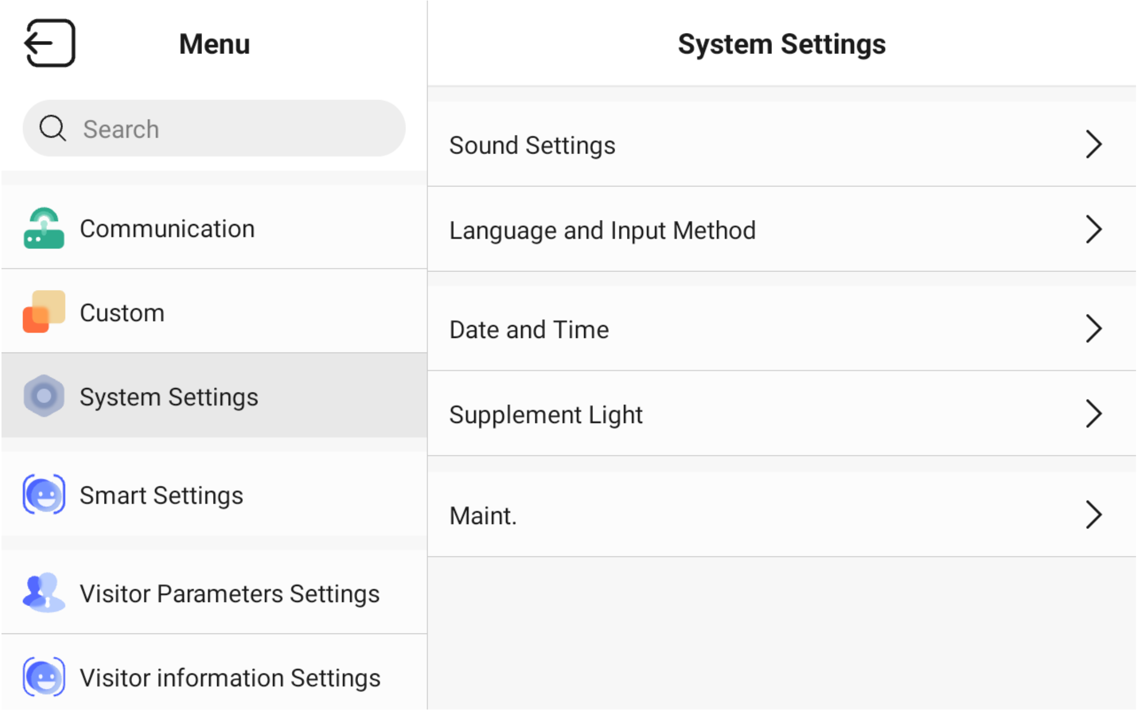


Figure 6-4 System Parameters

Table 6-1 System Parameters

Parameter	Description
Sound Settings	You can adjust the voice prompt and keypad sound ranging from 0 to 10. The larger the value, the louder the volume.
Language and Input Method	Set the device language.
Date and Time	Set the device time, date and time zone.
Supplement Light	You can enable the white light at bottom. The brightness ranges from 0 to 100.

System Maintenance

You can view the device system information, restore the system to factory settings or default settings, reboot the device, exit the system and start wizard.

Tap ⚙ in the top right corner of the home page and enter admin password. Tap **System Settings → Maint.**

System Information

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

Note

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

User Manual

You can scan the QR code to get the user manual for reference.

Device Upgrade

Online Update

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

Update via USB

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

Restore to Default Settings

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

Restore to Factory Settings

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

Configuration Wizard

You can reset the configuration wizard.

Reboot

Reboot the device.

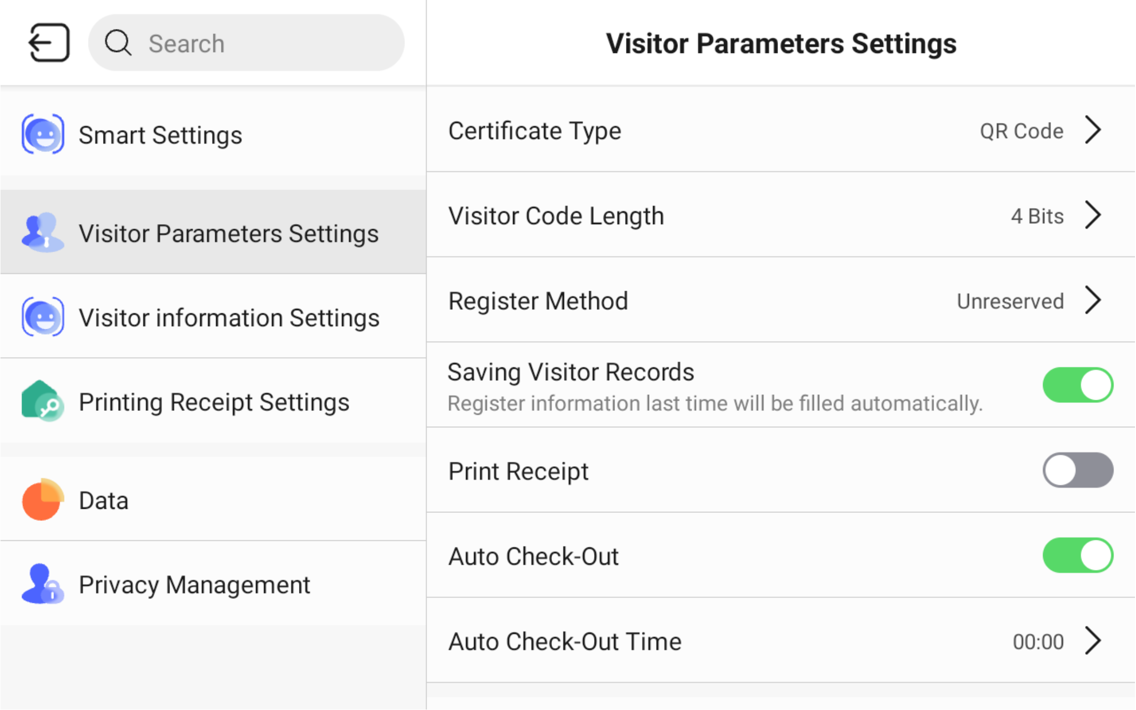
Exit

Exit the page.

Set Visitor Parameters

You can enable the functions for visitor check-in.

Tap ⚙ in the top right corner of the home page and enter admin password. Tap **Visitor Parameters Settings**.



Visitor Parameters Settings

Certificate Type: QR Code

Visitor Code Length: 4 Bits

Register Method: Unreserved

Saving Visitor Records: On
Register information last time will be filled automatically.

Print Receipt: Off

Auto Check-Out: On

Auto Check-Out Time: 00:00

Search
Smart Settings
Visitor Parameters Settings
Visitor information Settings
Printing Receipt Settings
Data
Privacy Management

Figure 6-5 Visitor Parameters Settings

Tap to enable the functions.

Credential Type

You can select QR code, card, QR code & card or none for credential.

Visitor Code Length

You can set the visitor code length of 4 or 6 digits.

Registered Method

You can set registered method.

Saving Visitor Records

When the function is enabled, visitor information will be recorded for the first-time visit. When revisits, the visitor only need to present his/her credential for the device to read and the information will be displayed on screen.

Print Receipt

When the function is enabled, you can print visitor receipt.

Auto Check Out

When the function is enabled, system will check out all visitors at 24 o'clock every day.

Device OCR Recognition

When the function is enabled, the device can recognize OCR.

Person and ID Comparison

When the function is enabled, the device will be able to process person and ID comparison.

Synchronize Visitor Data

When the function is enabled, you can synchronize visitor data and set sync. time interval.

Set Face Parameters

You can customize the face parameters to improve the face recognition performance.

Tap ⚙ in the top right corner of the home page and enter admin password. Tap **Smart Settings**.

Face Anti-spoofing

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

Face Liveness Level

You can select face liveness level. The higher the level, the fault acceptance rate will be lower and the false rejection rate will be higher.

Recognition Distance

Set the valid distance between the user and the camera when authenticating.

Face 1:1 Security Level

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

Face Picture Quality Grade Threshold

You can set face picture quality grade threshold.

Eco Mode Settings

You can enable ECO mode, change threshold, and set 1:1 threshold.

Import Data

Steps

1. Plug a USB flash drive in the device.
2. Tap ⚙ in the top right corner of the home page and enter admin password. Tap **Data → Import Data** .
3. Select data type.
4. Enter the created password when you exported the data. If you do not create a password when you exported the data, leave a blank in the input box and tap **OK** immediately.

Note

- If you want to transfer all person 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 person data before importing the profile photo.

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

Export Data

You can export captured picture or visitor records to your USB flash drive.

Before You Start
Plug in the USB flash drive.

Note

The supported USB flash drive format is FAT32. Make sure the spare space is larger then 512 M.

Steps

1. Tap ⚙ in the top right corner of the home page and enter admin password. Tap **Data → Export Data** .
2. Tap **Export Captured Picture** or **Export Visitor Records** to export the picture captured or visitor information recorded on the device to your USB flash drive.

Visitor Information Settings

Set the items that need to be filled and whether they are required fields when checked in.

Steps

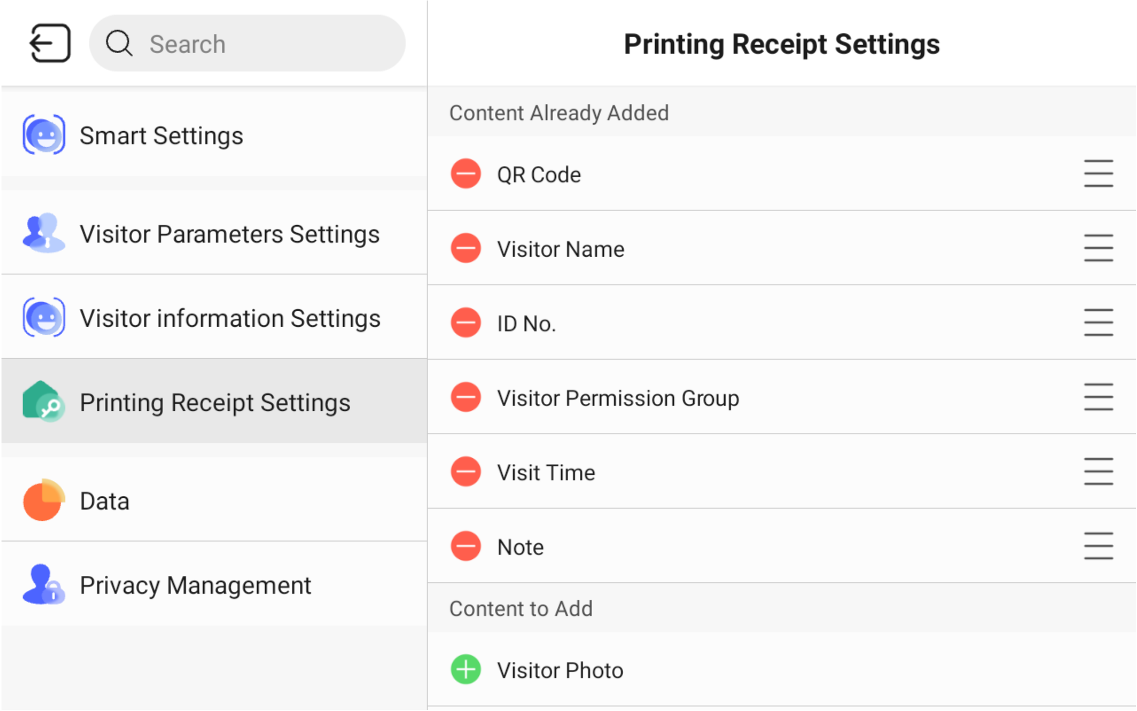
1. Tap ⚙ in the top right corner of the home page and enter admin password. Tap **Visitor Information Settings**.
2. Set the target items, including basic information, more information, host and other information items, as **Required**, **Not Required** or **Hide**.

Printing Receipt Settings

Set the printing contents on the receipt.

Steps

1. Tap ⚙ in the top right corner of the home page and enter admin password. Tap **Printing Receipt Settings**.



Printing Receipt Settings

Content Already Added

- QR Code
- Visitor Name
- ID No.
- Visitor Permission Group
- Visit Time
- Note

Content to Add

- Visitor Photo

Search
Smart Settings
Visitor Parameters Settings
Visitor information Settings
Printing Receipt Settings
Data
Privacy Management

Figure 6-6 Printing Receipt Settings

2. You can tap **+** to add the content and tap **-** to delete the content.

Set Privacy Parameters via Device

Set the picture uploading parameters.

Note

Different device models support different functions. Refers to actual model.

Tap ⚙ in the top right corner of the home page and enter admin password. Tap **Privacy Management → Privacy** .

Picture Uploading and Storage

Set picture uploading and storage parameters.

Save Pic When Auth.

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

Upload Pic. When Auth.

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

Change Device Password

You can change the device password by entering the old password.

Steps

1. Tap ⚙ in the top right corner of the home page and enter admin password. Tap **Privacy Management**.
2. Tap **Change Password**.
3. Enter the device old password.

   Note

   If you forget your password, you can tap **Forgot Password** and change the password. For details, see .
4. Enter new password and confirm the password.

   Caution

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

Chapter 7 Operation via Web Browser

7.1 Login

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

Note

Make sure the device is activated. For detailed information about activation, see ***Activation*** .

Login via Web Browser

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

Login via Remote Configuration of Client Software

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

7.2 Forget Password

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

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

Select **Verification Mode**.

Security Question Verification

Answer the security questions.

E-mail Verification

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

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

7.3 Download Web Plug-In

Both non-Plug-in live view and live view after downing plug-in are available. For better live view, downloading plug-in for live view is recommended.

Click ⚙ → **Download Web Pug-In** to download the pulg-in to the local.

7.4 Help

7.4.1 Open Source Software Licenses

You can view open source software licenses.

Click ⓘ → **Open Source Software Statement** on the upper-right corner to view the licenses.

7.4.2 View Online Help Document

You can view the help document for Web configuration.

Click ⓘ → **Online Document** on the upper right of the Web page to view the document.

7.5 Logout

Log out the account.

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

7.6 Quick Operation via Web Browser

7.6.1 Change Password

You can change the device password.

Click ◅ on the top right of the web page to enter the **Change Password** page. You can set security questions from the drop-down list and fill in the answers. Or you can set an E-mail address to receive verification code for password recovery.

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

7.6.2 Select Language

You can select a language for the device system.

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

By default, the system language is English.

Note

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

7.6.3 Time Settings

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

Time Zone

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

Time Sync.

NTP

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

Manual

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

Server Address/NTP Port/Interval

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

DST

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

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

7.6.4 Environment Settings

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

Steps

1. Click in the top right of the web page to enter the wizard page. After setting device language and time, you can click **Next** to enter the **Environment Settings** page.
2. Select **Indoor** or **Other**.

Note

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

Click **Next** to save the settings and go to the next paramater. Or click **Skip** to skip environment settings.

7.6.5 Privacy Settings

Set the picture uploading and storage parameters.

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

Picture Uploading and Storage

Save Picture When Authenticating

Save picture when authenticating automatically.

Save Registered Picture

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

7.7 Person Management

Click **Add** to add the person's information, including the basic information, certificate, authentication and settings.

Add Basic Information

Click **Person Management → Add** to enter the Add Person page.
Add the person's basic information, including the employee ID, the person's name, phone No., organization, gender, and person type.
Click **Save** to save the settings.

Set Permission Time

Click **Person Management → Add** to enter the Add Person page.
Enable **Long-Term Effective User**, or set **Long-Term Effective User**, and the person can only has the permission within the configured time period according to your actual needs.
Set the door permission.
Click **Save** to save the settings.

Authentication Settings

Click **Person Management → Add** to enter the Add Person page.
Set the authentication type.
Click **Save** to save the settings.

Add Card

Click **Person Management → Add** to enter the Add Person page.
Click **Add Card**, enter the **Card No.** and select the **Property**, and click **OK** to add the card.
Click **Save** to save the settings.

Add Face Picture

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

Click **+ Upload** to upload a face picture from the local PC.

Note

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

Click **Save** to save the settings.

Delete Person

On the person management page, check the person need to delete and click **Delete**.
Click **Clear All** to clear all person.

Edit Person

On the person management page, check the person need to edit. Click ✎ to edit the person information.

Filter

On the person management page, enter **Employee ID / Name / Card No.**. Select **Credential Status**, and click **Filter** to filter the person. Click **Reset** to clear all conditions.

7.8 Visitor Management

7.8.1 Overview

You can click home page icon and view the person information, network status, basic information, and device capacity.

Function Descriptions:

Person Information

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

Network Status

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

Basic Information

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

Device Capacity

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

7.8.2 Search Event

Click **Visitor → 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.

7.8.3 Set Visitor Basic Parameters

Set visitor basic parameters.

Click **Visitor → Basic Parameter** .

Configure parameters and click **Save**.

Visitor Reservation

Enable the function to allow visitor reservation via platform.

Visitor Code Length

Choose 4 or 6 character digits according to actual needs.

Note

Visitors can fill out the information on APP to generate an authorization code and make an appointment.

Register Method

You can select register method.

Auto Check-out/Auto Check-out Time

The system will auto check out all visitors at set auto check-out time when the function is enabled.

Manually Enter Visitor Information

You can enter visitor information manually when the function is enabled.

Saving Visitor Records

When saving visitor records is enabled, the visitor's information will be recorded. For revisits, the system will read from the card for information to displayed on the screen.

Authentication Mode

You can choose **Comparison between Credential Photo and Captured Face** or **Authentication Not Needed** from the drop-down list according to actual need.

Allow to Skip Person and ID Comparison by Manual Settings

You can check **Disable**, or **Skip Directly** to manage person and ID comparison.

Print Visitor Receipt with ID Photo

When the function is enabled, the system will use the credential photo as the profile image on the visitor receipt. If the function is disabled, the captured image will be used.

Credential Type

Other than card comparison, you can choose **QR Code**, **Card**, **QR Code & Card** or **None** for visitor check-in.

Auto Sync. Visitor Information

When the function is enabled, the visitor information of different devices added to the same APP account will synchronize automatically.

ID Card Comparison Threshold

Drag the block or enter the value to adjust the card comparison threshold. The higher the value is, the more unlikely for device to mismatch.

Auto-Sync Interval

Drag the block or enter an value to adjust auto-sync interval ranging from 5 to 60 minutes. The visitor information will be synchronized at the set intervals.

7.8.4 Authentication Settings

View Terminal Type and Model via PC Web

You can view terminal type and model.

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

View **Terminal Type** and **Terminal Model**.

Enable Authentication Device via PC Web

After enabling, the authentication terminal can be used for card swiping.

Steps

1. Click **Visitor → Parameter Settings → Authentication Settings** to enter the settings page.
2. Enable **Authentication Device**. After enabling, the terminal can be used for card swiping normally.
3. Click **Save**.

Set Recognition Interval via PC Web

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

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

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

Note

Please enter a number between 1 and 10.

Enable Alarm of Max. Failed Attempts via PC Web

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

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

When you select the terminal as main or sub card reader, slide to enable **Alarm of Max. Failed Attempts**, and set **Max. Authentication Failed Attempts**.

Click **Save**.

Enable/Disable Tampering Detection via PC Web

You can enable tampering detection, the device will automatically generate tampering events when the card reader is removed or taken away.

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

Enable or disable **Tampering Detection** according to your actual needs. After enabling the function, the device will automatically generate tampering events when the card reader is removed or taken away. If the function is disabled, no alarm events will be generated.

Click **Save**.

Set Authentication Plan

You can set authentication plan.

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

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

Click **Save**.

7.8.5 Set Check In Information

Select items that will be displayed on the visitor check-in page.

Click **Visitor → Visitor Check In Settings** .

Select the visitor information items as display at the **Display** column.

You can enable **Desensitize or Not**.

Click **Save**.

7.8.6 Set Printing Receipt Information

Select items to be printed on the receipt.

Click **Visitor → Printing Receipt Settings** .

Select the information items to be printed at the **Printing Content Settings** column.

Click ↓ to move the item position printed on the receipt.

7.8.7 Set Face Parameters

Enable/Disable Face Anti-spoofing via Web Browser

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

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

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

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

Set Anti-Spoofing Detection Level via PC Web

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

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

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

The higher the level, the lower the fake recognition rate and the higher the rejection rate.

Set Recognition Distance via PC Web

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

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

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

Set Application Mode and Installation Angle

You can set the application mode.

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

Select the **Application Mode**, and click **Save**.

Set Pitch Angle via PC Web

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

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

Note

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

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

Set Yaw Angle via PC Web

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

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

Note

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

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

Set Face Picture Quality Grade for Applying via PC Web

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

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

Note

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

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

Click **Save**.

Set 1:1 Face Grade Threshold via PC Web

Set 1:1 face grade threshold.

Go to **Visitor → Parameters Settings → Smart** .

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

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

Set Face 1:1 Matching Threshold via PC Web

Set face 1:1 matching threshold.

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

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

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

Set 1:N Matching Threshold via PC Web

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

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

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

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

Set Face Recognition Area via Web Browser

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

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

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

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

Click **Save**.

Click 📷 , ◉ , or ⛶ to capture, record, or go to full screen view.

Enable/Disable ECO Mode via PC Web

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

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

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

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

1:1 Security Level

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

Click **Save**.

Enable/Disable Face with Mask Detection via PC Web

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

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

Face without Mask Strategy

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

Reminder of Wearing Face Mask

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

Must Wear Face Mask

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

Face with Mask 1:1 Match Threshold (ECO)

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

Click **Save**.

7.8.8 Card Settings

Enable/Disable NFC Protection via PC Web

After enabling, the device can read NFC card.

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

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

Enable/Disable M1 Card via Web Client

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

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

Click to **Enable M1 Card**.

M1 Card Encryption

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

Sector

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

Note

You are advised to encrypt sector 13.

Click **Save**.

7.8.9 Privacy Settings

Set Event Storage Type via PC Web Browser

You can configure the event storage type.

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

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

Delete Old Events Periodically

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

Delete Old Events by Specified Time

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

Overwriting

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

Click **Save**.

Set Authentication Result via PC Web

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

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

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

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

Click **Save**.

Configure Picture Uploading and Storage via PC Web

You can set picture uploading and storage parameters.

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

Save Picture When Auth.

Save picture when authenticating automatically.

Save Registered Picture

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

Click **Save**.

Clear Device Pictures via PC Web

You can clear all registered, or captured face pictures.

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

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

7.8.10 Set Working Mode via PC Web

You can set the terminal parameters of the device.

Note

Only some models support this function, please refer to the specific device.

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

Working Mode

You can set the working mode as access control mode or permission free mode.

Access Control Mode

The access control mode is the device normal mode. You should authenticate your credential for accessing.

OCR

You can check OCR Identifier type according to your needs.

7.9 System Configuration

7.9.1 View Device Information via PC Web

View the device name, language, model, serial No., version, available cameras, and device capacity, etc.

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

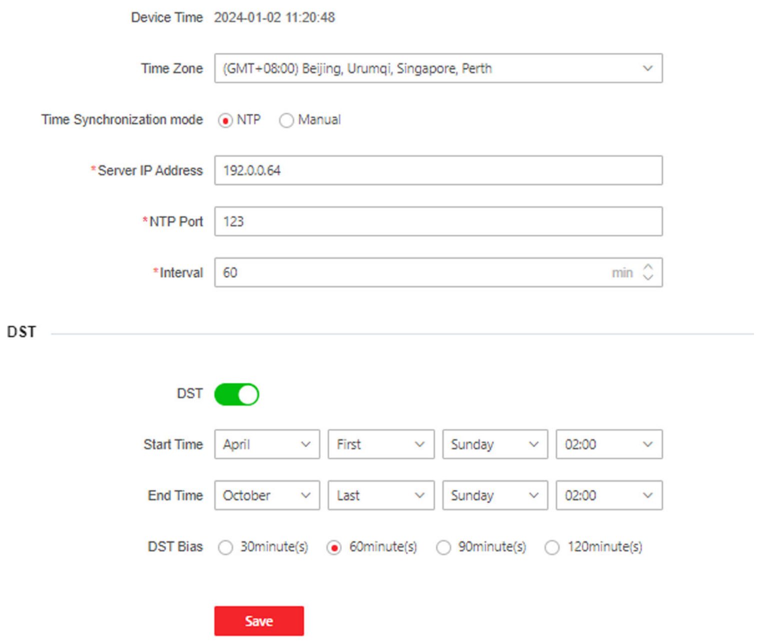
You can view the device name, language, model, serial No., version, available cameras, and device capacity, etc.

Click **Upgrade** in the Firmware Version, you can go to the upgrade page to upgrade the device.

7.9.2 Set Time

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

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



Device Time 2024-01-02 11:20:48

Time Zone (GMT+08:00) Beijing, Urumqi, Singapore, Perth

Time Synchronization mode ● NTP ○ Manual

*Server IP Address 192.0.0.64

*NTP Port 123

*Interval 60 min

DST

DST ●

Start Time April First Sunday 02:00

End Time October Last Sunday 02:00

DST Bias ○ 30minute(s) ● 60minute(s) ○ 90minute(s) ○ 120minute(s)

Figure 7-1 Time Settings

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

Time Zone

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

Time Sync.

NTP

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

Manual

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

Server Address Type/Server Address/NTP Port/Interval

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

7.9.3 Change Administrator's Password

Steps

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

⚠ **Caution**

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

7.9.4 Account Security Settings via PC Web

You can change the security questions and answers, or the email address for the device. After change the settings, once you forgot the device password, you should answer the new questions or use the new email address to reset the device password.

Steps

1. Click **System and Maintenance → System Configuration → System → User Management → User Management → Account Security Settings** .
2. Change the security questions or email address according your actual needs.
3. Enter the device password and click **OK** to confirm changing.

7.9.5 View Device Arming/Disarming Information via PC Web

View device arming type and arming IP address.

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

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

7.9.6 Network Settings

Set Basic Network Parameters via PC Web

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

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

NIC Type

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

DHCP

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

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

DNS Server

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

Set Wi-Fi Parameters

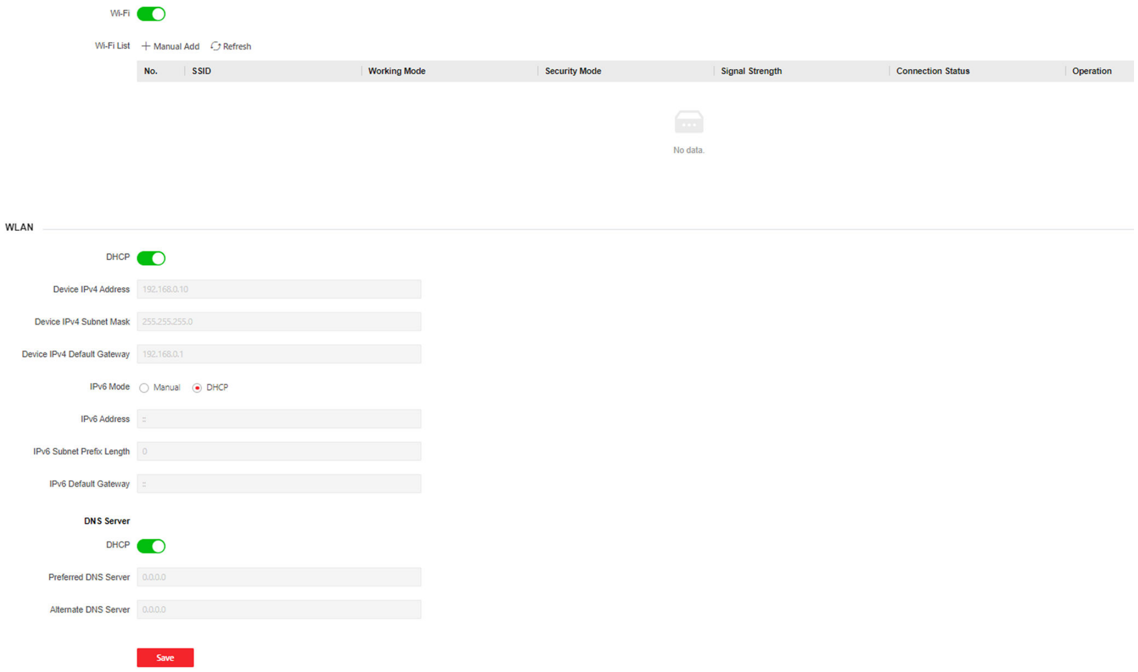
Set the Wi-Fi parameters for device wireless connection.

Steps

Note

The function should be supported by the device.

1. Click **System and Maintenance → System Configuration → Network → Network Settings → Wi-Fi** .



Wi-Fi: ON

Wi-Fi List

No.	SSID	Working Mode	Security Mode	Signal Strength	Connection Status	Operation

No data.

WLAN

DHCP: ON

Device IPv4 Address: 192.168.0.10

Device IPv4 Subnet Mask: 255.255.255.0

Device IPv4 Default Gateway: 192.168.0.1

IPv6 Mode: ○ Manual ● DHCP

IPv6 Address: ::

IPv6 Subnet Prefix Length: 0

IPv6 Default Gateway: ::

DNS Server

DHCP: ON

Preferred DNS Server: 0.0.0.0

Alternate DNS Server: 0.0.0.0

Figure 7-2 Wi-Fi Settings Page

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

Set Port via PC Web

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

Enable/Disable HTTP

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

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

Click**Save** after parameters are configured.

HTTP Port

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

HTTPS Port

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

HTTP Listening

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

View RTSP Port via PC Web

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

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

View the Port.

Enable SDK Service

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

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

Enter **Server Port**.

Click **Save** to enable the settings.

Set ISUP Parameters via PC Web

Set the ISUP parameters for accessing device via ISUP protocol.

Steps

Note

The function should be supported by the device.

1. Click **System and Maintenance → System Configuration → Network → Device Access → ISUP** .
2. Check **Enable**.
3. Set the ISUP version, server address, device ID, and the ISUP status.

Note

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

4. Set the ISUP listening parameters, including ISUP alarm center IP address/domain name, ISUP alarm center URL, and ISUP alarm center port.
5. Click **Save**.

Platform Access via PC Web

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

Steps

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

Note

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

2. Check **Enable** to enable the function.
3. **Optional:** Check the checkbox of **Custom**, and you can set the server address by yourself.
4. Enter the verification code.
5. Click **View** to view device QR code. Scan the QR code to bind the account.

Note

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

6. Click **Save** to enable the settings.

7.9.7 Set Video and Audio Parameters via PC Web

Configure Video Parameters via Web Browser

You can set quality, resolution and other parameters of device camera.

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

Set camera name, stream type, video type, resolution, bit rate type, video quality, frame rate, Max. bitrate, video encoding and I frame interval.

Click **Save**.

Configure Audio Parameters via PC Web

You can set device volume.

Go to **System and Maintenance → System Configuration → Video/Audio → Audio**.

Slide to enable **Voice Prompt**, and set **Output Volume**.

Tap **Save**.

7.9.8 Image Parameter Settings

Set Brightness/Contrast/Saturation/Sharpness via PC Web

You can set picture information such as brightness, contrast, saturation and sharpness of live view page.

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

Image Adjustment

Drag the block or enter numbers to set brightness, contrast, saturation and sharpness.

Click **Restore Default Settings** to restore the to the default.

Set LED Light via PC Web

You can adjust the brightness of the supplement light.

Steps

1. Click **System and Maintenance → System Configuration → Image → Display Settings** to enter the settings page.
2. Set the type, mode and brightness of the supplement light.
3. **Optional:** Click **Restore Default Settings** to restore the to the default.

Set WDR via PC Web

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

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

Click **Restore Default Settings** to restore the to the default.

Set Video Standard via PC Web

You can set the video standard of live view page.

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

Video Adjustment

Set the video frame rate during remote preview. You need to reboot the device to make the new settings effective.

PAL

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

NTSC

30 frames per second. Suitable for the USA, Canada, Japan, Taiwan (China), Korea, the Philippines, etc.

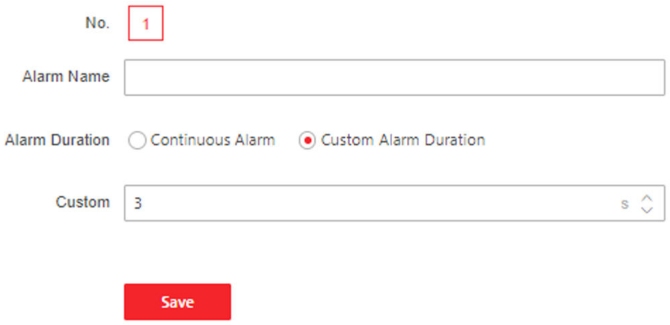
Click **Restore Default Settings** to restore the to the default.

7.9.9 Alarm Settings via PC Web

Set the alarm output parameters.

Steps

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



No. 1

Alarm Name

Alarm Duration ○ Continuous Alarm ● Custom Alarm Duration

Custom 3 s

Figure 7-3 Alarm Settings

Continuous Alarm

When the alarm is triggered, it will alarm continuously.

Custom Alarm Duration

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

7.9.10 Access Configuration

Set RS-485 Parameters via PC Web

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

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

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

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

No.

Set the RS-485 No.

Peripheral Type

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

Note

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

RS-485 Address

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

Note

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

Baud Rate

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

7.10 Preference Settings

7.10.1 Logo Management

Set a logo to show in the top left corner.

Steps

1. Click **System and Maintenance → Preference → Screen Display** .
2. Click + to add a local image.

3. Click **Import** to import the selected logo image.

Note

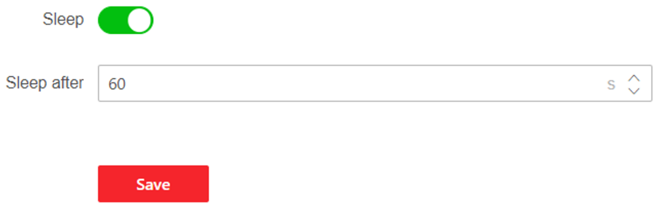
The logo image shall be no larger than 100 kb with a resolution of 400 × 400.

4. **Optional:** Click **Delete** to delete the selected logo image.

7.10.2 Set Sleep Time via PC Web

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

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



Sleep: on

Sleep after: 60 s

Figure 7-4 Sleep Settings

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

Click **Save**.

7.10.3 Customize Theme Mode via PC Web

Customize the theme mode on the authentication page/desk.

Steps

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

   Access Mode

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

   Advertisement

   The ad takes up the full screen of authentication page, and can be played in ad.
3. Click **Save**.

7.10.4 Set Notice Publication via PC Web

You can set the notice publication for the device.

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

Theme Management

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

Note

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

Add Program

You can set the program name and select program type.

Picture

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

Video

If you select Video, you can click **+** to add video.

Text

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

Play Schedule

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

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

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

Slide Show Interval

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

7.11 System and Maintenance

7.11.1 Reboot

You can reboot the device.

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

Click **Restart** to reboot the device.

7.11.2 Upgrade

Upgrade Locally via PC Web

You can upgrade the device locally.

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

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

Online Upgrading via PC Web

You can upgrade the device online.

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

Click**Check for Updates**to check whether there is updated versions.

If the device is connected to the network and added to Hik-Connect App, you can tap **Device Upgrade → Online Upgrade** on device for upgrading when there is an updated version in Hik-Connect App.

7.11.3 Restoration

Restore to Factory Settings via Web Browser

You can restore device to factory settings.

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

Click **Restore All**, all parameters will be restored to the factory settings. You should activate the device before usage.

Restore to Default Settings via PC Web

You can restore device to default settings.

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

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

7.11.4 Export Device Parameters via PC Web

Export device parameters.

Go to **System and Maintenance → Maintenance → Backup and Reset** .

Backup

Click **Export** to export device parameters.

Note

Export device parameters and import those parameters to other devices.

7.11.5 Import Device Parameters via PC Web

Import the configuration parameters.

Go to **System and Maintenance → Maintenance → Backup and Reset** .

Import Config File

Click 🗀 and select a file from local PC. Click **Import**.

7.11.6 Device Debugging

You can set device debugging parameters.

Enable/Disable SSH via Web Browser

You can enable SSH to perform remote debugging.

Click **System and Maintenance → Maintenance → Device Debugging → Log for Debugging**.

Enable SSH

SSH is used for remote debugging. When you don't need to use this service, it's recommended to disable SSH to improve security.

Print Device Log via PC Web

You can print out the device log.

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

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

Capture Network Packet via PC Web

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

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

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

Set ADB Remote Control

You can set ADB remote control.

Steps

1. Go to **System and Maintenance → Maintenance → Device Debugging** .
2. Enable **ADB Remote Control**.

7.11.7 View Log via PC Web

You can search and view the device logs.

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

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

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

7.11.8 Security Management

Set security level when login the PC web.

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

Security Mode

High security level when logging in and verify user information.

Compatible Mode

Compatible with old user verification method.

Click **Save**.

Chapter 8 Other Platforms to Configure

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

iVMS-4200 Client Software

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

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

HikCentral Access Control (HCAC)

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

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

Appendix A. 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.

Appendix B. 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.
ℹ **Note**	Provides additional information to emphasize or supplement important points of the main text.

Appendix C. Tips for Installation Environment

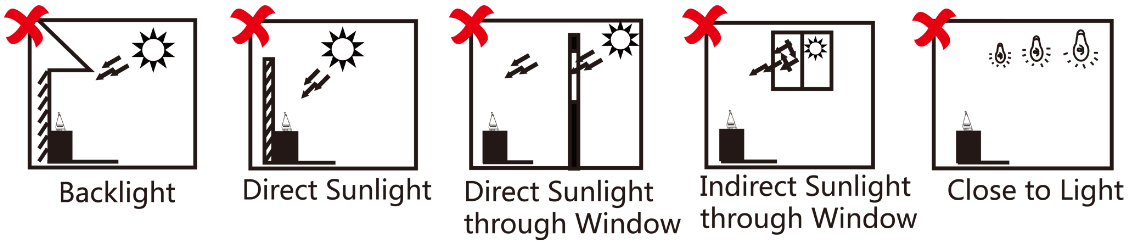
1. Light Source Illumination Reference Value

Candle: 10Lux

Bulb: 100~850Lux

Sunlight: More than 1200Lux

2. Avoid backlight, direct and indirect sunlight


Backlight
Direct Sunlight
Direct Sunlight through Window
Indirect Sunlight through Window
Close to Light

Appendix D. Dimension

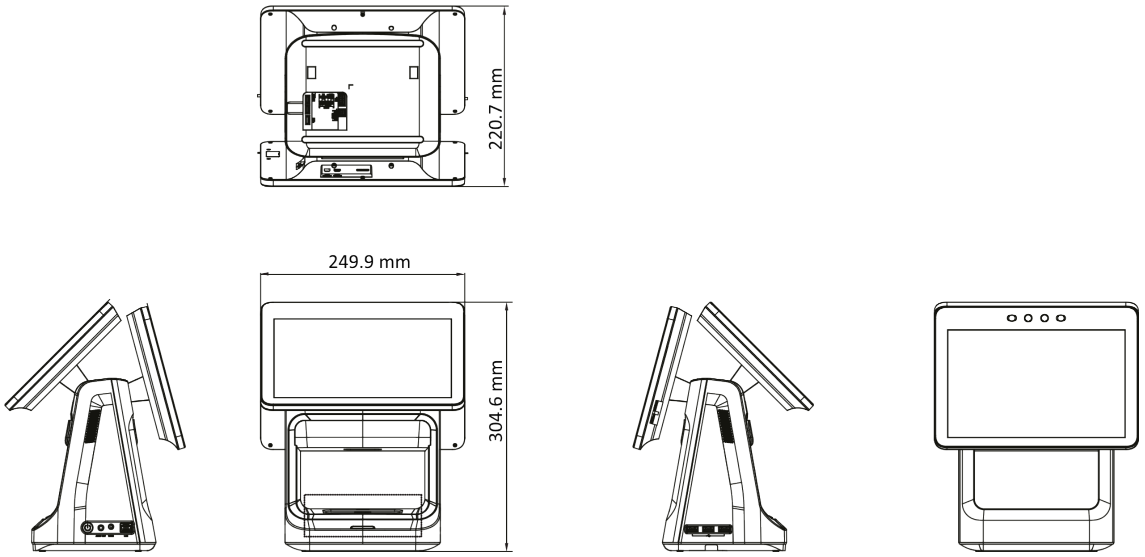


Figure D-1 Dual Small Screens Device

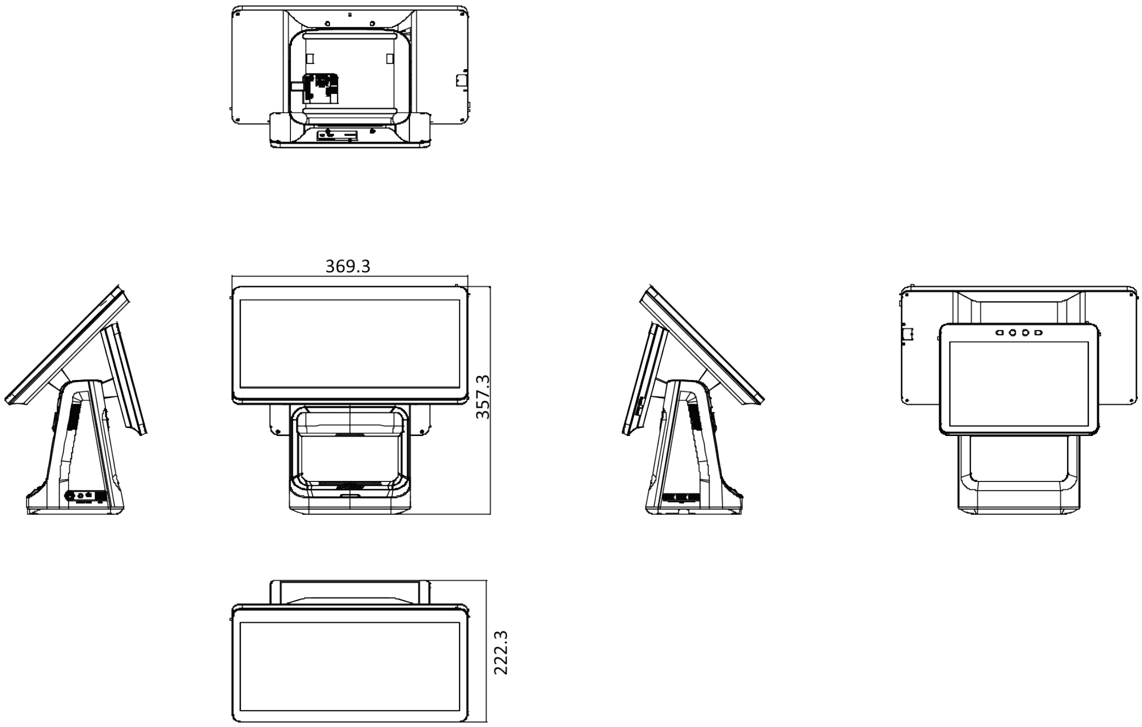


Figure D-2 Large and Small Screens Device

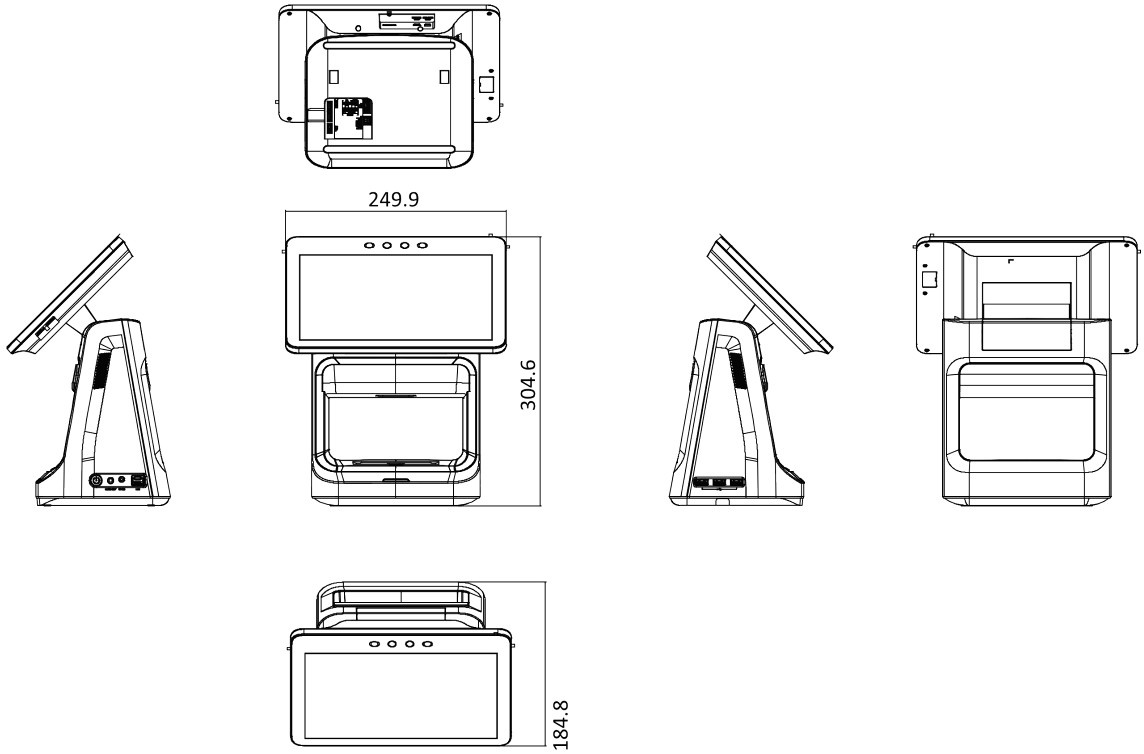


Figure D-3 Single Screen Device

See Far, Go Further