DS-K5032-3XFD Visitor Terminal

User Manual

Legal Information

About this Manual

The Manual includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only. The information contained in the Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of this Manual at the Hikvision website (***https://www.hikvision.com/***).

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

Trademarks

HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.

Other trademarks and logos mentioned are the properties of their respective owners.

Disclaimer

DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.

IN THE EVENT OF ANY CONFLICTS BETWEEN THIS MANUAL AND THE APPLICABLE LAW, THE LATTER PREVAILS.

Data Protection

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

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

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

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.

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.
- This equipment is not suitable for use in locations where children are likely to be present.
- To prevent possible hearing damage, do not listen at high volume levels for long periods.
- 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. 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.
- All the electronic operation should be strictly compliance with the electrical safety regulations, fire prevention regulations and other related regulations in your local region.
- Please use the power adapter, which is provided by normal company. The power consumption cannot be less than the required value.

- Do not connect several devices to one power adapter as adapter overload may cause over-heat or fire hazard.
- Please make sure that the power has been disconnected before you wire, install or dismantle the device.
- If smoke, odors or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service center.
- If the product does not work properly, please contact your dealer or the nearest service center. Never attempt to disassemble the device yourself. (We shall not assume any responsibility for problems caused by unauthorized repair or maintenance.)

⚠ Cautions:

- No naked flame sources, such as lighted candles, should be placed on the equipment.
- The ventilation should not be impeded by covering the ventilation openings with items, such as newspapers, table-cloths, curtains, etc. The openings shall never be blocked by placing the equipment on a bed, sofa, rug or other similar surface.
- The serial port of the equipment is used for debugging only.
- 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 100% applicable to anti-spoofing environments. If you require a higher security level, use multiple authentication modes.

Available Model

Product Name	Model
Visitor Terminal	DS-K5032-3XFD

Contents

Chapter 1 Overview

1.1 Overview

The visitor terminal is designed for visitor management, integrated with temperature measurement, which is mainly applied to enterprises, stations, university campuses, factories, etc.

1.2 Main Features

- Android operation system with dual-screen design.
- Temperature measuring range: 30 °C to 45 °C (86 °F to 113 °F), accuracy: 0.1 ° C, deviation: ± 0.5 °C
- Recognition distance: 0.3 to 2 m.
- Fast temperature measurement for visitor.
- Paperless visitor enrollment.
- Real-time visitors counting for the current day.
- Supports both stand-alone and networking application. TCP/IP and Wi-Fi are available for networking application.
- Up to 150,000 visitor records can be stored on the device.

Chapter 2 Appearance

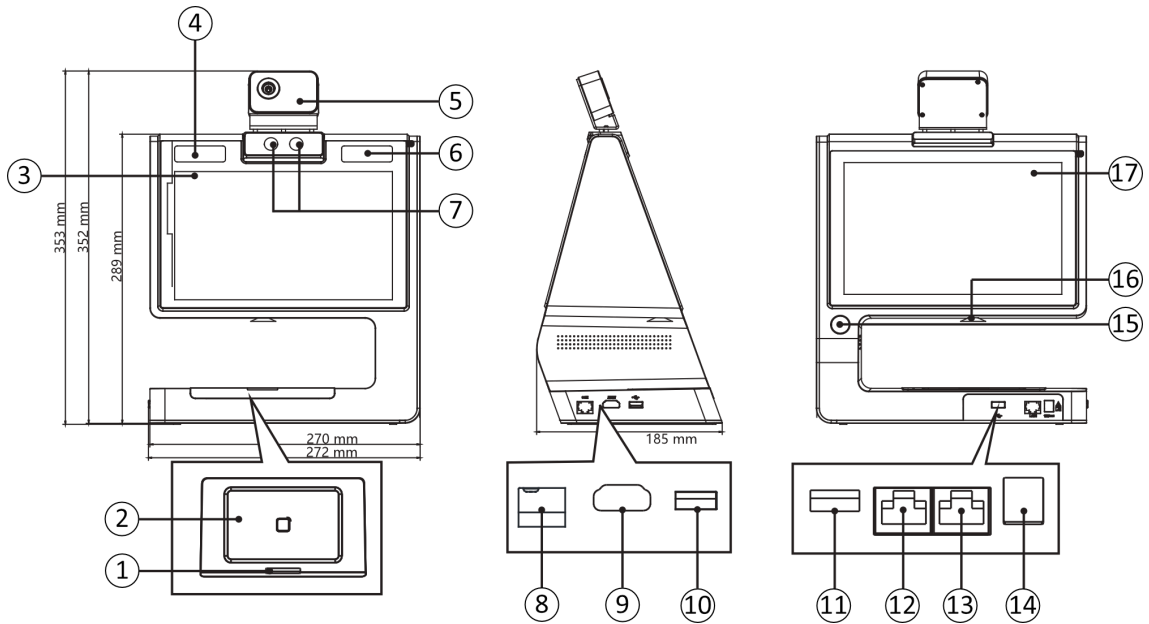Refer to the following contents for detailed information of the visitor terminal:

Figure 2-1 Visitor Terminal Diagram

Table 2-1 Description of Face Recognition Terminal

No.	Description
1	Indicator for Card Presenting
2	Card Presenting Area
3	Visitor Screen
4	Supplement Light
5	Thermographic Module
6	Supplement Light
7	Camera
8	Reserved
9	Reserved
10	USB 2.0 (Sub Interface)

No.	Description
	ⓘNote Supports the USB import function. You can use the interface to upload the event to the client software, etc.
11	USB 2.0 **ⓘNote** The interface can connect with an USB flash drive. You can import the allowlist to the device or export the events to the USB flash drive.
12	Reserved
13	Network Interface
14	Power Interface
15	Power Switch Hold: Power On/Power Off/Reboot Press: Sleep/Wake Up
16	Bottom Camera
17	Operator Screen

Chapter 3 Installation

3.1 Installation Environment

- Avoid backlight, direct sunlight, and indirect sunlight.
- For better face recognition, there should be light source in or near the installation environment.
- Sunlight, wind, hot/cool air from air conditioner and other external factors, which may affect surface temperature, will create the deviation of the temperature measurement. In order to get an accurate result, make sure the device is applied indoors and windlessly (where is relatively isolated from the outdoors). The working temperature should keep between 10 °C and 35 °C. If there are no suitable environments for temperature measurement (the area faces the indoor and connects the outdoor, the area at the door of the indoor environment, etc.), building a temporary temperature measurement environment is suggested.
- Influence Factors of Temperature Measurement:
  Wind: The wind will take the heat away, which may affect the measurement result.
  Sweat: The sweat will take the heat away, which may affect the measurement result.
  Air Conditioner (Cool Air): If the indoor temperature is low, the surface temperature may also lower than the actual temperature, which may affect the measurement result.
  Air Conditioner (Heat) or Heating: If the indoor temperature is high, the surface temperature may also higher than the actual temperature, which may affect the measurement result.
- In order to make the device work properly, you should wait for 90 min after the device is powered on.
- For details about installation environment, see ***Tips for Installation Environment*** .

3.2 Installation

Steps
1. Put the device on the surface.

   $\boxed{i}$**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.
4. **Optional:** Connect th device with the network.

Chapter 4 Wiring

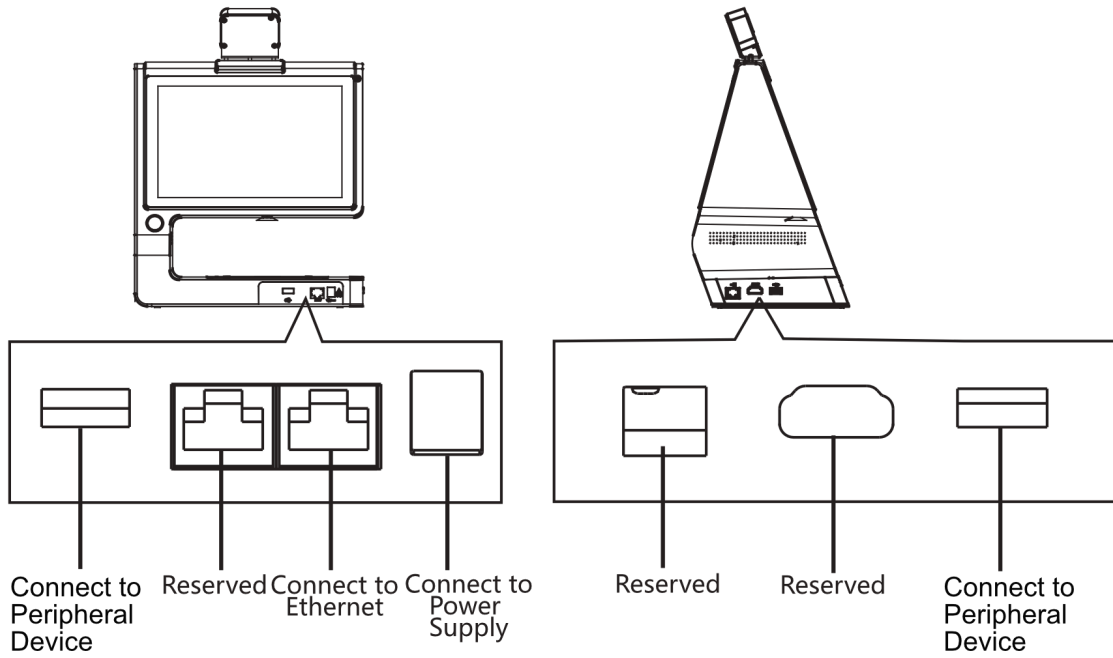The suggested wiring diagram is as follows:

Figure 4-1 Wiring Diagram

Chapter 5 Activation

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

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

The default values of the device are as follows:

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

5.1 Activate via Device

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

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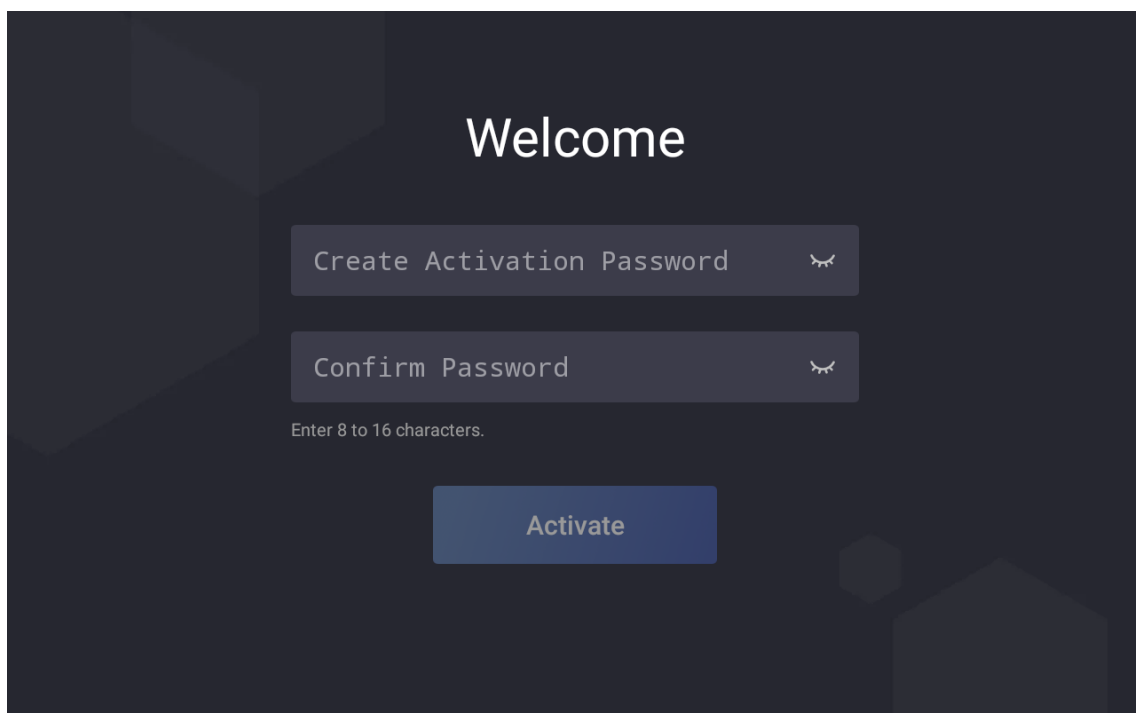

Figure 5-1 Activation Page

⚠️**Caution**

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

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

- Select a language. For details, see *__Select Language__* .
- Select a time zone. For details, see *__Set Time Zone__* .
- Set network. For details, see *__Set Network Parameters__* 。

5.2 Activate via Web Browser

You can activate the device via the web browser.

Steps

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

ℹ️**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.

ℹ️**Note**

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

3. Click **Activate**.

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

5.3 Activate via SADP

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

Before You Start

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

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

Steps

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

⚠ **Caution**

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

🛈 **Note**

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

4. Click **Activate** to start activation.
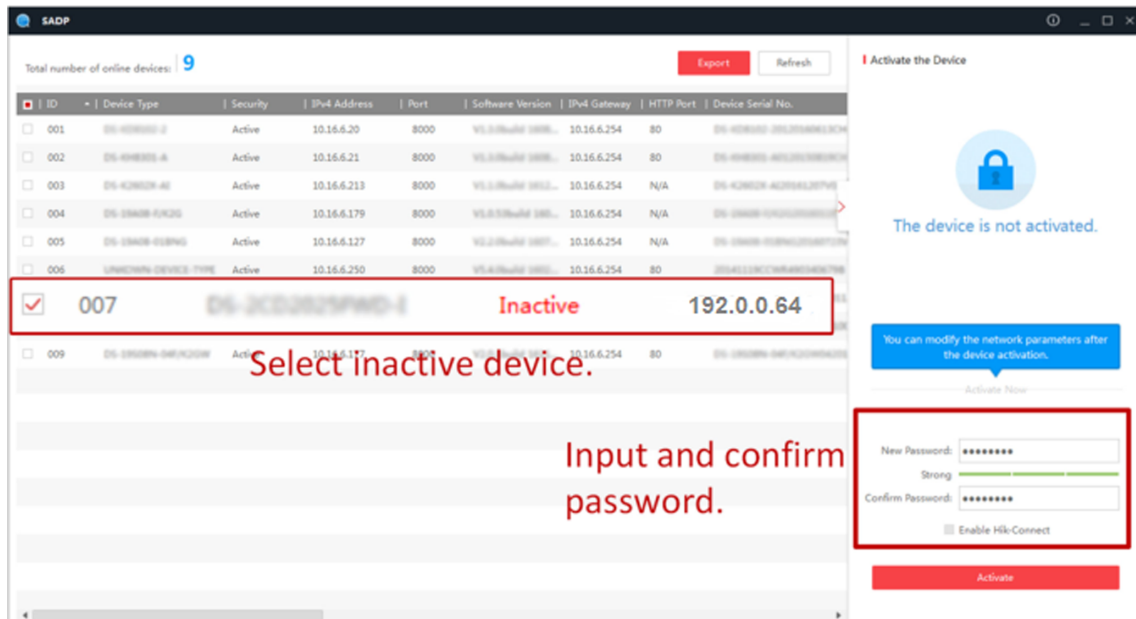
Status of the device becomes **Active** after successful activation.

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 6 Quick Operation

6.1 Select Language

You can select a language for the device system.

After the device activation, you can select a language for the device system.
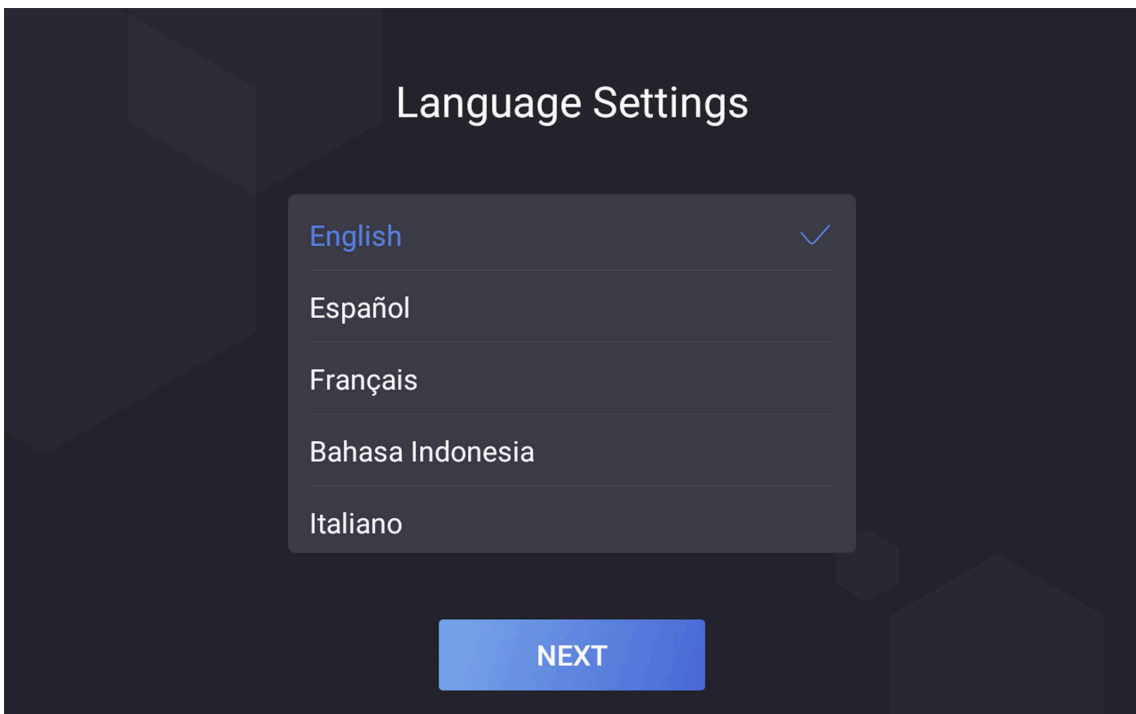
Figure 6-1 Select System Language

By default, the system language is English.

[i]**Note**

You will need to exit the APP and change the Android system language via Google Pinyin Input to the same language you choose for the APP system.

6.2 Set Time Zone

You can set a time zone for the device system.

Steps

1. Select a time zone according to your actual needs.
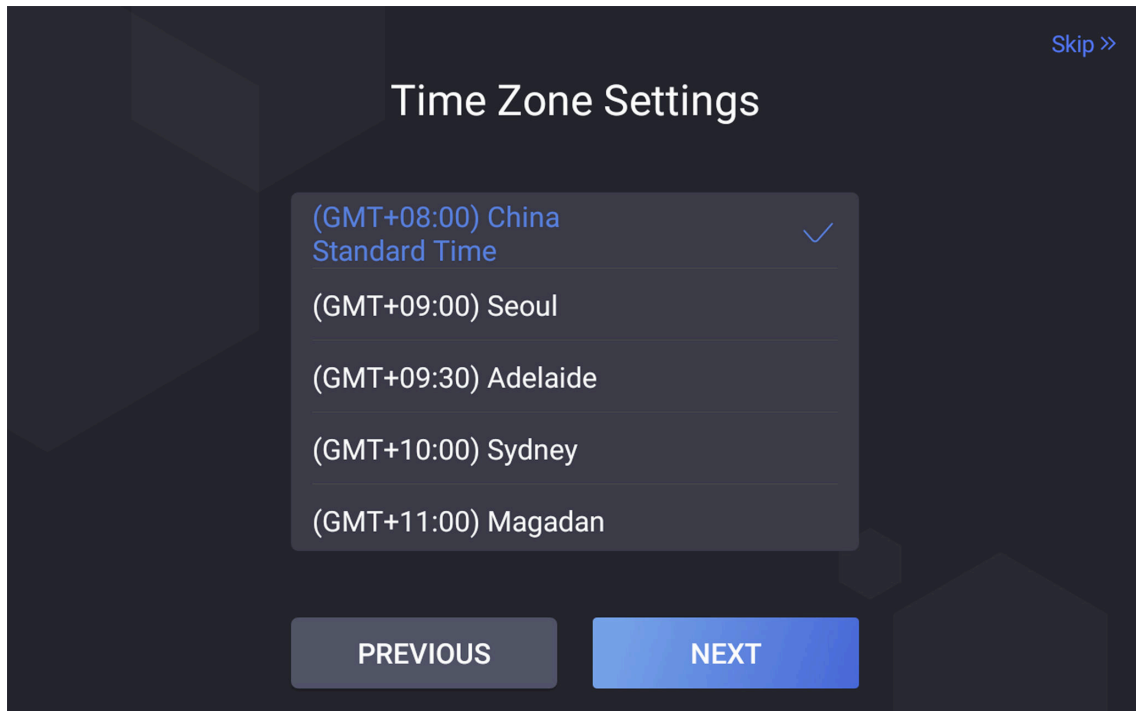
Figure 6-2 Time Zone Settings

⌷ᵢ**Note**

- The time zone will affect the device time.

2. Tap **Next**.

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

4. **Optional:** Tap **PREVIOUS** to back to the previous page.

6.3 Set Network Parameters

You can set the network for the device.

Steps

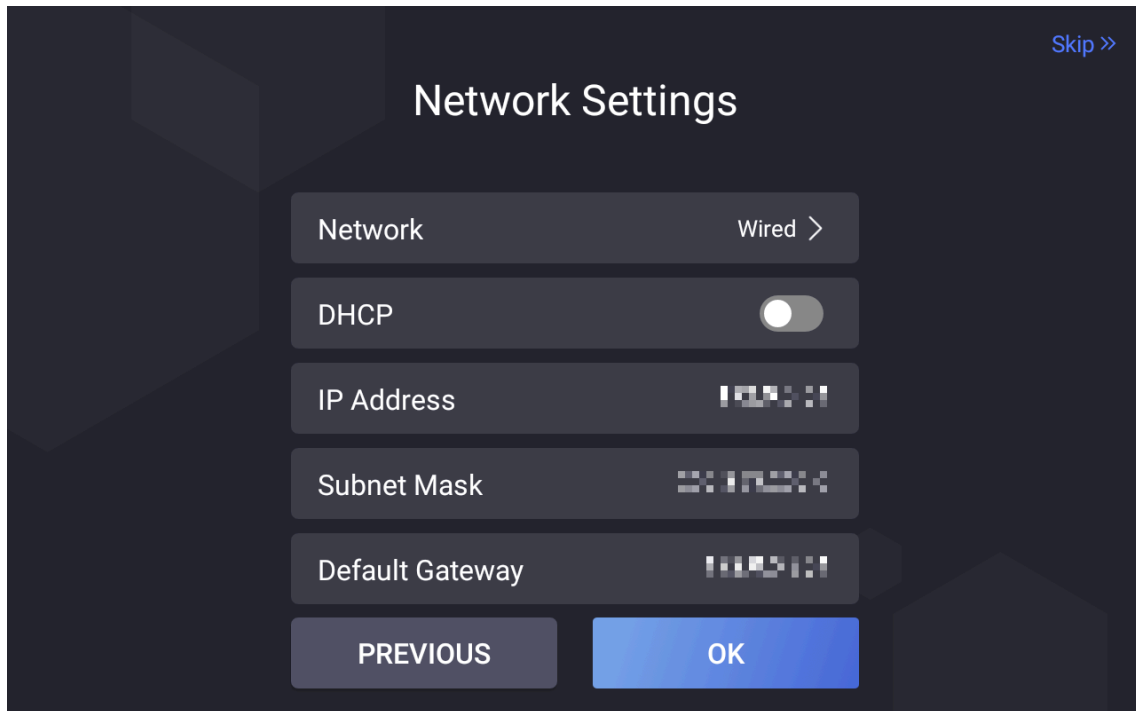1. Tap **Wired Network** or **Wi-Fi** for your actual needs.

Figure 6-3 Select Network

Wired Network

ⓘ**Note**

Make sure the device has connected to a network.

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

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

Wi-Fi

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

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

ⓘ**Note**

Disconnect the wired network before connecting a Wi-Fi.

---

2. Tap **Next**.
3. **Optional:** Tap **Skip** to skip network settings.
4. **Optional:** Tap **PREVIOUS** to back to the previous page.

Chapter 7 Basic Operation

7.1 Visitor Check In

7.1.1 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.
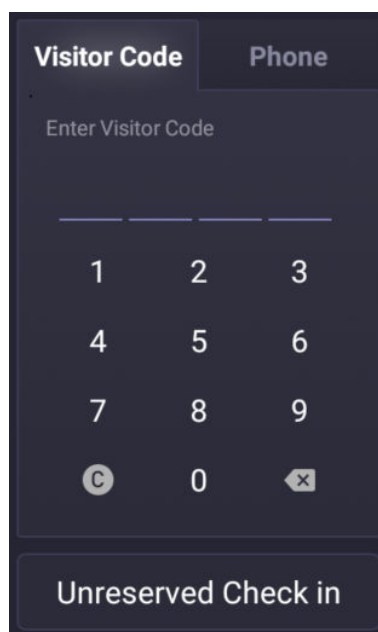

Figure 7-1 Reserved Visitor Check In

$\boxed{i}$**Note**
- The page and instructions are based on dual-screen devices and are referable for single-screen devices.
- Go to ***Set Basic Parameters*** and set the length of the visitor code.
- Visitor reservation is disabled by default. Go to ***Set Basic Parameters*** and enable **Visitor Reservation**.

2. Present the card on the card presenting area. The visitor's temperature will be displayed on top of the screen.

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 and measure temperature.
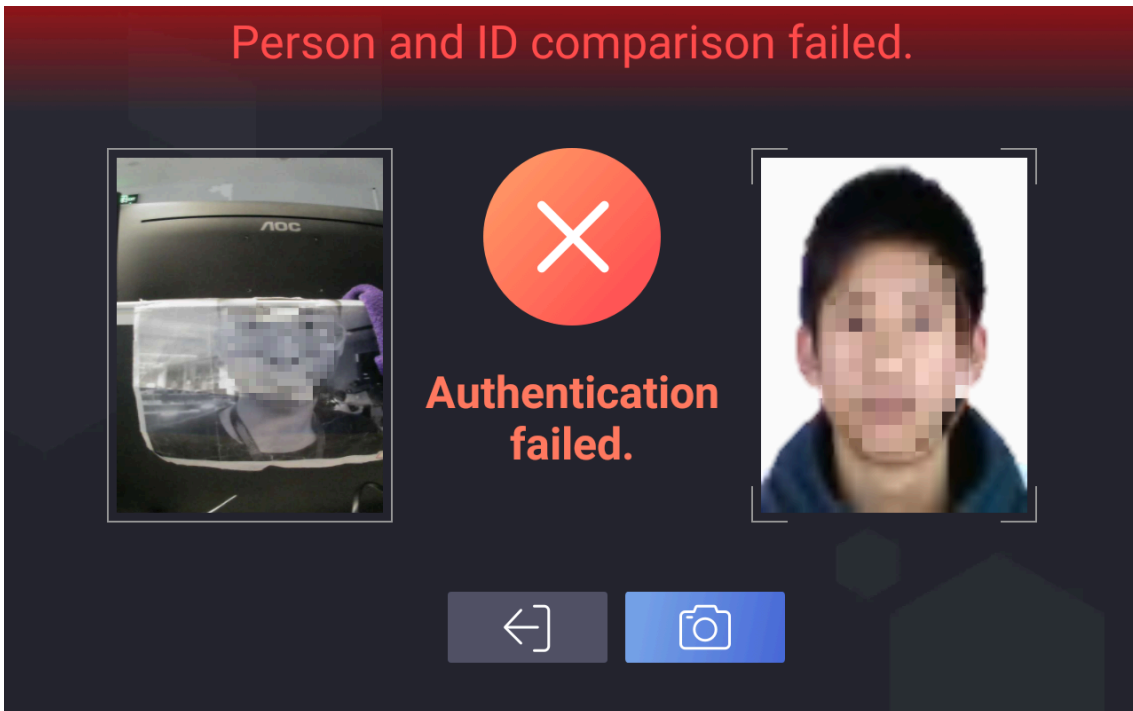

Figure 7-2 Failed Authentication

4. Fill in the rest of the visitor information.

[i]**Note**

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

5. Click **Check In** on the visitor check-in information page.
6. Optional: Tap **Live View** to display part of the visitor information on the visitor screen.

[i]**Note**

Refer to ***Printing Receipt Settings*** for configuration details.

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

7.1.2 Non-Reserved Visitor Check In

Check-in for unreserved visitors.

Before You Start

Complete the basic settings and visitor parameter settings. Refer to ***Set Basic Parameters*** and ***Visitor Check In Settings*** for details.

Steps

1. Enroll visitor information.

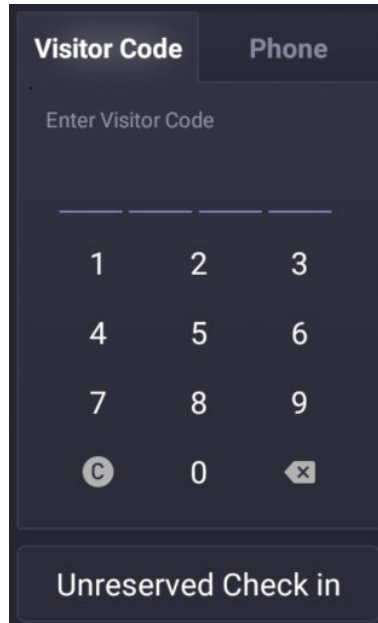   1) Tap **Unreserved Check In** in the lower right corner of the home page to enter the visitor check-in page.
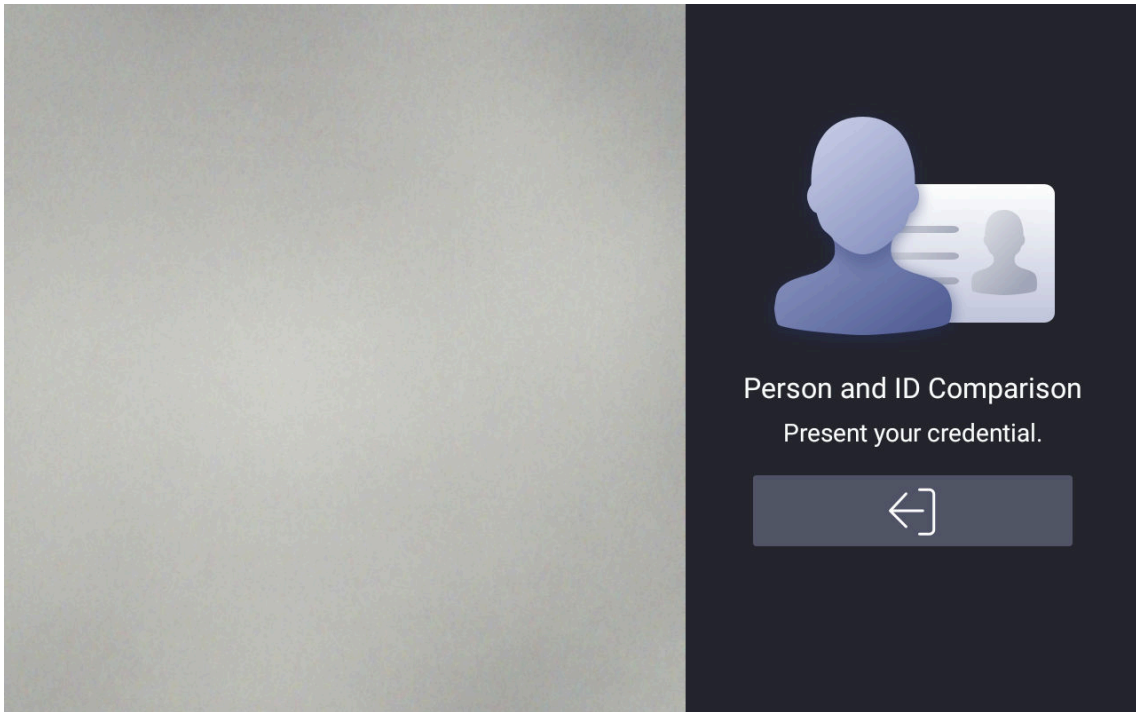

Figure 7-3 Visitor Check In

Figure 7-4 Visitor Check In

2) Present the card on the card presenting area for authentication. The visitor's temperature will be displayed on top of the screen.

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

Figure 7-5 Visitor Check-in Information

Note

If authentication fails, tap [←] to retry authentication, or tap [📷] to capture face picture and measure temperature.
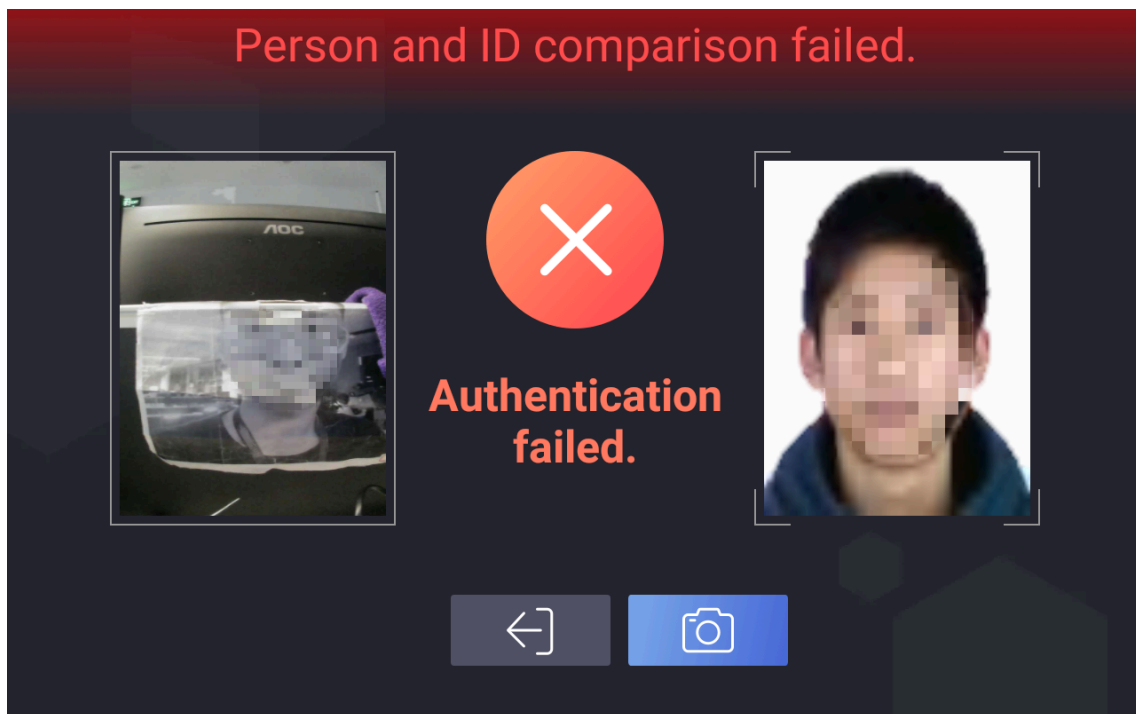
Figure 7-6 Failed Authentication

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

> **Note**
>
> - The system will perform recognition according to the configurations in **Settings → Basic Settings** . Refer to *Set Basic Parameters* for details.
> - The page and instructions are based on dual-screen devices and are referable for single-screen devices.
> - Go to *Visitor Check In Settings* and set the visitor information to be displayed.

4) Fill in the visitor information.

> **Note**
>
> Go to *Visitor Check In Settings* and set the visitor information to be filled in.

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

3. **Optional:** Tap **Live View** to display part of the visitor information on the visitor screen.

> **Note**
>
> Refer to *Printing Receipt Settings* for configuration details.

What to do next

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

7.1.3 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 Basic Parameters_** and **_Visitor Check In 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.
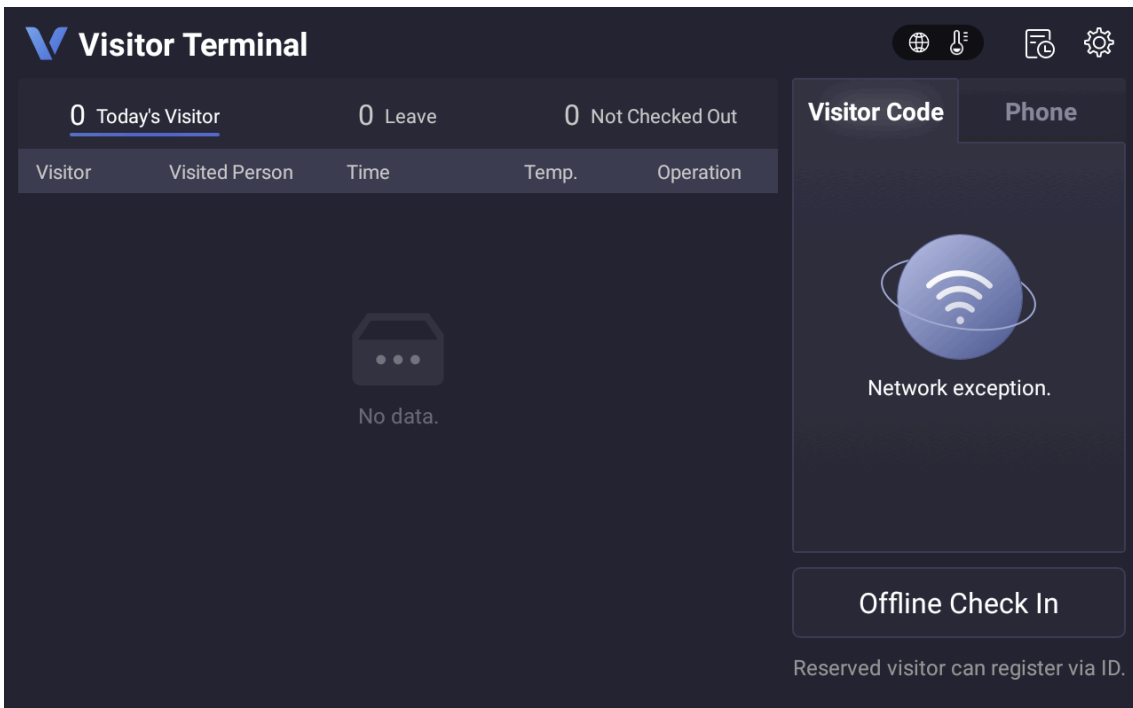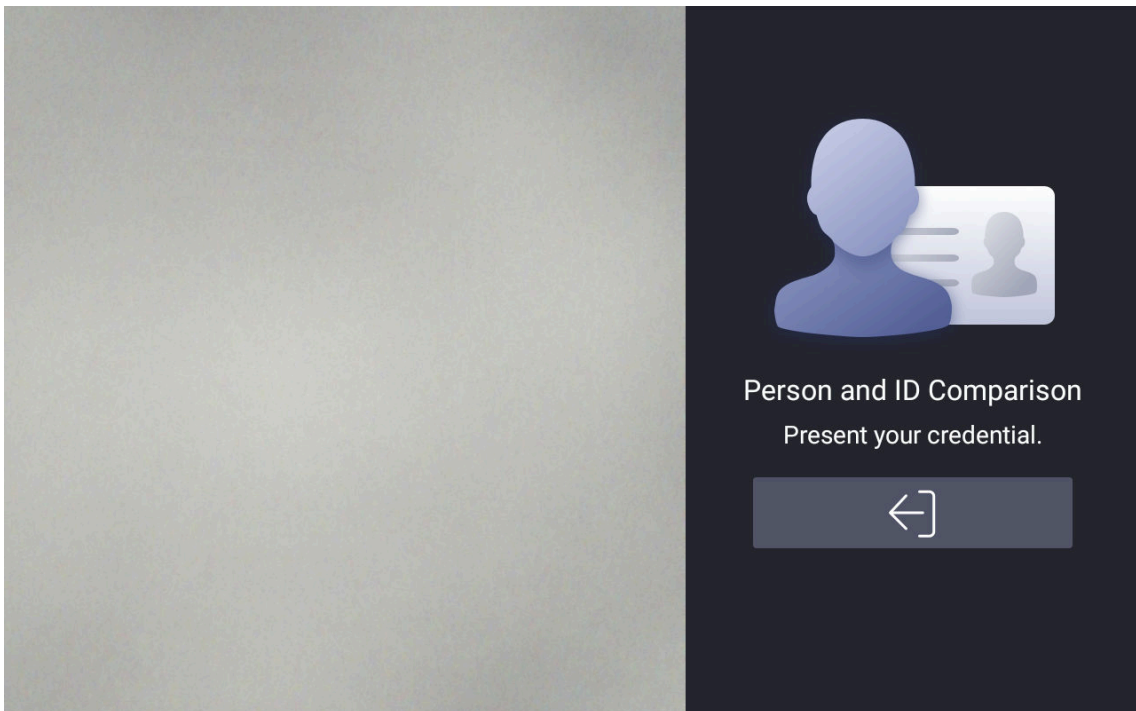

Figure 7-7 Offline Check In

Figure 7-8 Person and ID Comparison

2) Present the card on the card presenting area for authentication. The visitor's temperature will be displayed on top of the screen.

⬛**Note**

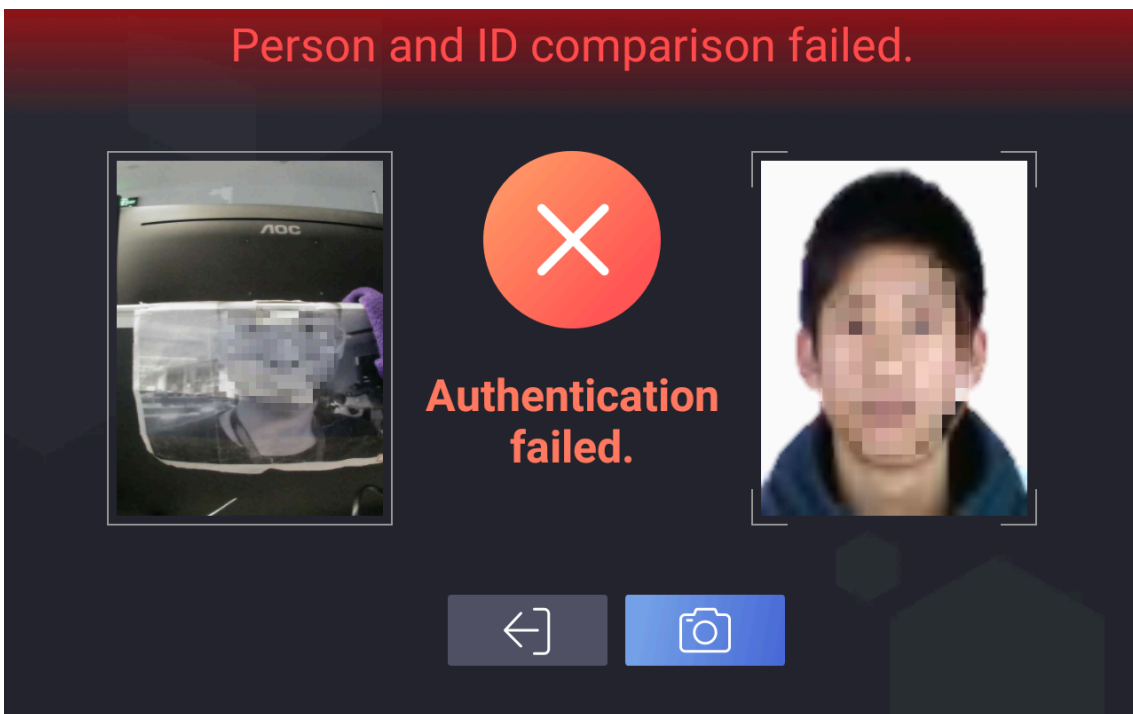If authentication fails, tap [⬅] to retry authentication, or tap [📷] to capture face picture and measure temperature.

Figure 7-9 Failed Authentication

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

> 🛈 **Note**
>
> - The system will perform recognition according to the configurations in **Settings → Basic Settings** . Refer to *__Set Basic Parameters__* for details.
> - The page and instructions are based on dual-screen devices and are referable for single-screen devices.
> - Go to *__Visitor Check In Settings__* and set the visitor information to be displayed.

4) Fill in the visitor information.

> 🛈 **Note**
>
> Go to *__Visitor Check In Settings__* and set the visitor information to be filled in.

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

3. **Optional:** Tap **Live View** to display part visitor information on the visitor screen.

> 🛈 **Note**
>
> Refer to *__Printing Receipt Settings__* for configuration details.

What to do next

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

7.2 Visitor Check Out

7.2.1 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.

⃞i Note

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

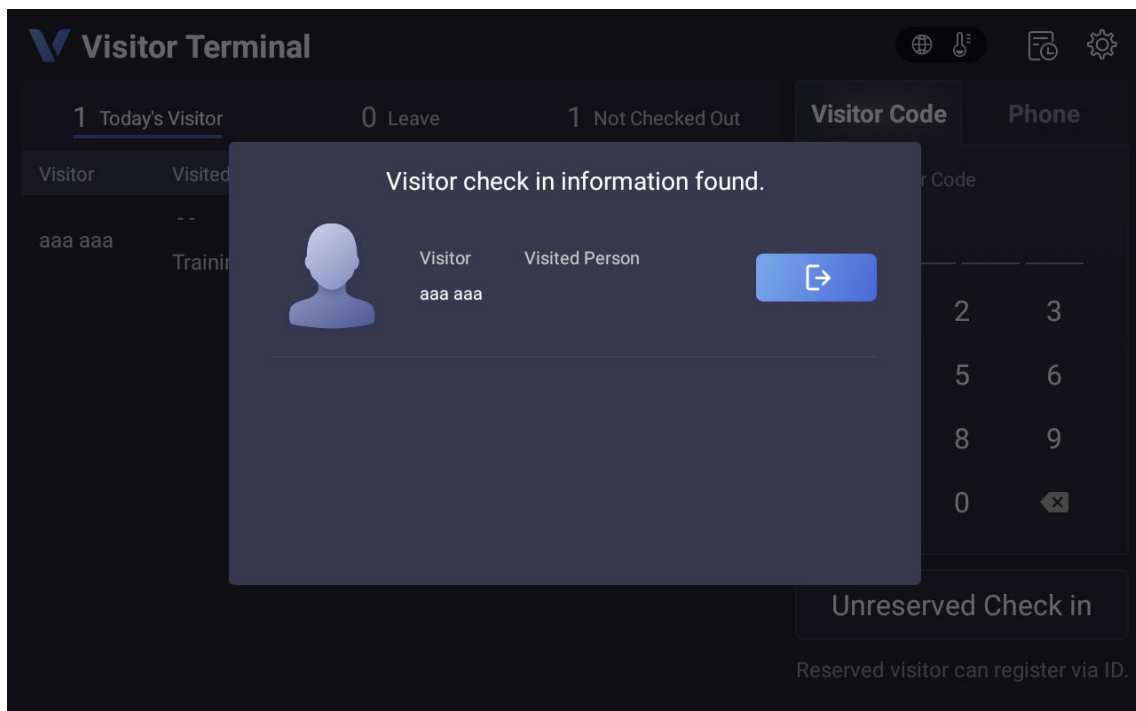The check-out window will pop up on the operator screen.
2. Tap **Check Out**.

Figure 7-10 Check Out

⃞i Note

The page and instructions are based on dual-screen devices and are referable for single-screen devices.

7.2.2 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**.

7.2.3 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**.

7.2.4 Auto Check Out

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

7.3 Staff-Service Visitor System

7.3.1 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 Reason**, or **Visiting Time**. Tap ☑ to start filtering.

7.3.2 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.

7.3.3 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. Tap **Communication Settings → Wired Network** or **Communication Settings → Wi-Fi** according to your actual needs.

2. Set network.

Wired Network

> 🛈**Note**
>
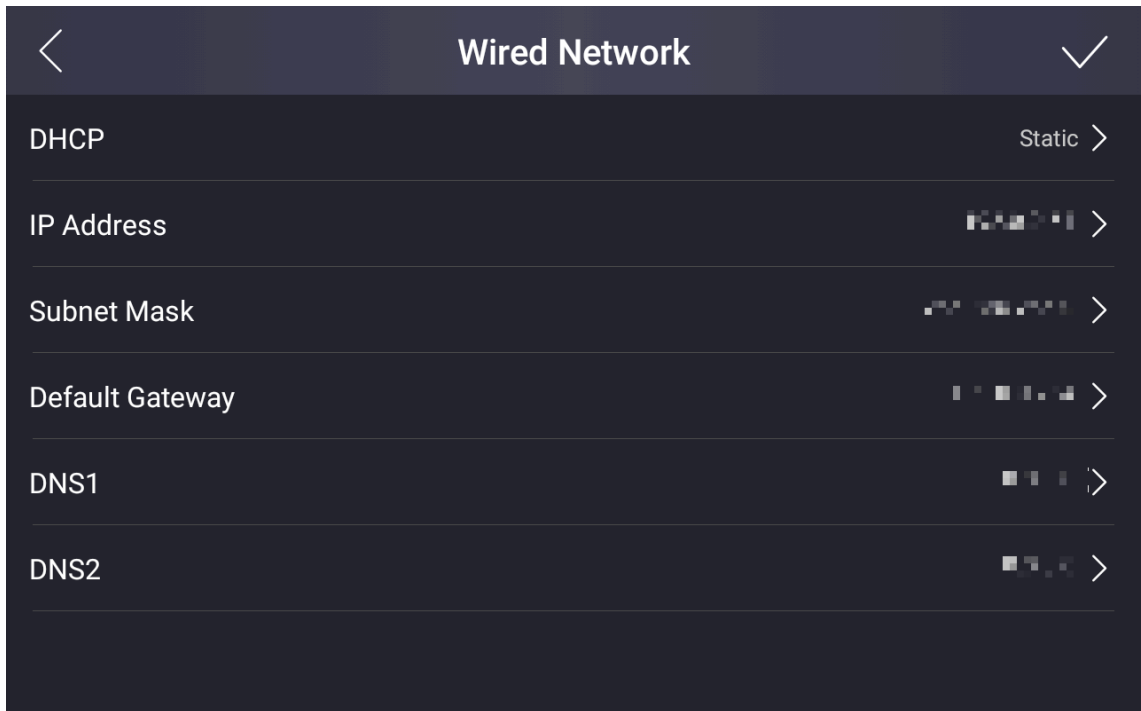> Make sure the device has connected to a network.

Figure 7-11 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.
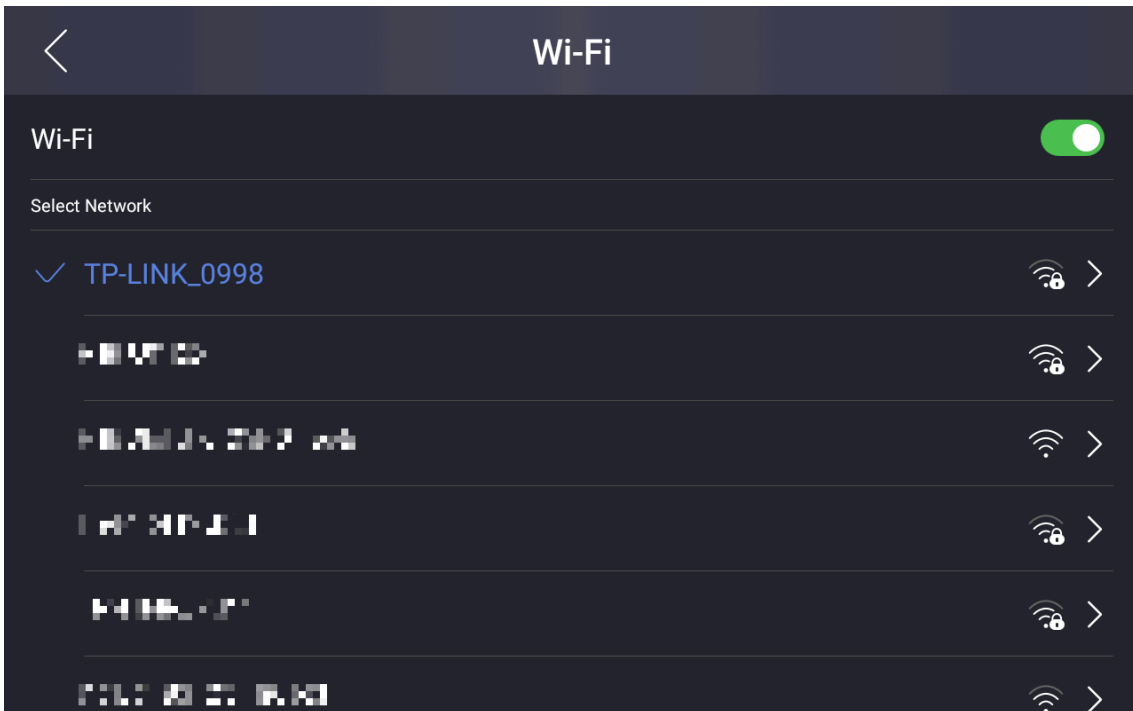
Tap ☑ to save the settings.

Wi-Fi

Figure 7-12 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.

Temperature Measurement Settings

You can set the temperature measurement parameters, including temp. detection, unit, Max. temperature, Min. temperature, temperature measurement distance and temp. limit to stop visitor registration.

Tap **Temperature Settings** to enter the Temperature Settings page. Edit the temperature measurement parameters on this page and tap ☑ to save the settings.
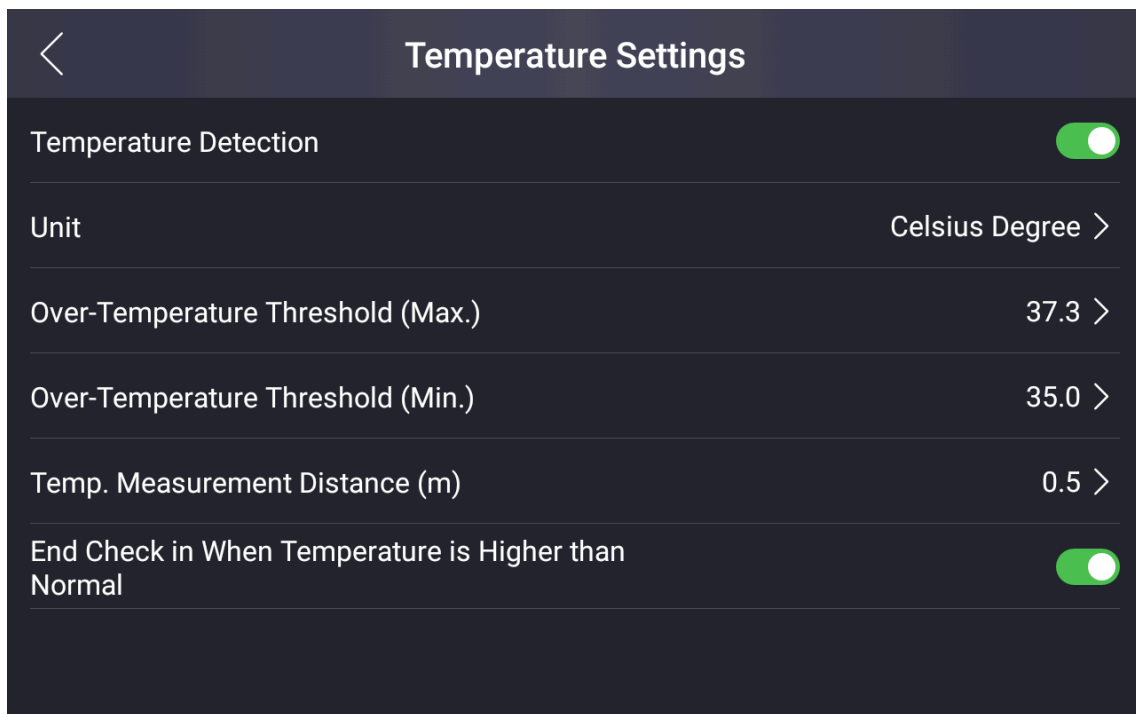
Figure 7-13 Temperature Measurement Parameters

The available parameters descriptions are as follows:

Temp. Detection

When enabling the function, the device will authenticate the permissions and at the same time take the temperature. When disabling the device, the device will authenticate the permissions only.

Unit

Select a temperature unit according to your preference.

Over-Temperature Threshold (Max.)

Configure the upper limit for temperature measurement result. Device will alarm when the visitor's temperature exceeds the threshold. The value is 37.3 ℃ by default.

Over-Temperature Threshold (Min.)

Configure the lower limit for temperature measurement result. Device will alarm when the visitor's temperature does not reach the threshold. The value is 35 ℃ by default.

Temp. Measurement Distance (m)

Configure the temperature measurement distance according to actual needs. Distance between 0.3 m to 2 m is recommended and is set 0.5 m by default.

End Check-in When Temperature is Higher than Normal

When the visitor's temperature exceeds the threshold, visitor check-in procedure will be terminated.

Set Basic Parameters

You can set basic parameters for the device.

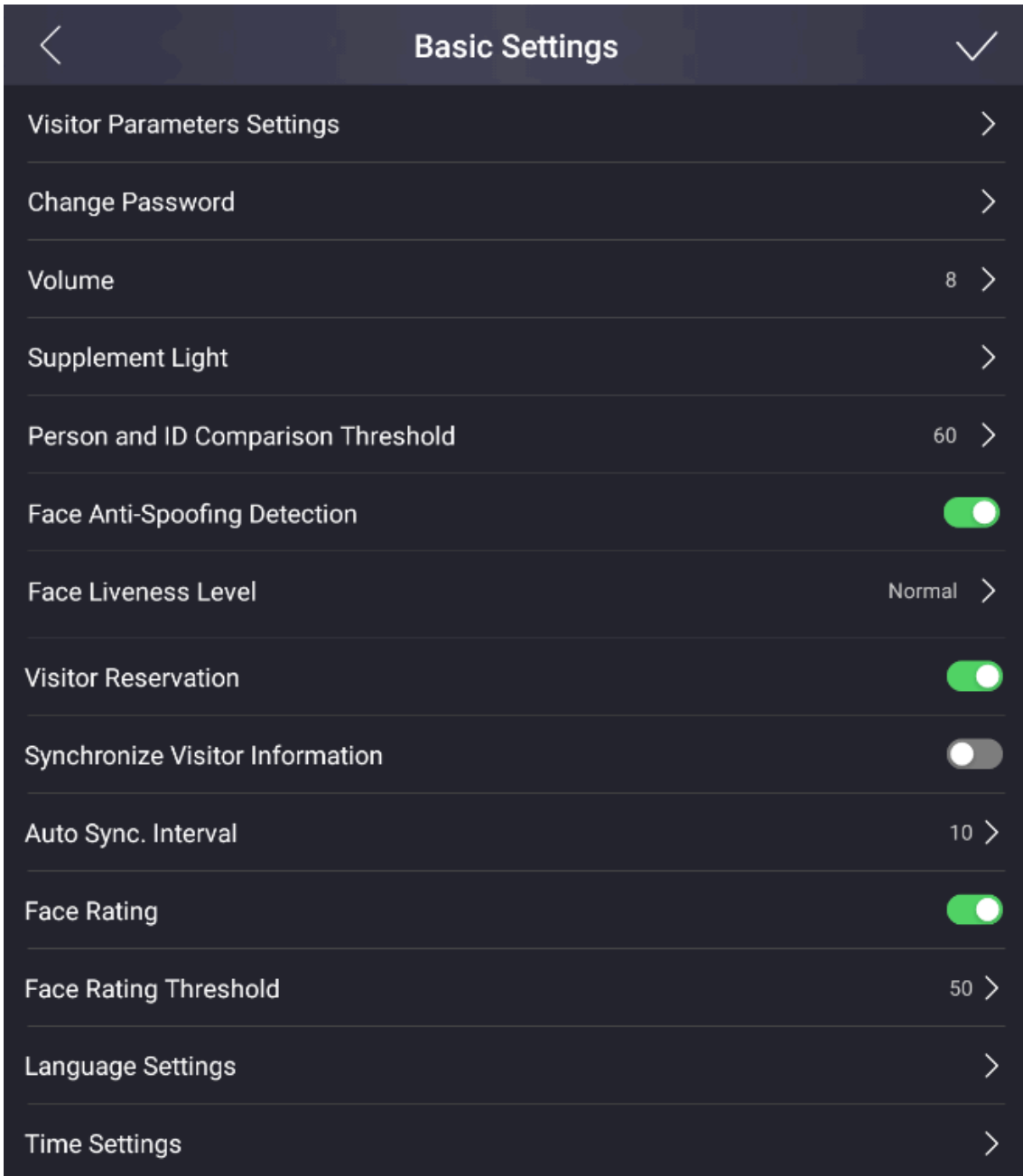Tap ⚙ in the top right corner of the home page. Tap **Settings → Basic Settings** .

Figure 7-14 Basic Parameters

Table 7-1 Basic Parameters

Parameter	Description
Visitor Parameters Settings	Set visitor parameters. Refer to **_Set Visitor Parameters_** for details.
Change Password	Enter old password and confirm new password. The password here is the activation password.
Volume	Adjust the voice volume ranging from 0 to 10. The larger the value, the louder the volume.
Supplement Light	Set the white or IR supplement light's brightness. The brightness ranges from 0 to 100.
Person and ID Comparison Threshold	Set the threshold for person and ID comparison. The larger the value is, the smaller the false accept rate and the larger the false rejection rate.
Face Anti-Spoofing Detection	If enabling the function, the device can recognize whether the person is a live one or not.
Face Liveliness Level	After enabling face anti-spoofing function, you can set the matching security level when performing live face authentication. note: Biometric recognition products are not 100% applicable to anti-spoofing environments. If you require a higher security level, use multiple authentication modes.
Visitor Reservation	Enable the function to allow check-in via visitor code or the last 4 digits of the phone number.
Synchronize Visitor Information	Enable the function to synchronize visitor information of the devices and the information on the platform automatically.
Auto Sync. Interval	Set the interval for visitor information auto synchronizing ranging from 5 to 60.
Face Rating	Enable the function to rate the face recognition.
Face Rating Threshold	Set the threshold for face rating. The larger the value is, the better the face picture quality is.
Language Settings	Set the device language.
Time Settings	Set the device time.

Set Visitor Parameters

You can enable the functions for visitor check-in.

Tap ⚙ in the top right corner of the home page. Tap **Basic Settings → Visitor Parameters Settings** to enter the page.
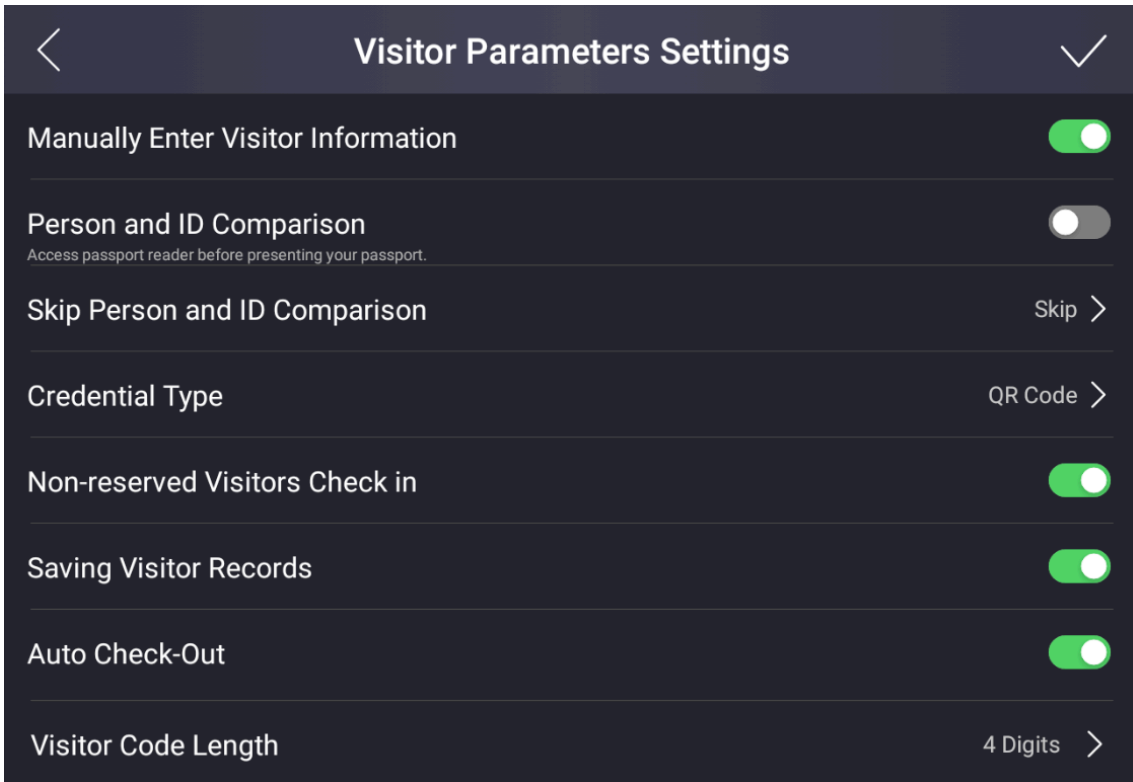

Figure 7-15 Visitor Parameters Settings

Tap to enable the functions.

Manually Enter Visitor Information

When the function is enabled, the staff can input visitor information manually.

Person and ID Comparison

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

Skip Person and ID Comparison

ⓘ**Note**

You need to enable **Person and ID Comparison** before you can skip the step.

When the function is enabled, you can choose to skip person and ID comparison.

Credential Type

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

Non-reserved Visitor Check In

When the function is enabled, unreserved visitors can check in on the device.

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.

Auto Check Out

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

Visitor Code Length

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

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. Tap **Data Management** to enter the page.
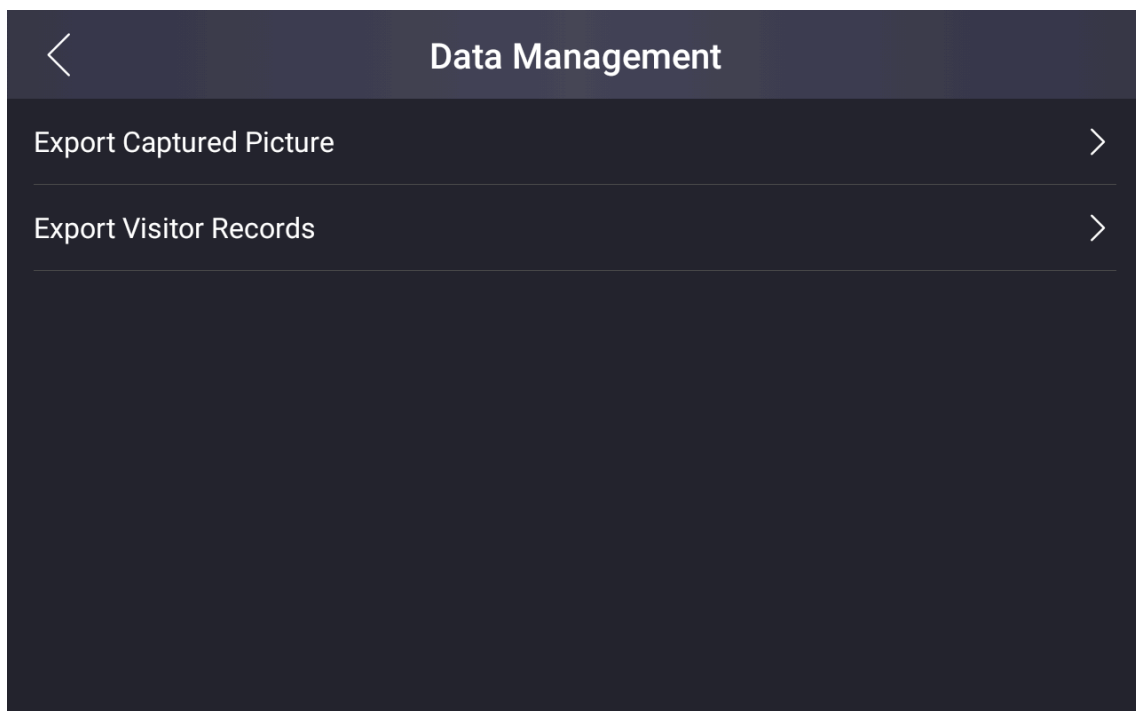

Figure 7-16 Data Management

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.

System Maintenance

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

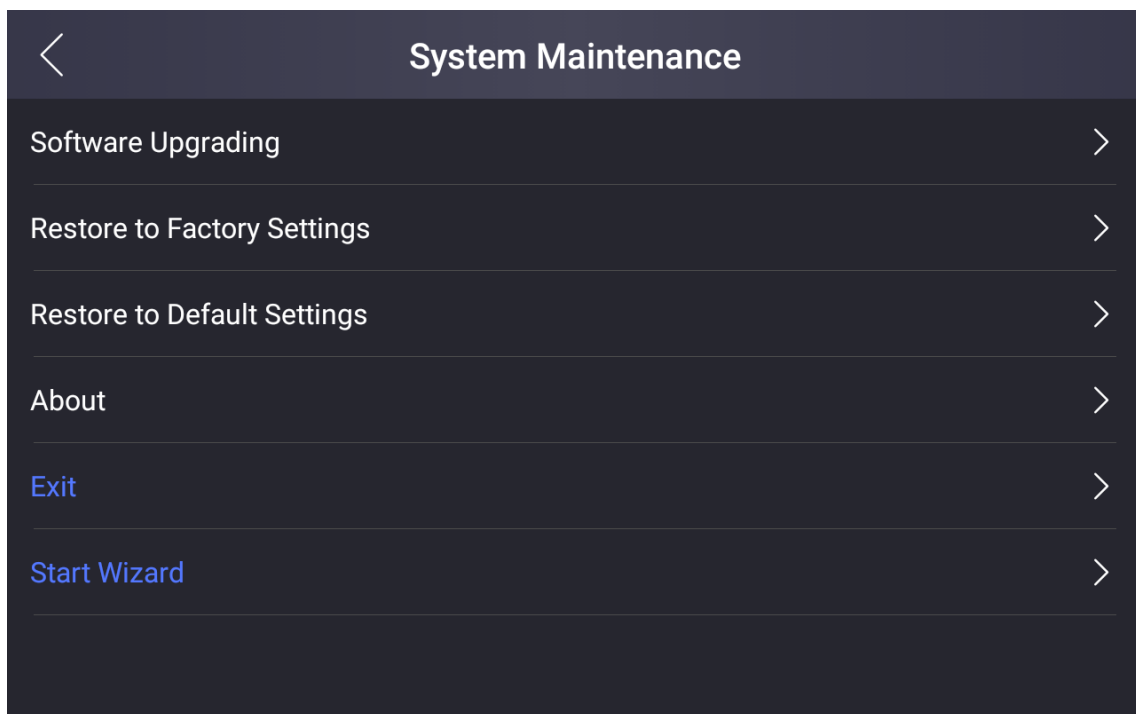Tap ⚙ in the top right corner of the home page. Tap **Settings → System Maintenance** .

Figure 7-17 System Maintenance

Software Upgrading

Plug the USB flash drive in the device USB interface.

- Tap **Upgrade → OK** , and choose the file with the extension of zip in the USB flash drive for the device to read and start system upgrading.
- Tap **Upgrade Component → OK** , and choose the file with the extension of dav in the USB flash drive for the device to read and start component upgrading.
- Tap **Upgrade Temperature Detection Module → OK** , and choose the file with the extension of dav in the USB flash drive for the device to read and start temperature detection module upgrading.

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.

About

You can view the device information.

$\boxed{i}$**Note**

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

Exit

Tap **Exit** to exit the application.

Start Wizard

Tap **Start Wizard** for language settings, time zone settings and network settings. Refer to **_Quick Operation_** for details.

Start Wizard

If you do not set the wizard information after activation or you want to set the parameters again, you can open the wizard on the settings page.

Tap ⚙ in the top right corner of the home page. Tap **System Maintenance → Start Wizard** .
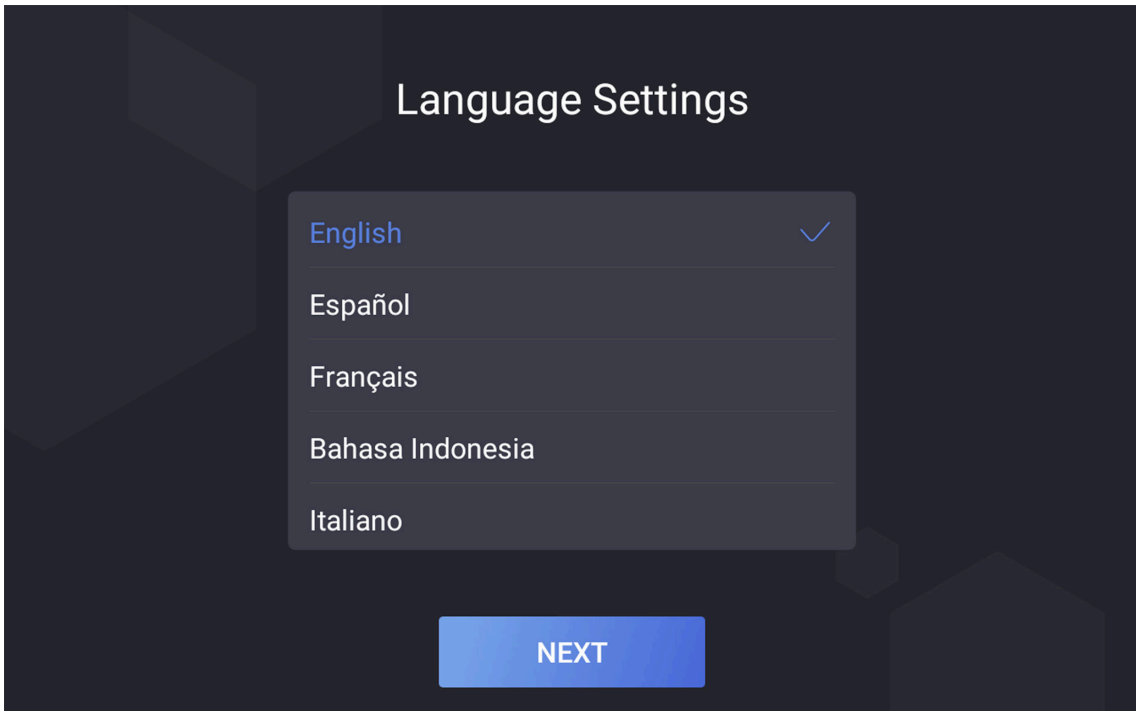
Select Language

Figure 7-18 Select Language Page

Select a language according to your actual needs. By default, the language is English.

⬛**Note**

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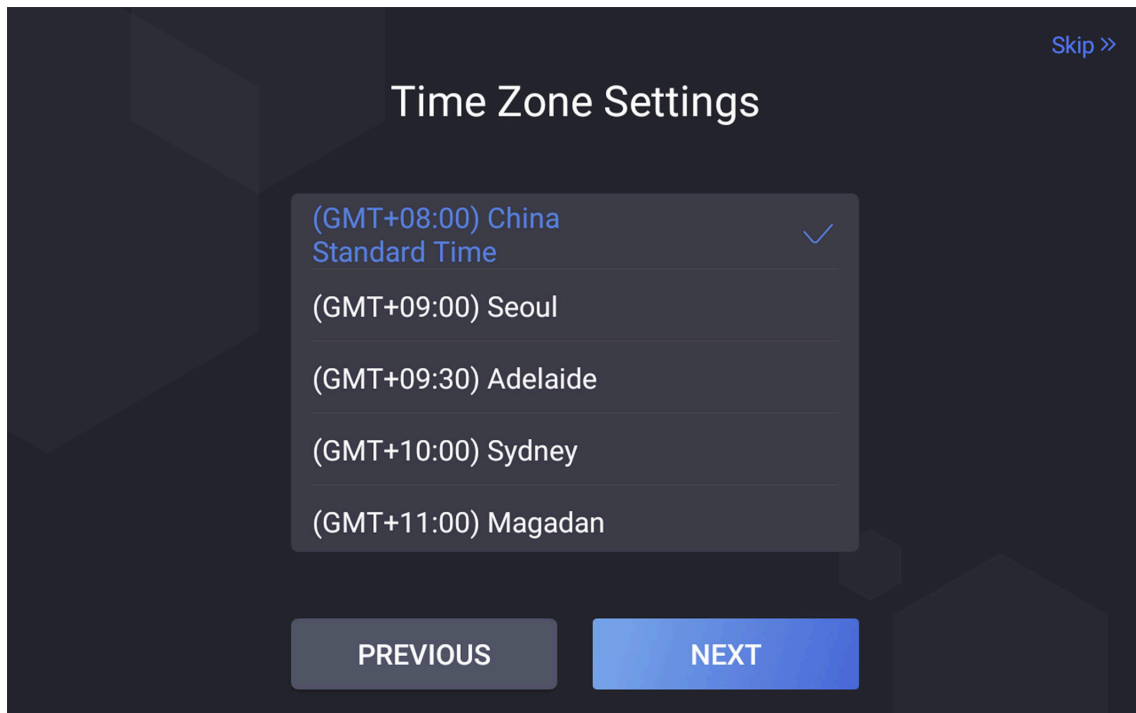
Tap **Next**.

Set Time Zone

Figure 7-19 Set Time Zone

Select a time zone according to your actual needs.

![Note icon]**Note**

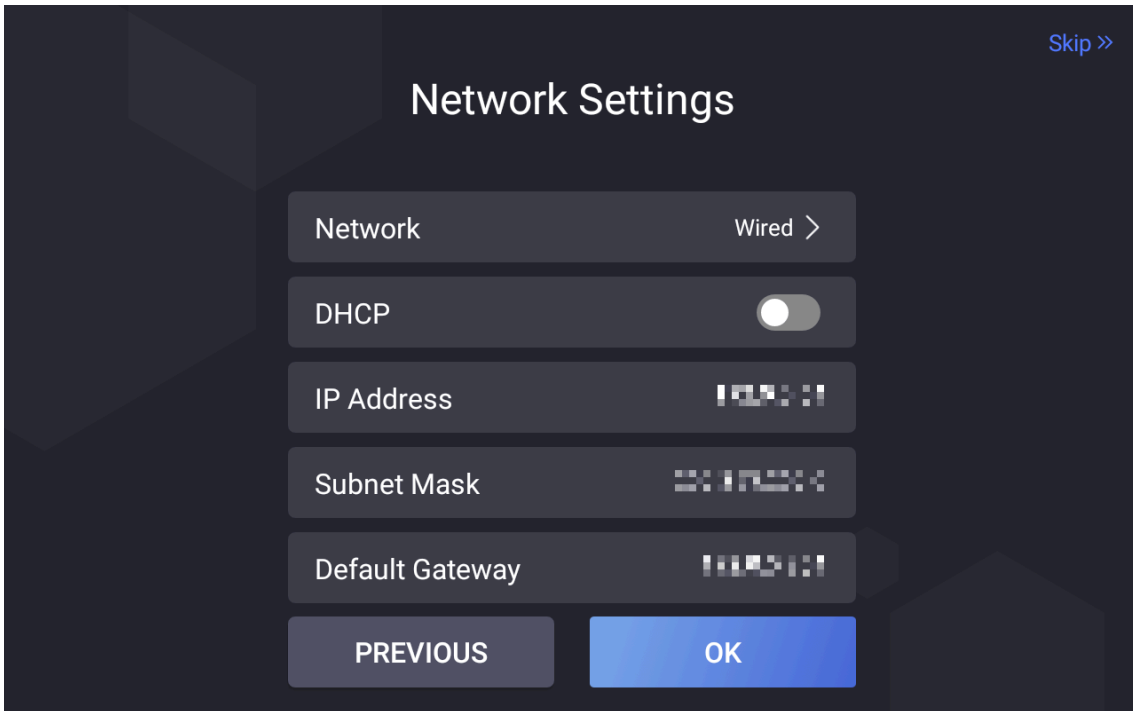The time zone will affect the device time.

Tap **Next**.

Set Network

Figure 7-20 Set Network

Select **Wired** or **Wireless**.

☐**i**│**Note**

Disconnect the wired network before connecting a Wi-Fi.

Wired

☐**i**│**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.

Tap **OK**. Or if you do not want to set the network parameters, tap **Skip** to skip network settings.

Visitor Check In 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. Tap **Custom Settings → Visitor Check in Settings** .

Figure 7-21 Visitor Check in Settings Page

2. Set the target items as **Required**, **Not Required** or **Hide**.

Visitor Name

Visitor name that the visitor needs to fill in when checking in.

Gender

Visitor's gender that the visitor needs to fill in when checking in.

Temp.

Visitor's temperature that the visitor needs to fill in when checking in.

Phone

Visitor's phone No. that the visitor needs to fill in when checking in.

Credential Type

Visitor's credential type that the visitor needs to fill in when checking in.

Email

Visitor's email address that the visitor needs to fill in when checking in.

Credential No.

Visitor's credential No. that the visitor needs to fill in when checking in.

Visitor Address

Visitor's address that the visitor needs to fill in when checking in.

License Plate No.

Visitor's license plate No. that the visitor needs to fill in when checking in.

Visitor Company

Visitor's company that the visitor needs to fill in when checking in.

Visiting Reason

Visitor's company that the visitor needs to fill in when checking in.

Visiting Area

Visiting area that the visitor needs to fill in when checking in.

Reception Depart.

The reception department that the visitor needs to fill in when checking in.

Receptionist

The receptionist' name that the visitor needs to fill in when checking in.

Belongings

The belongings that the visitor brings needs to fill in when checking in.

Visiting Time

The visiting time that the visitor needs to fill in when checking in.

Scheduled Leave Time

The scheduled leave time that the visitor needs to fill in when checking in.

Remark

The remark content that the visitor needs to fill in when checking in.

Custom 1/2/3

Customize visitor's check in information.

Printing Receipt Settings

Set the printing contents on the receipt.

Steps

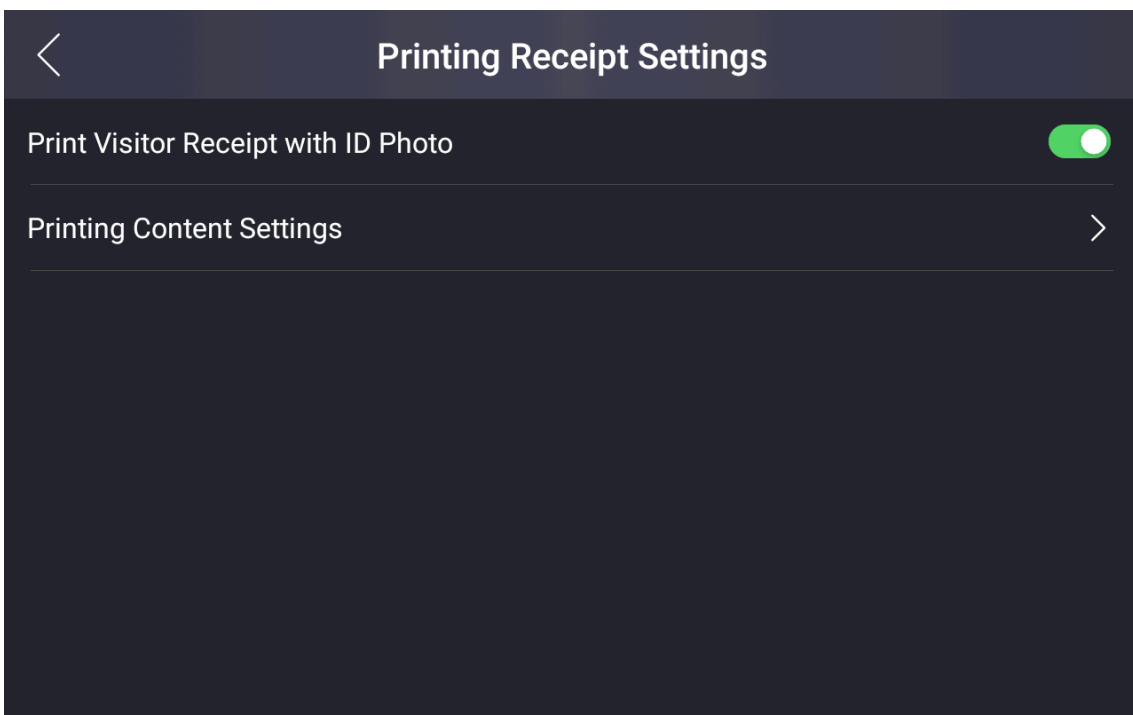**1.** Tap ⚙ in the top right corner of the home page. Tap **Custom Settings → Printing Receipt Settings** .

Figure 7-22 Printing Receipt Settings

2. Enable/disable **Print Visitor Receipt with ID Photo**. If enabling the function, the visitor's ID photo will be printed on the receipt. Otherwise, not.

3. Tap **Printing Content Settings**, and tap ↑ or ↓ , you can move the printing items on the receipt.

4. Optional: Tap ◁ on the upper left corner, you can exit the page.

Logo Management

Set the logo displayed on the upper left corner of the main page.

Steps

1. Tap ⚙ in the top right corner of the home page. Tap **Custom Settings → Logo Management** .

You can view the current logo picture.

2. Plug in the USB flash drive.

> ⓘ**Note**
>
> The supported USB flash drive format is FAT32.

3. Tap **Add** and select a logo picture from the USB flash drive.

> ⓘ**Note**
>
> The supported file size is less than 100 KB. The added picture will be cropped to 400 × 400.

4. Optional: Tap **Restore Default**, the device will use the default logo.

5. Optional: Tap **Add Again**, you can select the logo picture again.

6. Optional: Tap ◁ on the upper left corner, you can exit the page.

Screen Saver Settings

Manage the displayed picture on the visitor screen when the device is in screen saver mode.

Steps

1. Tap ⚙ in the top right corner of the home page. Tap **Custom Settings → Screen Saver** .
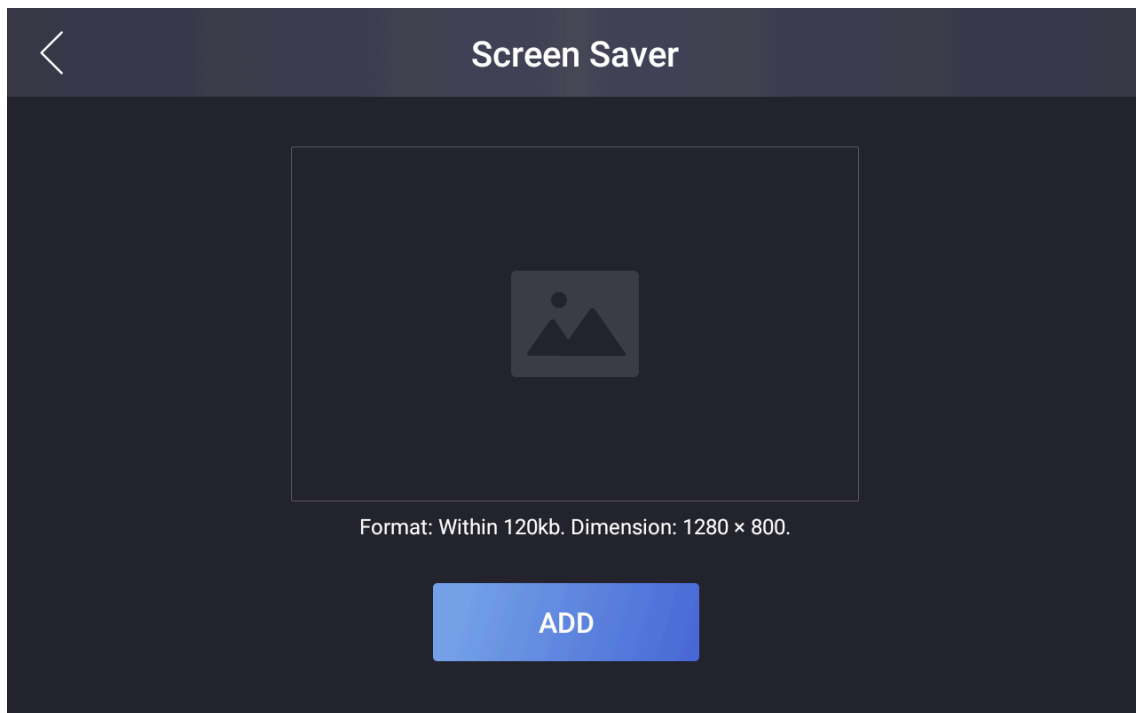

Figure 7-23 screen saver

2. Plug in the USB flash drive.

Note

The supported USB flash drive format is FAT32.

3. Tap **Add**, select a picture to add.

Note

The supported file size is less than 120 kb. The added picture will be cropped to 1280 × 800.

4. **Optional:** Tap **Restore Default**, the device will use the default picture for the screen saver.

5. **Optional:** Tap **Add Again**, you can select the picture again.

6. **Optional:** Tap ◁ on the upper left corner, you can exit the page.

Chapter 8 Operation via Web Browser

8.1 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.

8.2 Person Management

Click and add the person's basic information.

Click **OK** to save the person.

Add Basic Information

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

Figure 8-1 Add User

Add the person's basic information, including the employee ID, the person's name, the role, and the organization.

Click **Save** to save the settings.

8.3 Configuration

8.3.1 View Device Information

View the device name, language, model, serial No., firmware version, web version, plugin version, number of channels, number of alarm output, device capacity, etc.

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

You can view the device name, language, model, serial No., firmware version, web version, plugin version, number of channels, number of alarm output, device capacity, etc.

8.3.2 Set Time

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

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

Time Zone	(GMT+08:00) Beijing, Urumqi, Singapore, Perth ▾
Time Sync.	● NTP ○ Manual
Server Address	2.com
NTP Port	7
Interval	7 minute(s)

Save

Figure 8-2 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.

8.3.3 Set DST

Steps

1. Click **Configuration → System → System Settings → DST** .

Figure 8-3 DST Page

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

8.3.4 View Open Source Software License

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

8.3.5 Upgrade and Maintenance

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

Reboot Device

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

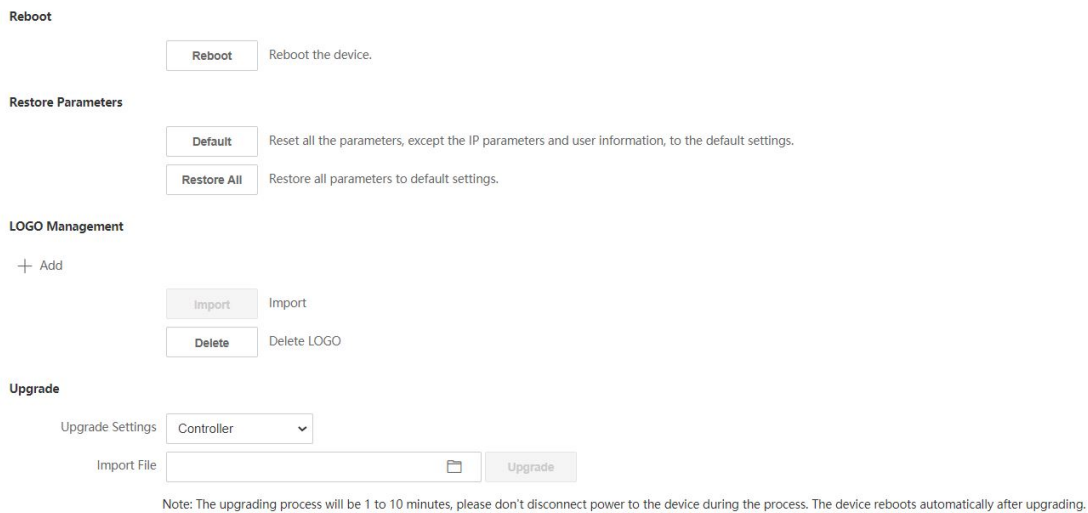**Figure 8-4 Upgrade and Maintenance Page**

Click **Reboot** to reboot the device.

Restore Parameters

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

Restore All

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

Default

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

Logo Management

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

Click ＋ to select a local image.

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

Click **Delete** to delete the logo image.

Note

The logo image shall be no larger than 100 kb with a resolution of 400 × 400. Refer to *__Logo Management__* for details.

Upgrade

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

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

ⓘNote

Do not power off during the upgrading.

8.3.6 Security Mode Settings

Set the security mode for logging in the client software.

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

Select a security mode from the drop-down list, and click **Save**.

Security Mode

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

Compatible Mode

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

Enable SSH

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

Enable HTTP

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

8.3.7 Change Administrator's Password

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

⚠️**Caution**

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

---

your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.

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

8.3.8 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.

8.3.9 Network Settings

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

⊞Note

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

Set Basic Network Parameters

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

Figure 8-5 TCP/IP Settings Page

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

DHCP

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

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

NIC Type

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

DNS Server

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

Set Port Parameters

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

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

HTTP

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

RTSP

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

HTTPS

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

Server

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

Set Wi-Fi Parameters

Set the Wi-Fi parameters for device wireless connection.

Steps

$\boxed{\mathbf{i}}$**Note**

The function should be supported by the device.

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

Figure 8-6 Wi-Fi Settings Page

2. Check **Wi-Fi**.

3. Select a Wi-Fi

- Click 🔗 of a Wi-Fi in the list and enter the Wi-Fi password.
- Click **Add** and enter a Wi-Fi's name, password, and encryption type. Click **Connect**. When the Wi-Fi is connected, click **OK**.

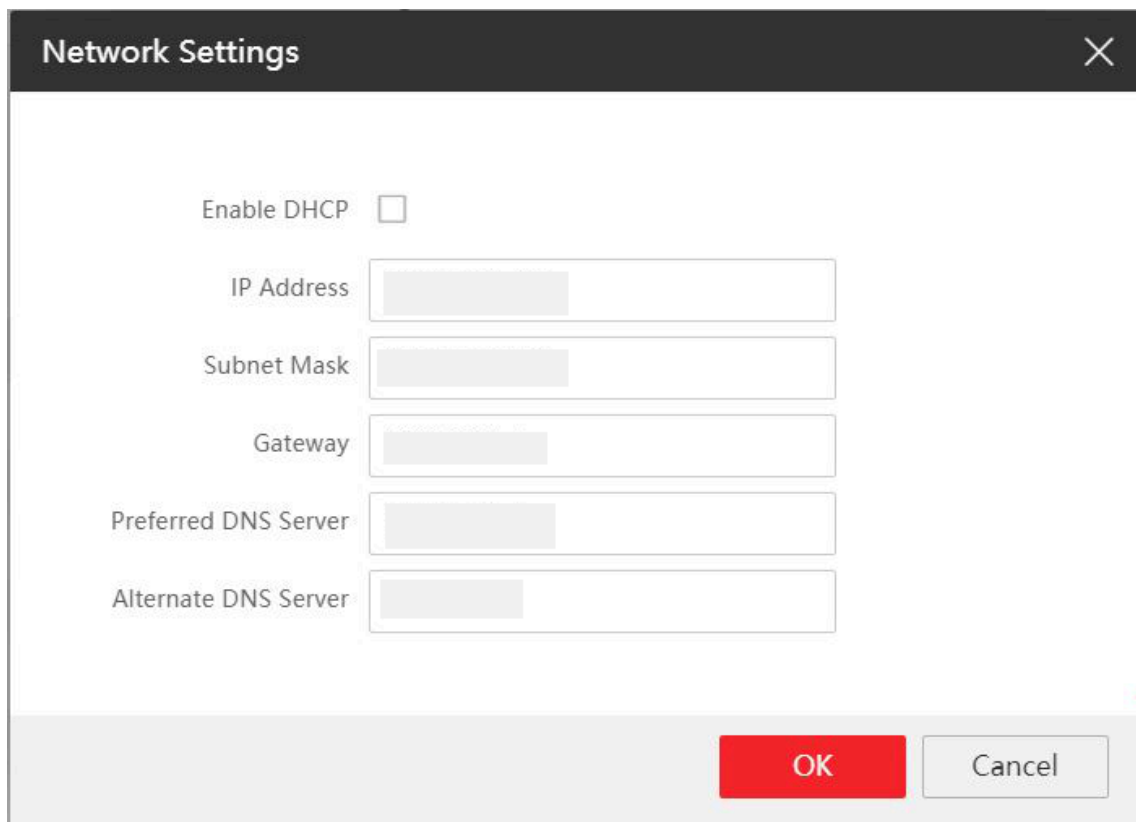**4. Optional:** Set the WLAN parameters.

1) Click **Network Settings**.

Figure 8-7 WLAN Settings

    2) Set the IP address, subnet mask, and default gateway. Or check **Enable DHCP** and the system
        will allocate the IP address, subnet mask, and default gateway automatically.

5. Click **Save**.

8.3.10 Set Audio Parameters

Set the image quality, resolution, and the device volume.

Set Audio Parameters

Click **Configuration → Video/Audio → Audio** .
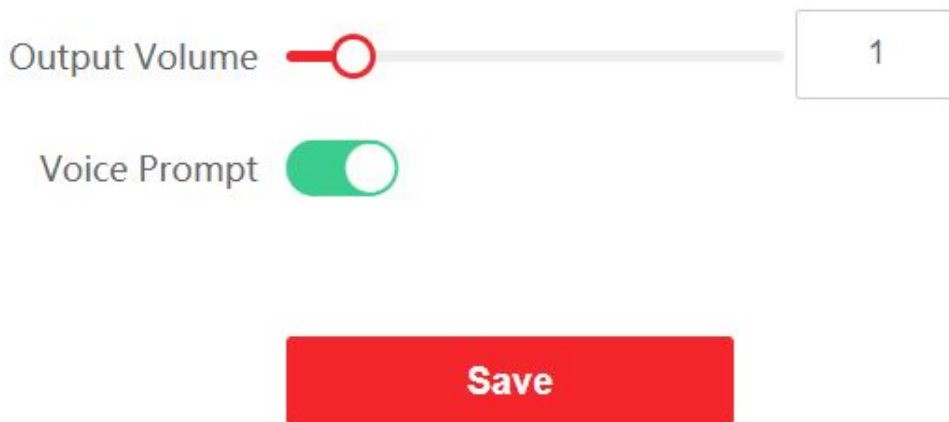
Figure 8-8 Set Audio Parameters

Drag the block to adjust the output volume.

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

You can also enable **Voice Prompt**.

Ⓘ**Note**

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

8.3.11 Set Image Parameters

Set brightness, contrast, saturation and hue parameters.

Steps

1. Click **Configuration → Image** .

2. Configure the parameters to adjust the image.

Brightness

Drag the block or enter the value to adjust the live video's brightness. The value of brightness is set 64 by default.

Contrast

Drag the block or enter the value to adjust the live video's contrast. The value of contrast is set 32 by default.

Saturation

Drag the block or enter the value to adjust the live video's saturation. The value of saturation is set 64 by default.

Hue

Drag the block or enter the value to adjust the live video's hue. The value of hue is set 48 by default.

Start/end recording video.

Capture the image.

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

8.3.12 Set Authentication Parameters

Click **Configuration → General → Authentication Settings** .

Note

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

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

Figure 8-9 Authentication Settings

Card Reader

Select **Main Card Reader**.

Note

Main Card Reader: you can configure the device card reader's parameters.

Enable Card Reader

Enable the card reader's function.

Recognition Interval

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

8.3.13 Temperature Measurement Settings
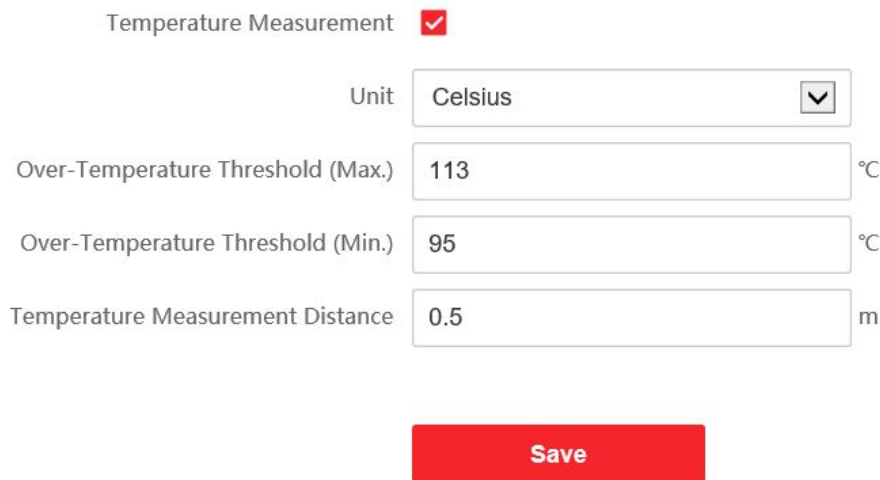
You can set the temperature measurement parameters, including unit, Max. temperature, Min. temperature and temperature measurement distance.

Steps

ⓘ**Note**

Only devices with temperature measurement function supports the settings.

1. Click **Configuration → Temperature → Temperature Settings** .

Figure 8-10 Temperature Measurement Settings

2. Enable **Temperature Measurement**.

3. Configure the temperature measurement parameters.

Unit

Select a temperature unit according to your preference.

Over-Temperature Alarm Threshold (Max./Min.)

Configure the limit for temperature measurement result. Device will alarm when the visitor's temperature exceeds or does not reach the threshold. The max. value is 37.3 ℃ and the min. value is 35 ℃ by default.

Temperature Measurement Distance

Edit the distance according to actual situation. The person needs to approach within the set value to trigger the temperature measurement.
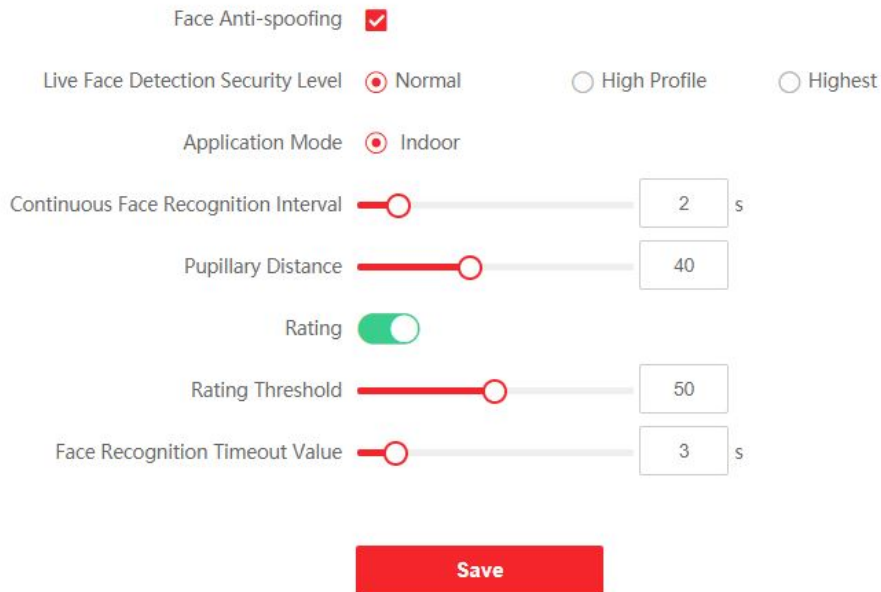
4. Click **Save**.

8.3.14 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 8-11 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 100% applicable to anti-spoofing environments. If you require a higher security level, use multiple authentication modes.

Live Face Detection Security Level

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

Application Mode

Select either others or indoor according to actual environment.

Continuous Face Recognition Interval

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

Pupillary Distance

Set the pupillary distance when starting face authentication.

Rating

Enable rating to start rating for face authentication.

Rating Threshold

Set the rating threshold when authenticating. 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.

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.
Click **Save** to save the settings.
Click or to record videos or capture pictures.

8.3.15 Visitor Settings

Logo Management

Set a logo to show in the top left corner.

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

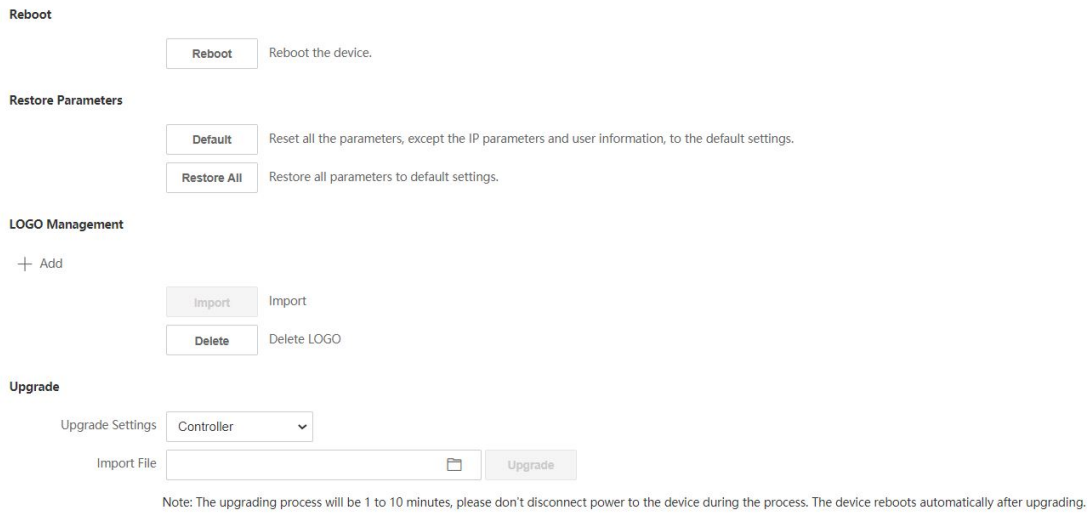**Figure 8-12 Logo Management**

2. Click $+$ to add a local image.

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

![i]**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.

Set Visitor Basic Information

Set visitor basic information.

Click **Configuration → Visitor → Basic Parameter** .

Figure 8-13 Visitor Basic Parameters

Configure parameters and click **Save**.

Manually Enter Visitor Information

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

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 Check-out

The system will auto check out all visitors at 24 o'clock every day 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.

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.

Allow Non-Reserved Check In

When the function is enabled, visitors without appointment are allowed to check-in on site.

Skip Person and ID Comparison

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

Visitor Code Length

Choose 4 or 6 character digits according to actual needs.

$\boxed{i}$**Note**

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

Auto Sync. Visitor Information

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

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.

Visitor Reservation

Enable the function to allow visitor reservation via platform.

Custom Item List 1/2/3

Set custom information for visitor check-in.

Set Check In Information

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

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

Check In Information List

No.	Information	Required	Display
01	ID Card No.	✓	✓
02	Phone Number	✓	✓
03	License Plate No.	✓	✓
04	Arrival Time	✓	✓
05	Receptionist	✓	✓
06	Personal Belongings	✓	✓
07	Visiting Reason	✓	✓
08	Remarks	✓	✓
09	Visitor Name	✓	✓
10	Visitor Gender	✓	✓
11	Visitor ID Type	✓	✓
12	Visitor Company	✓	✓
13	Visiting Area	✓	✓
14	Custom Item List1	✓	✓
15	Custom Item List2	✓	✓
16	Custom Item List3	✓	✓
17	Visitor Address	✓	✓
18	Visitor Temperature	✓	✓
19	Visitor Leave Time	✓	✓
20	Reception Department	✓	✓
21	Email	✓	✓

Save

Figure 8-14 Visitor Check In Settings

Select the visitor information items as required at the **Required** column.

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

Click **Save**.

Set Printing Receipt Information

Select items to be printed on the receipt.

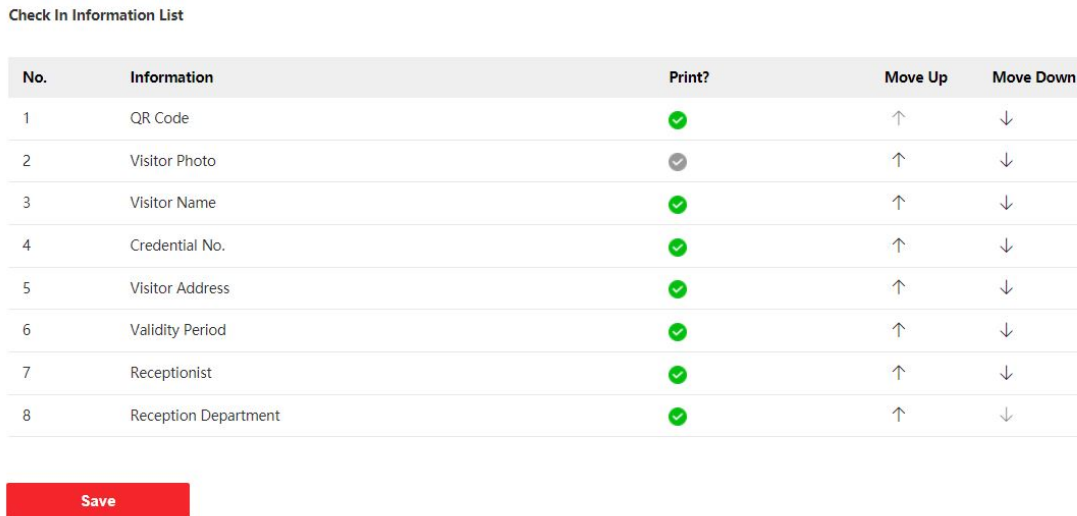Click **Configuration → Visitor → Printing Receipt Settings** .

Check In Information List

No.	Information	Print?	Move Up	Move Down
1	QR Code	✓	↑	↓
2	Visitor Photo	✓	↑	↓
3	Visitor Name	✓	↑	↓
4	Credential No.	✓	↑	↓
5	Visitor Address	✓	↑	↓
6	Validity Period	✓	↑	↓
7	Receptionist	✓	↑	↓
8	Reception Department	✓	↑	↓

Save

Figure 8-15 Printing Receipt Settings

Select the information items to be printed at the **Print** column.
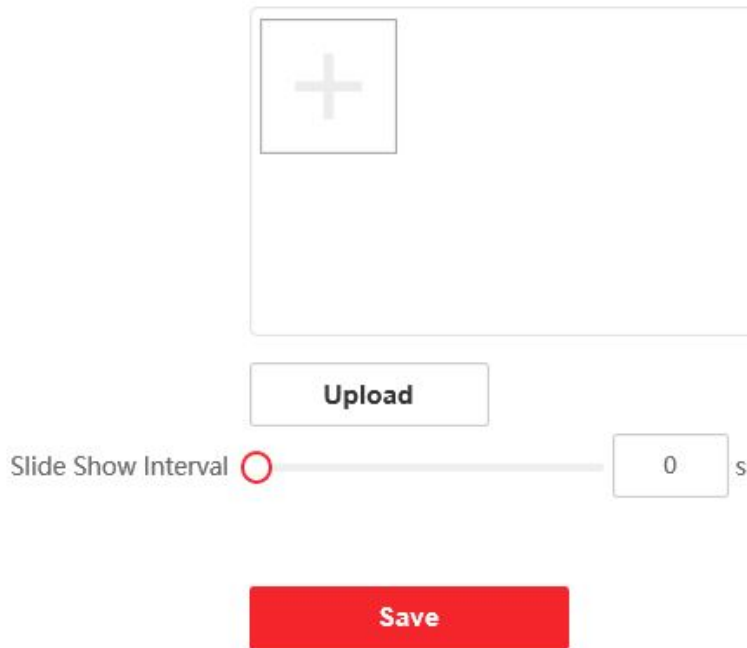
Click ↑ or ↓ to move the item position printed on the receipt.

8.3.16 Set Screen Saver Picture

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

Click **Configuration → Notice Publication** .

Figure 8-16 Notice Page

Screen Saver Picture

Click + to add a local picture.

Ⓘ**Note**

Only JPG and MP4 format are allowed. No more than 10 pictures can be added.

Click **Upload**.

Slide Show Interval

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

Click **Save** to save the configurations.

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.
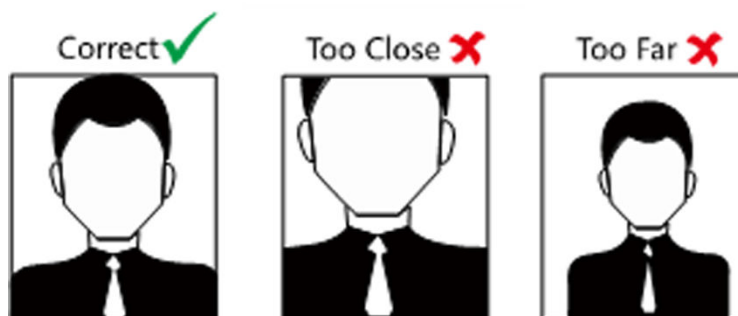- Do not make your hair cover your eyes, ears, etc. and heavy makeup is not allowed.

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

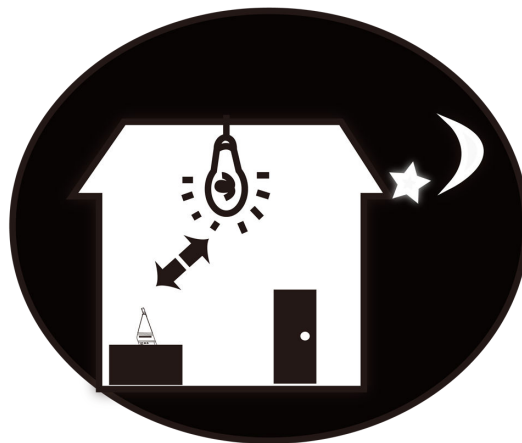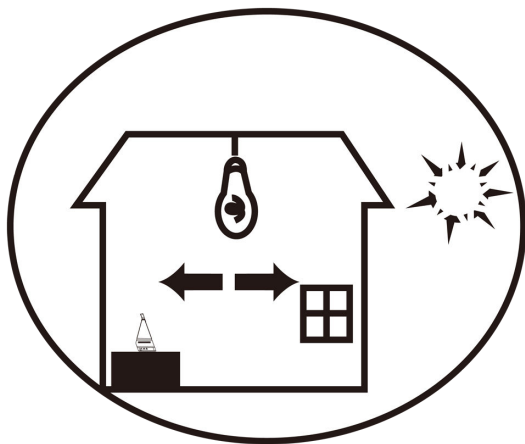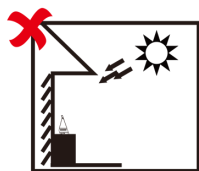1. Light Source Illumination Reference Value

Candle: 10Lux
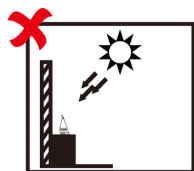
Bulb: 100~850Lux

Sunlight: More than 1200Lux

2. Install the device at least 2 meters away from the light, and at least 3 meters away from the window or door.
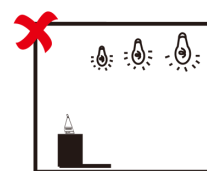
3.Avoid backlight, direct and indirect sunlight

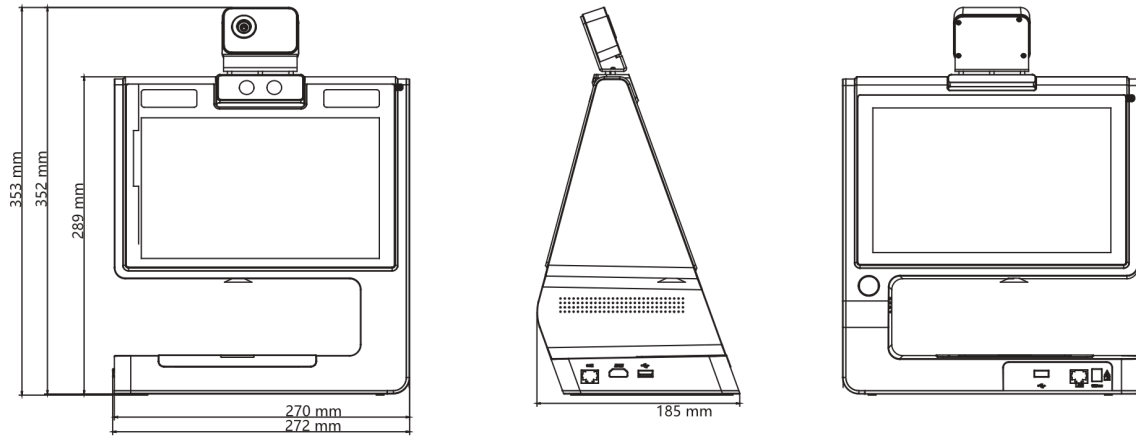Backlight   Direct Sunlight   Direct Sunlight   Indirect Sunlight   Close to Light
                                        through Window   through Window

Appendix C. Dimension

353 mm
352 mm
289 mm

270 mm
272 mm

185 mm

Appendix D. Communication Matrix and Device Command

Communication Matrix

Scan the following QR code to get the device communication matrix.
Note that the matrix contains all communication ports of Hikvision access control and video intercom devices.

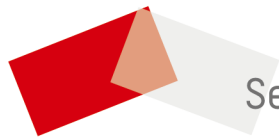**Figure D-1 QR Code of Communication Matrix**

Device Command

Scan the following QR code to get the device common serial port commands.
Note that the command list contains all commonly used serial ports commands for all Hikvision access control and video intercom devices.

Figure D-2 Device Command

See Far, Go Further

UD20494B-A