



DS-K5032-3XFD Visitor Terminal

User Manual

Legal Information

©2020 Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

About this Manual

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

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

Trademarks

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

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

Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS MANUAL AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED “AS IS” AND “WITH ALL FAULTS AND ERRORS”. HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.

YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR

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

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

Data Protection

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

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

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:

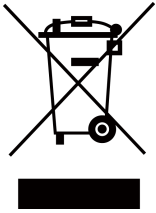
1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

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
1.1 Overview	1
1.2 Main Features	1
Chapter 2 Appearance	2
Chapter 3 Installation	4
3.1 Installation Environment	4
3.2 Installation	4
Chapter 4 Wiring	5
Chapter 5 Basic Operation	6
5.1 First Time Use	6
5.1.1 Create Administrator Account	6
5.1.2 Connect to HikCentral Professional (Optional)	7
5.2 Login	9
5.3 Visitor Registration	10
5.4 Visitor Check-Out	12
5.5 View Visitor Details	13
5.6 Export Visitor Information	13
5.7 System Settings	14
Appendix A. Tips When Collecting/Comparing Face Picture	18
Appendix B. Tips for Installation Environment	19
Appendix C. Dimension	20
Appendix D. Communication Matrix and Device Command	21

Chapter 1 Overview

1.1 Overview

The visitor terminal is a kind of access control device for face recognition and visitor management, integrated with temperature screening function, which is mainly applied in security access control systems, such as 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 1.5 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 130,000 visitor records can be stored on the device.

Chapter 2 Appearance

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

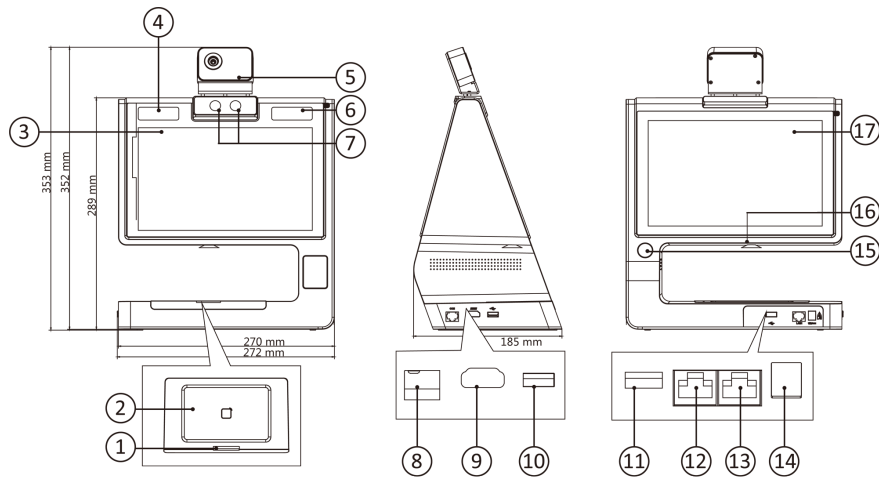




Figure 2-1 Visitor Terminal Diagram

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)  Note Supports the USB import function. You can use the interface to upload the event to the client software, etc.
11	USB 2.0

No.	Description
	 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.



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:

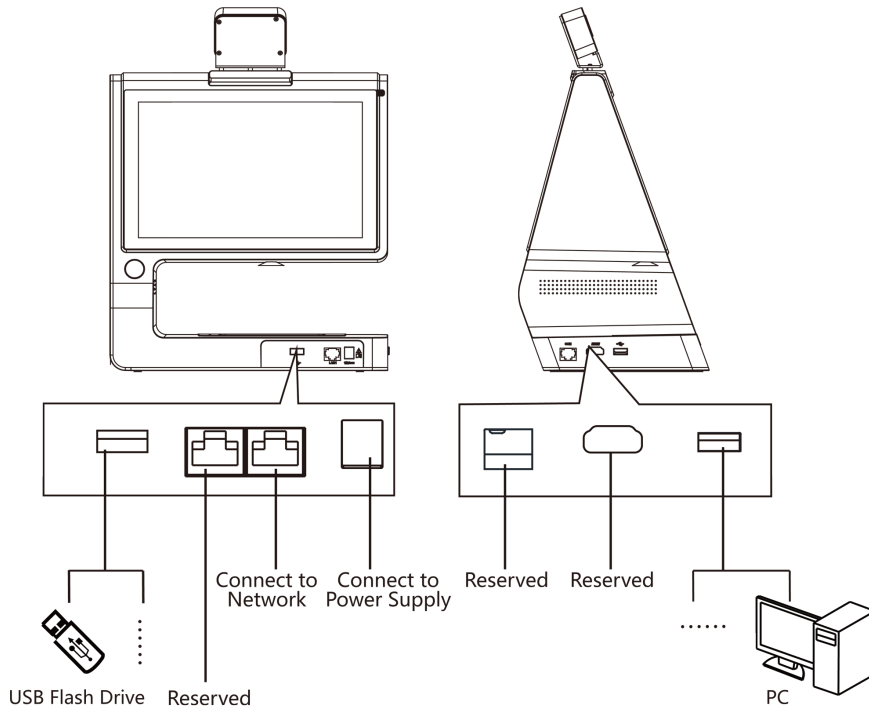


Figure 4-1 Wiring Diagram

Chapter 5 Basic Operation

5.1 First Time Use

For the first time use of the visitor terminal, you should create an administrator account. The password of the account is used for authorizing the skipping of person and ID comparison on a self-service visitor terminal; And it is recommended that you set network parameters to connect the visitor terminal to the HikCentral Professional system to allow data sharing between them.

5.1.1 Create Administrator Account

For the first time login, you should create an administrator account first before you can do further operations.

Steps



The password of the account can be used for authorizing the skipping of person and ID comparison on a self-service visitor terminal. For details, see .

1. Start the visitor terminal.

The account registration page will be displayed on the screen of the visitor terminal.

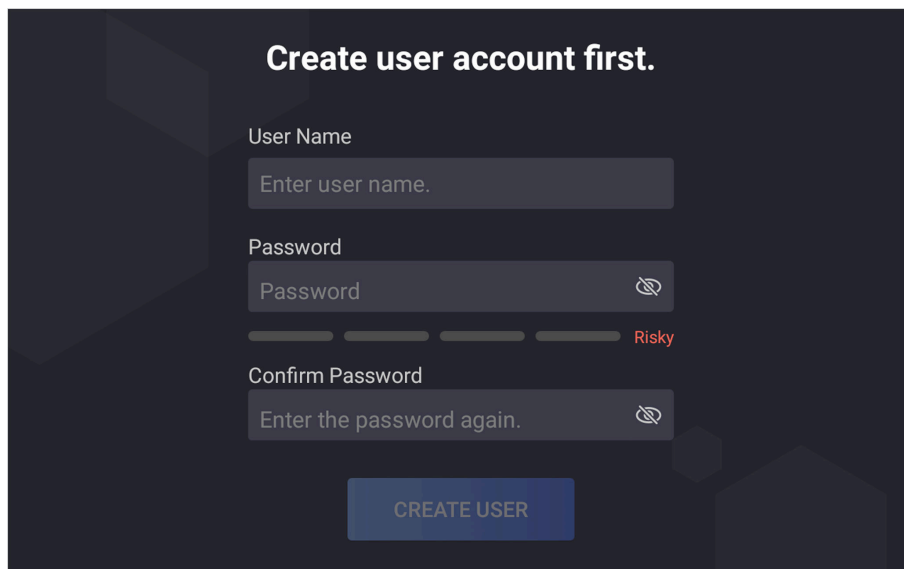


Figure 5-1 Registration

- 2.** Create a user name for the administrator account of the visitor terminal.
3. Create a password for the administrator account.

 **Note**

The password should contain 8 to 16 characters with the combination of at least two of the followings: digits, letters, and special characters

 **Note**

We highly recommend you to create a strong 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.

4. Enter the password again in the Confirm Password field to confirm the password.
5. Tap **Create User** to create the administrator account.
6. **Optional:** Connect the visitor terminal to the HikCentral Professional system.

 **Note**


For details, see **Connect to HikCentral Professional (Optional)** .

5.1.2 Connect to HikCentral Professional (Optional)

You can connect the visitor terminal to the HikCentral Professional system. After that, the visitor terminal and the HikCentral Professional system will be able to transmit data with each other. This allows you to use more functions to manage visitors.

Table 5-1 Main Functionality Differences between a Connected Visitor Terminal and a Disconnected One

Functionality	Connected to HikCentral Professional	Disconnected
Visitor Access Permission	On a staff-service visitor terminal, you can set person group and access group for the visitors to define access levels for them. On a self-service visitor terminal, the person group and access group are set by default. The visitor is not allowed to change the settings.	The person group settings and access group settings are not available.
Access by Facial Comparison	If the profile photo of the visitor is uploaded and access group is set, the visitor is allowed to access the specified doors and floors by face comparison after registration.	No matter the profile photo of the visitor is uploaded and access group is set or not, the visitor is not allowed to access doors and floors after registration.

Functionality	Connected to HikCentral Professional	Disconnected
Access by Card	<p>On a staff-service terminal, you can issue cards for visitors. After that, the visitor can access doors and floors using the card.</p> <p> Note Card is not supported by self-service visitor terminal.</p>	On a staff-service terminal, issuing cards for visitors is not available.
License Plate Number	License plate number can be set during visitor registration.	Setting license plate number is not supported.
Visitee	Visitee can be set during visitor registration.	Setting Visitee is not supported.
Extended Open Duration	Extended Open Duration can be set during visitor registration.	Setting Extended Open Duration is not supported.

After you create the administrator account, a window will pop up to remind you to configure network.

You can tap **Platform Access** on the window to enter the Platform Access page, and then set the parameters including IP address, port number, user name, and password, etc.

Use HTTPS

If the HikCentral Professional system uses HTTPS protocol, enable this parameter. If not, disable it.

IP

Enter the IP address of the HikCentral Professional system.

Port

Enter the port No. of the HikCentral Professional system.

User Name

Enter the user name of the administrator account of the visitor terminal.

Password

Enter the password of the administrator account of the visitor terminal.

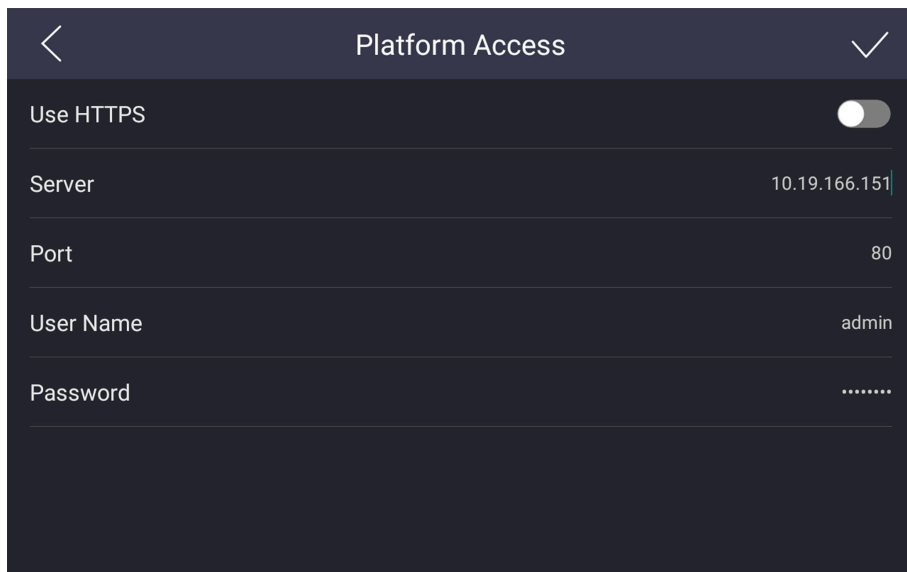



Figure 5-2 Platform Access Page

You can also tap **Later** to enter the Home page directly. If you want to configure network later, you can tap  on the upper-left corner of the Home page, and then select **Network Settings** → **Platform Access** to connect the visitor terminal to the HikCentral Professional system. For details, see *System Settings* .

5.2 Login

You can log in to the visitor terminal as an administrator. You can also use a HikCentral Professional account to log in to the visitor terminal if the visitor terminal is connected to the HikCentral Professional system.

Note

- For details about connecting the visitor terminal to the HikCentral Professional system, see *Connect to HikCentral Professional (Optional)* .
- If you want to log in to the visitor terminal using a HikCentral Professional account, make sure that you have the permission to access the Visitor module of HikCentral Professional, and that you have connected the visitor terminal to the HikCentral Professional system.

After entering user name and password, you can click **Login** to log in to the visitor terminal.

Note

You can turn on **Remember Password** and **Auto Login** to let the visitor terminal remember the password and log in automatically afterwards.

5.3 Visitor Registration

On a staff-service visitor terminal, visitors are not allowed to register by herself/himself. The reception personnel or other similar staff needs to operate on the visitor terminal to register the visitors.

Steps

1. Tap **Register** on the home page to start registering the visitor.

You enter the Person and ID comparison page.

2. Let the visitor position her/his face in front of the camera of the visitor terminal, and then tap **Capture** when the face image is clear.

Note

- You can tap **Skip** at the upper-right corner of the page to skip person and ID comparison. It is recommended that you do person and ID comparison to prevent identity theft.
- Based on the visitor terminal settings, the **Skip** button may not appear on the Person and ID comparison page. For details about visitor terminal settings, see **System Settings** .

The system will compare your currently-captured face picture with the face picture on your ID, and then display the comparison result. If the two pictures match, you enter the Visitor Information page.

Note

If person and ID comparison is disabled, the system will not do the comparison. For details about enabling/disabling person and ID comparison, see **System Settings** .

3. Set visitor information.

Note

You can define the required visitor information. For details, see **System Settings** .

Visitor Group

Select a visitor group for the visitor.

Latest Time for Check-Out

The latest allowed time point for the visitor to check out.

Valid Times for Visit

The maximum times a visitor can enter and exit a specified area via QR code authentication (QR code here refers to the QR code on visitor pass). For example, assume that you enter 5 as the valid times and define the door of the news release room as the door that the visitor can access, the visitor can enter/exit the door(s) by scanning the QR code on visitor pass for 5 times at most.

Access Group

Access group is a group of persons who have the same access permissions for a group of doors and floors. You can select access group(s) for the visitor to define the doors and floors that she/he can access during the same authorized time period.

 **Note**

- Make sure you have connected the visitor terminal to the HikCentral Professional system, or setting the parameter will be unavailable.
 - For details about setting access group, see *HikCentral Professional Web Client User Manual*.
-

Extended Open Duration

The time interval between the door is unlocked and locked again for the person whose extended access function enabled.

 **Note**

The parameter is only available if the visitor terminal is connected to the HikCentral Professional system. For details about connecting visitor terminal to the system, see ***Connect to HikCentral Professional (Optional)***.

Card

Swipe the card on the card swiping area to enroll a card for the visitor. After that, you can give the card to the visitor as a credential for accessing specified doors and floors.

 **Note**

- Make sure you have select card as the allowed visitor credential, or the parameter will be unavailable For details about setting allowed visitor credentials, see ***System Settings***.
 - The parameter is only available if the visitor terminal is connected to the HikCentral Professional system. For details about connecting visitor terminal to the system, see ***Connect to HikCentral Professional (Optional)***.
-

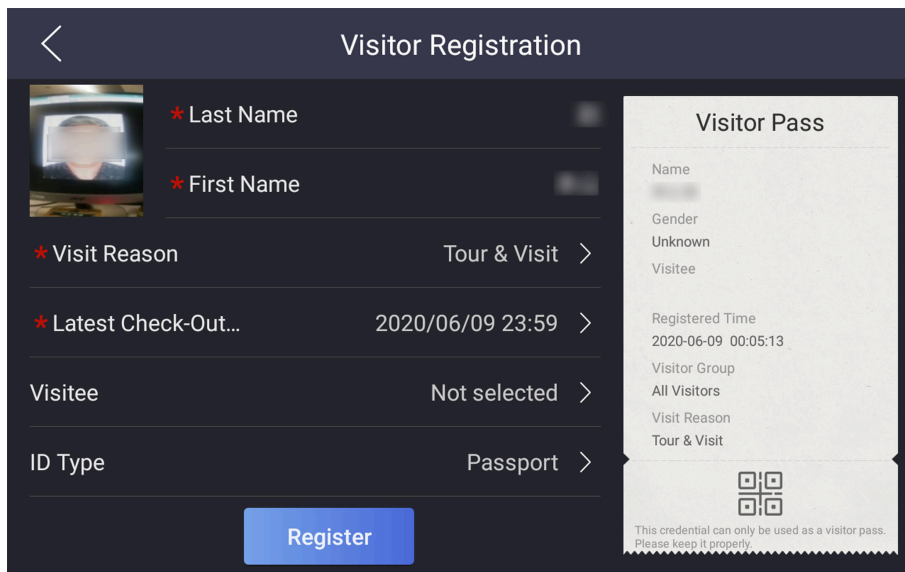


Figure 5-3 Visitor Registration

4. Tap **Register to complete registration.**


If you have selected visitor pass as the allowed visitor credential, a visitor pass will be printed. The visitor can access the doors and floors in the specified area by scanning the QR code on the scanner at the access points (i.e., doors and floors).

Note


For details about setting allowed visitor credentials, see **System Settings** .

5.4 Visitor Check-Out

For a staff-service visitor terminal, the visitors cannot check out by herself/himself. Only the reception personnel and similar staff can check out the visitors.

You can tap  in the Operation column of the visitor list to manually check out a visitor, or select a visitor form the visitor list, and then tap **Check out** to check out the visitor.

You can also place the passport, visitor pass onto the scanning area of the terminal, or swipe card to check out the visitor.


If there are large amount of registered visitors, you can tap  and then set filter conditions such as name and phone number to filter the visitors.

Note

If a visitor has not been checked out until the **Latest Time for Check-Out**, the visitor will be checked out automatically.


5.5 View Visitor Details

For a staff-service visitor terminal, once a visitor registration completes, a visitor record will be displayed on the visitor list. And the total number of visitors on the current day, the number of the checked-out visitors, and the number of visitors who haven't been checked out will be displayed. You can also view visitor details, including visatee, visit reason, latest check-out time, valid times for visit, access group, and skin-surface temperature (if temperature screening is supported), etc.

You can tap  in the Operation column of the visitor list to view the visitor details. If the visitor has been checked out, you can tap **Register Again** on the visitor details page to register her/him again if required.

Note

For details about visitor registration, see **Visitor Registration** .

If there are large amount of registered visitors, you can tap  and then set filter conditions such as name and phone number to filter the visitors.

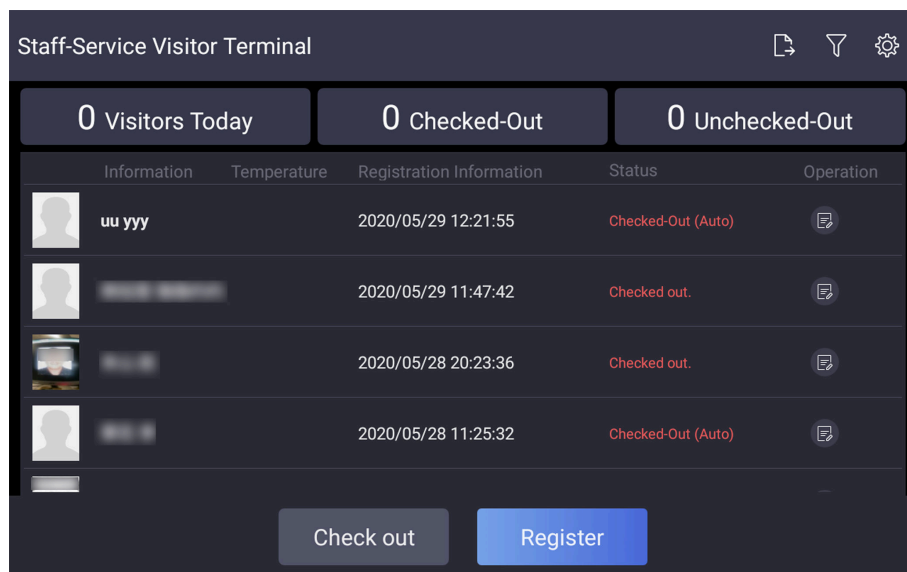


Figure 5-4 Visitor List


5.6 Export Visitor Information

For a staff-service visitor terminal, you can export the visitor information acquired by it to a USB flash disk as an encrypted file.

Before You Start


- Make sure you have plugged a USB flash disk to the visitor terminal.
- Make sure at least a visitor has been registered on the visitor terminal.

Steps

1. Tap  in the upper-right corner of the home page.
The Encrypted Exportation window pops up.
2. Create a password to encrypt the to-be-exported file, and then confirm it.
3. Tap **Export**, and then select directory to export the visitor information to the USB flash disk.

5.7 System Settings

You can configure system settings for the visitor terminal, such as person and ID comparison, visitor credential type, and network settings.

Tap  in the upper-right corner of the visitor terminal's home page to enter the system settings page.

Note

For self-service visitor terminal, you are required to authenticate your identity as the administrator first. In this case, enter the administrator password to authenticate.

Language

Switch system language.

Time

Set time zone and current time for the visitor terminal.

Time Zone

Select the time zone where the visitor terminal locates.

Current Time

Set the current time for the visitor terminal.

Person and ID Comparison

If enabled, the visitors are required to capture a face picture via the visitor terminal at the beginning of registration. After that, the system will compare the face picture with the profile picture on the scanned ID (e.g., passport). In this way, using fake ID for registration will be prevented.

Person and ID Comparison Threshold

Set the threshold (0 to 100) of similarity level for determining that the visitor's captured face picture and her/his ID photo match with each other. The higher the value, the stricter the facial comparison will be.

Note

It is recommended that you use the default value (60).

Allow Skipping Person and ID Comparison

If enabled, the visitor is allowed to skip person and ID comparison at the beginning of her/his registration.

Allow Skipping Person and ID Comparison/Temperature Screening

Note

The parameter is only available on the staff-service terminal that supports temperature screening.

If enabled, the visitor is allowed to skip person and ID comparison and temperature screening at the beginning of her/his registration.

Face Rating Threshold

Set a value to define the threshold to determine if the captured face picture is qualified. If the face rating of the captured face picture is lower than the threshold, the visitor terminal system will regard the capture as failed, and the visitor will be required to capture a face picture again.

Temperature Screening

Note

Temperature screening is only supported by certain models of the staff-service visitor terminal.

After enabled, the visitor terminal will measure the skin-surface temperatures of the visitors and highlight the abnormal temperatures in red during face data acquisition.

Temperature Alarm Threshold (Max.)

Set the maximum skin-surface temperature that is considered normal.

If the skin-surface temperature of a visitor is higher than the threshold, temperature alarm will be triggered (the abnormal temperature will be highlighted in red on the screen).

Temperature Alarm Threshold (Min.)

Set the minimum skin-surface temperature that is considered normal.

If the skin-surface temperature of a visitor is lower than the threshold, temperature alarm will be triggered (the abnormal temperature will be highlighted in red on the screen).

Max. Measurement Distance (m)

The maximum allowed distance (unit: m) between the visitor terminal and the visitor for measuring her/his skin-surface temperature. If the distance between them is longer than the configured value, temperature measurement may fail.

You should set the value according to the environment where the visitor terminal locates. For example, if the light condition is not sound, you can set a relatively shorter distance.

Visitor Credential

Note

The parameter is not supported on self-service visitor terminal. It is only available on staff-service visitor terminal.

Set the visitor credential allowed to be used as the pass in your company or organization. You can select card or visitor pass.

Card

The card is issued via HikCentral ProfessionalWeb Client. For details about issuing cards, see *HikCentral Professional Web Client User Manual*.



Note

Only when the visitor terminal is connected to the HikCentral Professional system, will the card be available to be used as a type of credential by the visitor. See **Connect to HikCentral Professional (Optional)** for details about connecting the visitor terminal to the system.

Visitor Pass

The visitor pass with a QR code will be printed by the visitor terminal once the visitor completes registration.

Required Visitor Information

Select ID No., phone number, and (or) visatee as the required visitor information which should be entered during visitor registration.

Use ID Photo as Profile

If enabled, the photo on the ID of the visitor will be used as her/his profile picture in the visitor terminal system and the HikCentral Professional system.

Network Settings

Wired Network

View the details of the connected wired network, such as the IP address of the wired network.

Wi-Fi

View available Wi-Fi addresses and connect the visitor terminal to one of them.

Platform Access

Set parameters to connect the visitor terminal to the HikCentral Professional system, thus allowing the data communication between the visitor terminal and the HikCentral Professional system.

The parameters includes HTTPS, IP address, port, user name, password, etc.

IP

Enter the IP address of the HikCentral Professional system.

Port

Enter the port No. of the HikCentral Professional system.

User Name

Enter the user name of the HikCentral Professional system.

Password

Enter the password of the HikCentral Professional account.

Visitor Privacy Settings

Set parameters related to visitor privacy.

Save and Display Captured Face Picture

After enabled, the captured face pictures of the visitors will be saved and displayed on visitor terminal.

Visitor Records Retention Period

Set the retention period for the registered visitor information. The visitor information will be deleted automatically when the retention period expires.

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.

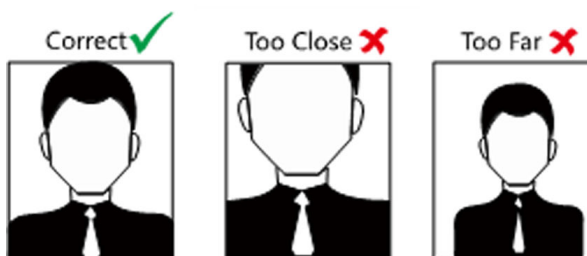
Posture

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

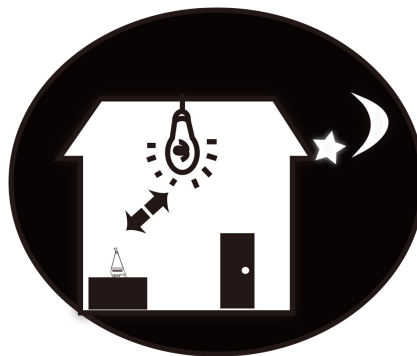
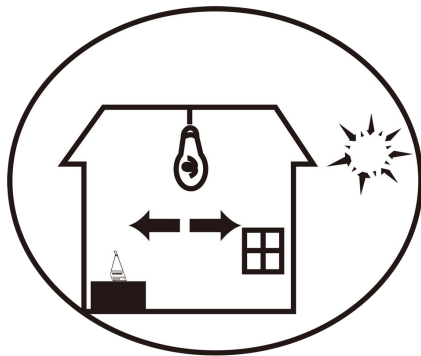


Bulb: 100~850Lux

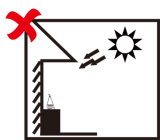


Sunlight: More than 1200Lux

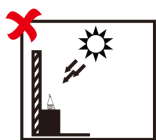
2. Install the device at least 2 meters away from the light, and at least 3 meters away from the window or door.



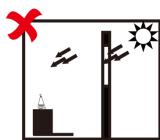
3. Avoid backlight, direct and indirect sunlight



Backlight



Direct Sunlight



Direct Sunlight through Window

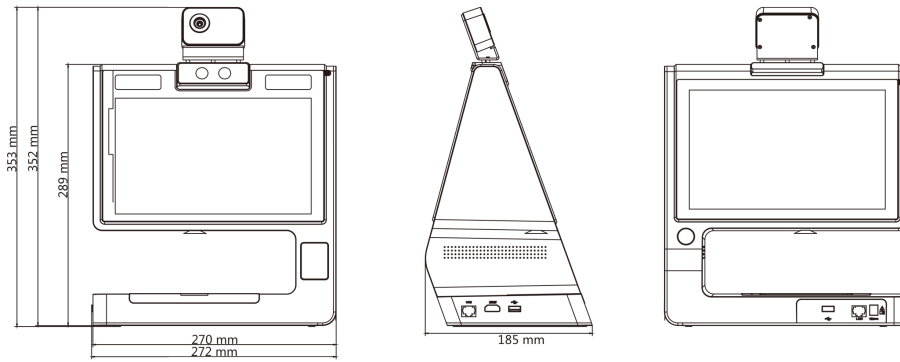


Indirect Sunlight through Window



Close to Light

Appendix C. Dimension



Appendix D. Communication Matrix and Device Command

Communication Matrix

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

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



Figure D-1 QR Code of Communication Matrix

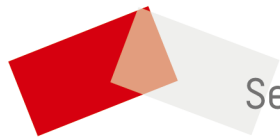
Device Command

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

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



Figure D-2 Device Command



See Far, Go Further