



DS-K1F600-D6E Series Enrollment Station

User Manual



Legal Information

User Manual

©2019 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/en/>).

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 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 INSPECTION, 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.

Available Model

| Product Name | Model | Description |
|--------------------|-----------------|---|
| Enrollment Station | DS-K1F600-D6E | Supports enroll face and card No. |
| | DS-K1F600-D6E-F | Supports enroll face, fingerprint, and card No. |

Use only power supplies listed in the user instructions:

| Model | Manufacturer | Standard |
|-----------------------------|--|----------|
| ADS-26FSG-12 12018EPB | SHENZHEN HONOR ELECTRONIC CO LTD | PB |
| ADS-26FSG-12 12018EPI-01 | SHENZHEN HONOR ELECTRONIC CO LTD | PI |
| ADS-26FSG-12 12018EPCU | SHENZHEN HONOR ELECTRONIC CO LTD | PCU |
| ADS-26FSG-12 120EPG | SHENZHEN HONOR ELECTRONIC CO LTD | PG |
| MSA-C1500IC12.0- 18P-BR | MOSO Power Supply Technology Co., Ltd | PBR |

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, the RoHS Directive 2011/65/EU



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

designated collection points. For more information see: www.recyclethis.info



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



Safety Instruction

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

The precaution measure is divided into Dangers and Cautions:

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

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

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

Danger:

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

Cautions:

- Do not drop the device or subject it to physical shock, and do not expose it to high electromagnetism radiation. Avoid the

equipment installation on vibrations surface or places subject to shock (ignorance can cause equipment damage).

- Do not place the device in extremely hot (refer to the specification of the device for the detailed operating temperature), cold, dusty or damp locations, and do not expose it to high electromagnetic radiation.
- The device cover for indoor use shall be kept from rain and moisture.
- Exposing the equipment to direct sun light, low ventilation or heat source such as heater or radiator is forbidden (ignorance can cause fire danger).
- Do not aim the device at the sun or extra bright places. A blooming or smear may occur otherwise (which is not a malfunction however), and affecting the endurance of sensor at the same time.
- Please use the provided glove when open up the device cover, avoid direct contact with the device cover, because the acidic sweat of the fingers may erode the surface coating of the device cover.
- Please use a soft and dry cloth when clean inside and outside surfaces of the device cover, do not use alkaline detergents.
- Please keep all wrappers after unpack them for future use. In case of any failure occurred, you need to return the device to the factory with the original wrapper. Transportation without the original wrapper may result in damage on the device and lead to additional costs.
- Improper use or replacement of the battery may result in hazard of explosion. Replace with the same or equivalent type only. Dispose of used batteries according to the instructions provided by the battery manufacturer.
- Biometric recognition products are not completely applicable to anti-spoofing environments. If you require a higher security level, use multiple authentication modes.
- Input voltage should meet both the SELV (Safety Extra Low Voltage) and the Limited Power Source with 100~240 VAC or 12 VDC according to the IEC60950-1 standard. Please refer to technical specifications for detailed information.
- Please take care of your card and report card loss in time when card is lost.
- Multiple card types are supported. Please select an appropriate card type according to the card performance and the usage scenarios.
- Working temperature: -10 °C to 50 °C (14 °F to 122 °F)

Contents

| | |
|---|-----------|
| 1 Overview | 1 |
| 2 Appearance | 1 |
| 3 Activation | 2 |
| 3.1 Activate via Device | 2 |
| 3.2 Activate via SADP | 3 |
| 4 Enroll Administrator's Face | 4 |
| 5 Enroll via Device | 4 |
| 5.1 Enroll Face via Device | 4 |
| 5.2 Enroll Fingerprint via Device | 5 |
| 5.3 Enroll Card via Device | 6 |
| 6 Enroll via Client Software | 7 |
| 6.1 Enroll Face via Client Software | 7 |
| 6.2 Enroll Fingerprint via Client Software | 9 |
| 6.3 Enroll Card via Client Software | 11 |
| 6.4 Get Person Information from Enrollment Station | 13 |
| 6.5 Import Person Information in Batch | 13 |
| 7 Basic Operation | 14 |
| 7.1 Login by Administrator | 14 |
| 7.2 Add Administrator | 14 |
| 7.3 Communication Settings | 15 |
| 7.4 Manage Enrollment | 16 |
| 7.5 Basic Settings | 17 |
| 7.5.1 Set Time | 17 |
| 7.5.2 Set Sound | 17 |
| 7.5.3 Set Enrollment Rule | 17 |
| 7.5.4 Other Settings | 18 |
| 7.5.5 Set Biometric Parameters | 19 |
| 7.6 Data Management | 20 |

| | |
|---|-----------|
| 7.6.1 Import User | 20 |
| 7.6.2 Export Enrolled Data | 21 |
| 7.6.3 Clear Enrolled Data | 21 |
| 7.7 System Maintenance | 22 |
| A. Tips When Collecting/Comparing Face Picture | 24 |
| B. Tips for Scanning Fingerprint | 25 |
| C. Communication Matrix and Device Command | 26 |

1 Overview

Introduction

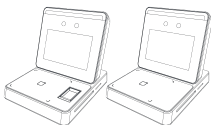


Figure 1-1 Product Appearance

The enrollment station can realize multiple user information's enrollment on one device. It supports enrolling face picture, fingerprint (parts of the device model support), 13.56 MHz IC card No., and 125KHz ID card No.

Features

- 3.97-inch LCD touch screen for face recognition, parameters configuration, live view, etc.
- 2 MP wide-angle dual-lens
- Face anti-spoofing
- Face recognition distance: 0.3 m to 1 m
- Deep learning algorithm
- Face recognition duration < 0.2 s/User; face recognition accuracy rate $\geq 99\%$
- 2,000 user capacity, 2,000 face capacity, 20,000 card capacity, and 20,000 fingerprint capacity
- Enrolls data via the device and transmits the data from the device to the platform via TCP/IP protocol. Enrolls data remotely via the client software
- Stand-alone operation
- Manage, search and set device data after logging in the device locally

2 Appearance

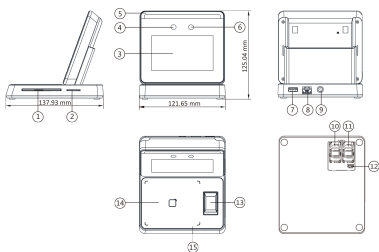


Figure 2-1 Appearance

Table 2-1 Appearance Description

| No. | Description |
|-----|----------------------------|
| 1 | PSAM3 Card Slot (Reserved) |
| 2 | PSAM4 Card Slot (Reserved) |
| 3 | Screen |
| 4 | Camera |
| 5 | Supplement Light |
| 6 | Camera |
| 7 | USB Interface |
| 8 | Network Interface |
| 9 | Power Interface |
| 10 | PSAM Card Slot (Reserved) |
| 11 | PSAM Card Slot (Reserved) |
| 12 | Debugging Port |
| 13 | Fingerprint Module |
| 14 | Card Presenting Area |
| 15 | Indicator |

3 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 (super administrator): admin

3.1 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 be activated.

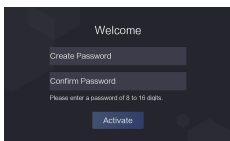


Figure 3-1 Activation Page



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

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

After activation, if you need to add the device to the client software or other platforms, you should edit the device IP address. For details, see *Communication Settings*.

3.2 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

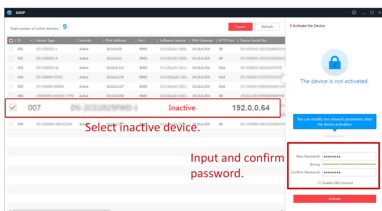
1. Run the SADP software and search the online devices.
2. Find and select your device in online device list.
3. Input new password (admin password) and confirm the password.



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.

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.

4 Enroll Administrator's Face

After activation, you should enroll an administrator's face for further operation. The administrator can login the device backend to manage and configure data.

Steps

1. After activation, tap **OK** on the pop-up window. You will enter the face enrollment page.

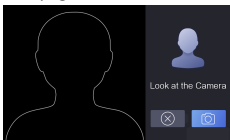



Figure 4-1 Face Enrollment Page

2. Enroll the administrator's face.

- 1) Tap  and follow the instructions to enroll the face.

Note

Make sure that the enrolling face is in face shaped area.

- 2) Tap  to exit the face enrollment page and back to the initial page.

Note

After logging in the device backend, you can enter the **Administrator** module to edit the administrator's information. For details, see **Add Administrator**.

5 Enroll via Device

5.1 Enroll Face via Device

Before You Start

- Power on and activate the device. For details about the activation, see **Activation**.
- Enable **Face Required** in **Set Enrollment Rule** after logging in the device backend.

Steps


1. Tap  on the initial page.
2. **Optional:** If you have added an administrator's face in **Add Administrator** and enabled **Verify by Administrator** in **Set Enrollment Rule**, you should verify the administrator's permission.






Figure 5-1 Authenticate Administrator Page

- Make sure the face is in the face recognition frame when authentication.



Note

For details about face recognition, see **Tips When Collecting/Comparing Face Picture**.

- Tap  on the right side and enter the administrator's name and password.
3. Enter the User Enrollment page.
 - Create an employee ID and tap **Add**
 - Present a card on the card presenting area.
 4. Enroll face.
 - 1) Tap  to enter the face enrollment page.
 - 2) Tap  and follow the instructions to enroll the face.


Note

Make sure that face is in the face recognition frame.

- 3) **Optional:** Tap  to enroll the face again.
- 4) Tap  to complete the face enrollment.

Note

For details about face recognition, see **Tips When Collecting/Comparing Face Picture**.

5. **Optional:** Tap  to edit the employee ID.

5.2 Enroll Fingerprint via Device

Before You Start

- Power on and activate the device. For details about the activation, see **Activation**.
- Set fingers in **Select Finger** in **Set Enrollment Rule** after logging in the device backend.

Steps


1. Tap  on the initial page.
2. **Optional:** If you have added an administrator's face in **Add Administrator** and enabled **Verify by Administrator** in **Set Enrollment Rule**, you should verify the administrator's permission.





Figure 5-2 Authenticate Administrator Page

- Make sure the face is in the face recognition frame when authentication.

Note


For details about face recognition, see **Tips When Collecting/Comparing Face Picture**.

- Tap  on the right side and enter the administrator's name and password.
3. Enter the User Enrollment page.
 - Create an employee ID and tap **Add**
 - Present a card on the card presenting area.
 4. Enroll fingerprint.
 - 1) Tap  to enter the Select Finger page.
 - 2) Select a finger on the Select Finger page.

Note

You can set fingers in **Set Enrollment Rule**.

- 3) Follow the instructions and press a finger on the fingerprint module.

If the fingerprint is enrolled, the enrolled fingerprint on Select Finger page will turn to blue.
 - 4) **Optional:** Tap the enrolled fingerprint (in blue) and tap **OK** in the dialogue box to clear the enrolled data and enroll a new fingerprint.
5. **Optional:** Tap  to edit the employee ID.

5.3 Enroll Card via Device

Before You Start

- Power on and activate the device. For details about the activation, see **Activation**.
- Set **Card Number per User** and **Card No. Length** in **Set Enrollment Rule** after logging in the device background.

Steps


1. Tap  on the initial page.
2. **Optional:** If you have added an administrator's face in **Add Administrator** and enabled **Verify by Administrator** in **Set Enrollment Rule**, you should verify the administrator's permission.






Figure 5-3 Authenticate Administrator Page

- Make sure the face is in the face recognition frame when authentication.

 **Note**

For details about face recognition, see *Tips When Collecting/Comparing Face Picture*.

- Tap  on the right side and enter the administrator's name and password.
- 3. Enroll card.**
- Present card on the card presenting area and tap **OK** in the dialogue box. Create an employee ID and tap **Next**.
 - Create an employee ID in the input box, and tap **Add** to enter the User Enrollment page. Tap  and present card on the card presenting area.
- 4. Optional:** Tap  to edit the employee ID.

6 Enroll via Client Software

6.1 Enroll Face via Client Software

Before You Start

- Download and install the client software on your computer before enrollment.
- Power on and activate the device. For details about the activation, see *Activation*.

Follow the steps below to enroll face.

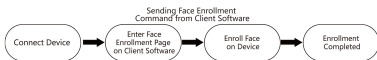


Figure 6-1 Flow Diagram of Enrolling Face

Steps

1. Connect the device to the network.
2. Place the device on the desk.
3. Login the client software on the computer.
4. Add an organization.
 - 1) Click **Person** to enter the Person page.
 - 2) Click **Add** on the upper left of the page.

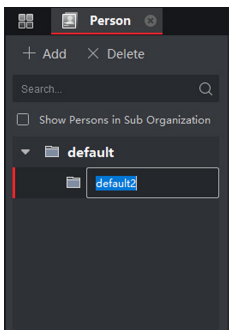


Figure 6-2 Add Organization

3) Create an organization name.

Note

Up to 10 levels of organizations can be added.

The added organizations will be displayed in the list on the left of the page.

5. Add person.

- 1) Select an organization from the list on the left.
- 2) Click **Add** on right panel.
- 3) Set the person's basic information, including the person's name, email, tel, effective period, and remark.

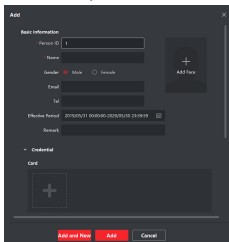



Figure 6-3 Add Person

Note

Once the person information is expired, the credentials and access control settings of the person will be invalid and the person will have no authorization to access the doors.

6. Enroll the face.

- 1) On the Add window, click **Add Face** → **Remote** .
- 2) Enable **Verify by Device** to check whether the device managed in the client can recognize the face in the photo.
- 3) Select the enrollment station from the drop-down list.
- 4) Click **Settings** and set the enrollment station's IP address, port No., user name and password.
- 5) **Optional:** Enable **Face Anti-Spoofing** function and set the liveness level according to your actual needs.

- 6) Click **OK**.
 - 7) Face the enrollment station's camera and capture a picture according to the instructions on the enrollment station.
 - 8) Click  to capture again.
 - 9) Click **OK**.
7. Confirm to add the person.
 - Click **Add** to add the person and close the Add Person window.
 - Click **Add and New** to add the person and continue to add other persons.

6.2 Enroll Fingerprint via Client Software

Before You Start

- Download and install the client software on your computer before enrollment.
- Power on and activate the device. For details about the activation, see **Activation**.

Follow the steps below to enroll fingerprint.

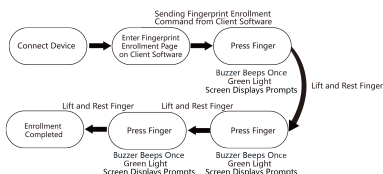


Figure 6-4 Flow Diagram of Enrolling Fingerprint

Steps

1. Connect the device to the network.
2. Place the device on the desk.
3. Login the client software on the computer.
4. Add an organization.
 - 1) Click **Person** to enter the Person page.
 - 2) Click **Add** on the upper left of the page.

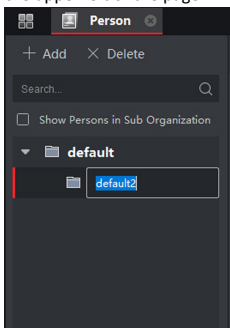


Figure 6-5 Add Organization

- 3) Create an organization name.

 **Note**

Up to 10 levels of organizations can be added.

The added organizations will be displayed in the list on the left of the page.

5. Add person.

- 1) Select an organization from the list on the left.
- 2) Click **Add** on right panel.
- 3) Set the person's basic information, including the person's **name**, email, tel, effective period, and remark.

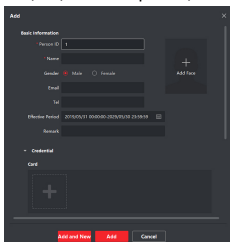


Figure 6-6 Add Person

 **Note**

Once the person information is expired, the credentials and access control settings of the person will be invalid and the person will have no authorization to access the doors.

6. On the Credential → Fingerprint panel, click +.

7. In the pop-up window, select the collection mode as Remote and select Enrollment Station as the fingerprint recorder from the drop-down list.

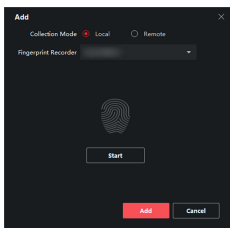


Figure 6-7 Add Fingerprint Page

8. Set the enrollment station's information.

- 1) Click **Settings** and set the enrollment station's IP address, port No., user name and password.
- 2) Click **OK**.

9. Enroll the fingerprint.

- 1) Click **Start** to start enrollment.
- 2) Follow the instructions on the enrollment station to enroll the fingerprint.
- 3) Click **Add** to save the enrollment.

10. Confirm to add the person.

- Click **Add** to add the person and close the Add Person window.
- Click **Add and New** to add the person and continue to add other persons.

6.3 Enroll Card via Client Software

Before You Start

- Download and install the client software on your computer before enrollment.
- Power on and activate the device. For details about the activation, see **Activation**.

Follow the steps below to enroll face.

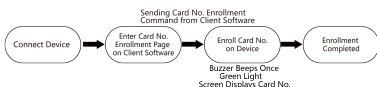


Figure 6-8 Flow Diagram of Enrolling Card

Steps

1. Connect the device to the network.
2. Place the device on the desk.
3. Login the client software on the computer.
4. Add an organization.
 - 1) Click **Person** to enter the Person page.
 - 2) Click **Add** on the upper left of the page.

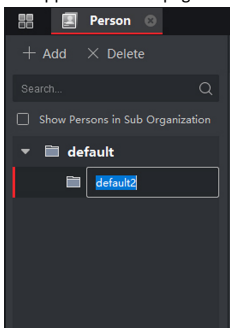


Figure 6-9 Add Organization

- 3) Create an organization name.

Note

Up to 10 levels of organizations can be added.

The added organizations will be displayed in the list on the left of the page.

5. Add person.

- 1) Select an organization from the list on the left.
- 2) Click **Add** on right panel.
- 3) Set the person's basic information, including the person's **name**, email, tel, effective period, and remark.

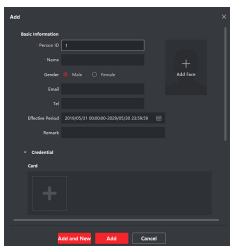


Figure 6-10 Add Person

 **Note**

Once the person information is expired, the credentials and access control settings of the person will be invalid and the person will have no authorization to access the doors.

6. On the Add window, click **Credential** → **Card** .

7. Add the card No.

- 1) Click + → **Settings** .
- 2) Set the mode as **Remote** and select the card enrollment station from the drop-down list.
- 3) Set the enrollment station's IP address, port No., user name and password.
- 4) Set the RF card type. The device can recognize the checked card type.
- 5) Click **OK**.

8. Enter the card No.

- Enter the card number manually.
- Place the card on the card enrollment station and click **Read** to get the card No. The card number will display in the Card No. field automatically.

9. Select the card type according to actual needs.

Normal Card

The card is used for opening doors for normal usage.

Duress Card

When the person is under duress, he/she can swipe the duress card to open the door. The door will be unlocked and the client will receive a duress event to notify the security personnel.

Patrol Card

This card is used for the inspection staff to check the their attendance of inspection. By swiping the card on the specified card reader, the person is marked as on duty of inspection at that time.

Dismiss Card

By swiping the card on the card reader, it can stop the buzzing of the card reader.

10. Click **Add**.

11. Confirm to add the person.

- Click **Add** to add the person and close the Add Person window.

- Click **Add and New** to add the person and continue to add other persons.


6.4 Get Person Information from Enrollment Station

You can get the person information from the device for further operations.

Steps



Note

- If the person name stored in the device is empty, the person name will be filled with the issued card No. after importing to the client.

 - If the card number or person ID (employee ID) stored on the device already exists in the client database, the person with this card number or person ID will not be imported to the client.
-

1. Enter **Person** module.
2. Select an organization to import the persons.
3. Click **Get from Device**.
4. Select **Enrollment Station** from the drop-down list.
5. Configure the enrollment station's information.
 - 1) Click **Settings**.
 - 2) Set the enrollment station's IP address, port, user name of the device administrator, and password.
 - 3) Click **OK**.
6. Click **Get** to start importing the person information to the client.

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

6.5 Import Person Information in Batch

You can import the persons information in batch.

Steps

1. Enter the **Person** module.
2. Select an organization to import the person.
3. Click **Get from Device**.
4. Select **Enrollment Station** from the drop-down list.
5. Configure the enrollment station's information.
 - 1) Click **Settings**.
 - 2) Set the enrollment station's IP address, port, user name of the device administrator, and password.
 - 3) Click **OK**.
6. Click **Export Template** and you can export the template to the PC.
7. Edit person's basic information and save.
8. Click **Import**. Select the file edited in Step 7.

The edited basic information will be imported to the client software.

What to do next

After the basic information is imported to the client software, you should enroll other information such as the face, fingerprint, etc. For details, see **Enroll via Client Software**.

7 Basic Operation

7.1 Login by Administrator

Login the device backend to set the device basic parameters. If an administrator is added to the device, you can login by verifying the administrator's permission.

Before You Start

Add an administrator and add a face picture for the administrator. For details, see **Add Administrator**.

Steps

1. Long tap on the initial page for 3 s to enter the administrator authentication page.



Figure 7-1 Authenticate Administrator Page

2. Authenticate the administrator's face to enter the home page.

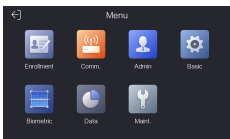




Figure 7-2 Home Page

Note

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

3. **Optional:** Tap  and you can enter the added admin user name and password to login.
4. **Optional:** Tap  and you can exit the page and be back to the initial page.

7.2 Add Administrator

The administrator can login the device backend and configure the device parameters.

Steps

1. Long tap on the initial page for 3 s and login the device home page.
2. Tap **Admin** to enter the Administrator page.

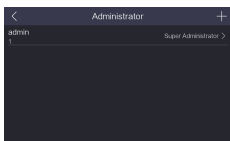



Figure 7-3 Administrator Page

3. Set the administrator's parameters.

- Edit the super administrator's parameters: Tap **admin** and edit the super administrator's face and password.
- Add a new administrator: Tap  and set the administrator's type, add face and password.

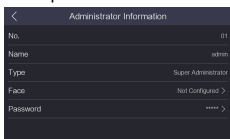



Figure 7-4 Administrator Information Page

Super Administrator

Contains all management and operation permissions.

Normal Administrator

Supports enrollment management and communication management. During remote configuration, the normal administrator can only gain parameters.

4. Tap  to save the settings.

 **Note**

- By default, the system contains a super administrator (admin). You cannot edit its No., name, and type. and you cannot delete it.
 - The admin user has higher permission level than other administrators.
 - The administrator's No. and name cannot be edited on the device. You should authenticate the administrator before editing the other administrator's information.
 - Up to 5 administrators can be added.
 - The face of the super administrator and normal administrator cannot be the same.
-

7.3 Communication Settings

Set the device wired network and wireless network.

Set Wired Network Parameters

Make sure the device has connected the Ethernet.

Long tap on the initial page for 3 s and login the home page. Tap **Comm. → Wired Network** .



Figure 7-5 Set Wired Network

Set the device IP address, subnet mask, and gateway.

Set Wireless Network Parameters


The device can connect to the Ethernet via wireless connection.


Long tap on the initial page for 3 s and login the home page. Tap **Comm.** → **Wi-Fi**.



Figure 7-6 Wi-Fi Page

After enabling **WLAN**, you should select a Wi-Fi for connection.

Select a Wi-Fi and enable **DHCP** and enter the Wi-Fi's password to connect. Tap  to connect the Wi-Fi.

Or disable the **DHCP** function, and enter the Wi-Fi's password, IP address, subnet mask, and gateway. Tap  to connect the Wi-Fi.

Tap  to disconnect the Wi-Fi.

7.4 Manage Enrollment

You can view the enrolled person information and delete the enrolled data.

Steps

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



Figure 7-7 Enrollment Management Page


2. You can view all enrolled person's information on this page.

3. You can also perform the following operations.

Incomplete

Tap **Incomplete** and the system will list the persons which have not enrolled all data.

View Details

Tap a person in the list to view details. Tap  to delete the person and all enrolled data.

Face/ Fingerprint/ Card

Tap a person in the list to enter the User Information page. You can delete the enrolled data according to actual requirements.

 **Note**

Only parts of the device models support fingerprint recognition function. Refer to the actual page for details.

Search

Enter a person's employee ID and tap the search icon, or present a card on the card presenting area. The system will enter the User Information page.

7.5 Basic Settings

7.5.1 Set Time

You can set the device time format and the current time.

Long tap on the initial page for 3 s and login the device home page. Tap **Basic** → **Time** .

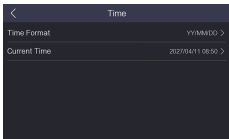


Figure 7-8 Time Settings Page

You can set the device time format and the current time.

7.5.2 Set Sound

Enable or disable the **Keypad Sound** and **Voice Volume**. You can also adjust the **Voice Volume**.

Long tap on the initial page for 3 s and login the device home page. Tap **Basic** → **Sound** .

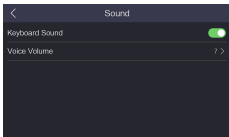


Figure 7-9 Sound Settings

You can enable or disable the device keypad sound and voice volume. Voice volume is also adjustable.

 **Note**

The available volume range is from 0 to 10. The larger the value, the louder the volume. 0 represents disable the voice prompt function.

7.5.3 Set Enrollment Rule

Set the enrollment rules before data enrollment.

Long tap on the initial page for 3 s and login the home page. Tap **Basic** → **Enrollment Rules** .

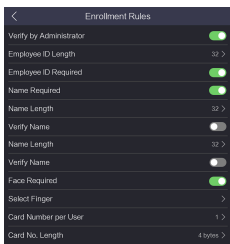


Figure 7-10 Enrollment Rules Page

The configurable rules and descriptions are as follows:

Verify by Administrator

If enabling the function, you should verify the administrator's permission before enrollment.

Employee ID Length

Set the employee ID's length when enrolling a person's information.

Employee ID Required

You must enroll the employee ID when enrolling a person's information.

Name Required

You must enroll the person's name when enrolling a person's information.

Name Length

Set the name's length when enrolling a person's information.

Verify Name

When enter a name in the enroll user page, the system will compare the name with all names in the database to avoid name duplication.

Face Required

You must enroll the person's face when enrolling a person's information.

Select Finger

Set the enrolling fingers when enrolling a person's fingerprint.

Card Number per User

Set the maximum card number that a person can enroll.

Card No. Length

Set the card No.'s length when enrolling a person's information.

7.5.4 Other Settings

You can set the device white light brightness, IR light brightness, and video standard.

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

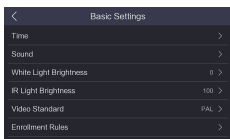


Figure 7-11 Basic Settings Page

White Light Brightness

Set the supplement white light's brightness. The brightness range is from 1 to 100. 0 refers to turning off the light. 1 refers to the darkest, and 100 refers to the brightest.

IR Light Brightness

Set the IR light brightness when the IR light is enabled. The brightness range is from 1 to 100. 0 refers to turning off the light. 1 refers to the darkest, and 100 refers to the brightest.

Video Standard

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

PAL

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

NTSC

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

7.5.5 Set Biometric Parameters

You can customize the face parameters to improve the face recognition performance. The configurable parameters includes face anti-spoofing, liveness security level, pitch angle, yaw angle, pupillary distance, and WDR.

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

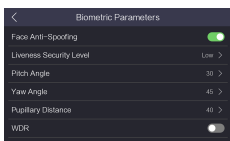



Figure 7-12 Biometric Parameters Page

Table 7-1 Face Picture Parameters

| Parameter | Description |
|--------------------|--|
| Face Anti-Spoofing | Enable or disable the face anti-spoofing function. If enabling the function, the device can recognize whether the person is a live one or not. |

| Parameter | Description |
|-------------------------|---|
| |  Note Biometric recognition products are not completely applicable to anti-spoofing environments. If you require a higher security level, use multiple authentication modes. |
| Liveness Security Level | After enabling face anti-spoofing function, you can set the matching security level when performing live face authentication. |
| Pitch Angle | The maximum pitch angle when starting face authentication. By default, the angle is 30°. |
| Yaw Angle | The maximum yaw angle when starting face authentication. By default, the angle is 45°. |
| Pupillary Distance | The minimum resolution between two pupils when starting face recognition. The actual resolution should be larger than the configured value. By default, the resolution is 40. |
| WDR | It is suggested to enable the WDR function if installing the device outdoors. When there are both very bright and very dark areas simultaneously in the view, you can enable the WDR function to balance the brightness of the whole image and provide clear images with details. |

7.6 Data Management

You can import user list, export user list template, export enrolled data, and clear enrolled data.

7.6.1 Import User

Import the user information from the USB flash drive to the device.

Before You Start

Plug the USB flash drive in the USB interface on the device.

Steps

1. Long tap on the initial page for 3 s and login the home page.
2. Tap **Data**.

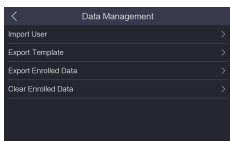


Figure 7-13 Data Management Page

3. Tap Export Template.

The template will be exported to the USB flash drive.

4. Edit the exported table and enroll the user information.



Note

Make sure the edited file is saved in the folder named "DS-K1F600" in the root directory of the USB flash drive.

5. Tap Import User.



Note

Up to 2000 users can be imported.

Result

The system will read the user information in the USB flash drive automatically and import the data to the device.

7.6.2 Export Enrolled Data

Export enrolled data from the device to the USB flash drive.

Before You Start

Plug the USB flash drive in the USB interface on the device.



Note

- The supported USB flash drive format is FAT32.
 - The system supports the USB flash drive with the storage of 1G to 32G. Make sure the free space of the USB flash drive is more than 512M.
 - The exported user data is a DB file, which cannot be edited.
-

Steps

1. Long tap on the initial page for 3 s and login the home page.
2. Tap **Data**.

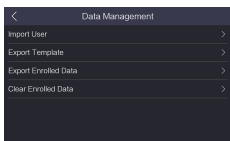


Figure 7-14 Data Management Page

3. Tap Export Enrolled Data.

All enrolled data will be exported to the USB flash drive.

7.6.3 Clear Enrolled Data

Delete all enrolled data in the device, including all face pictures, fingerprints, card, etc.

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

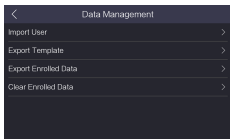


Figure 7-15 Data Management Page

Tap **Clear Enrolled Data** to delete all enrolled data in the device, including all face pictures, fingerprints, card, etc.

7.7 System Maintenance

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

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

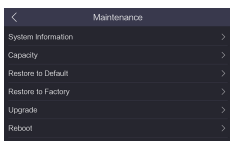


Figure 7-16 Maintenance Page

System Information

You can view the device information.

Note

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

Capacity

You can view the number of administrator, user, face picture, card, and event.

Note

- Parts of the device models support displaying the fingerprint number. Refers to the actual page for details.
 - The capacity varies according to the configured enrollment rules. For details about setting enrollment rules, see **Set Enrollment Rule**.
-

Restore to Default

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

Restore to Factory

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

Upgrade

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

Reboot

The device will reboot after the confirmation.

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.

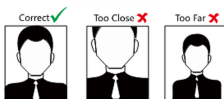
Posture

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.



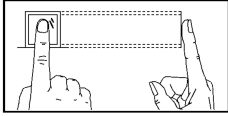
B. Tips for Scanning Fingerprint

Recommended Finger

Forefinger, middle finger or the third finger.

Correct Scanning

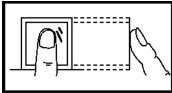
The figure displayed below is the correct way to scan your finger:



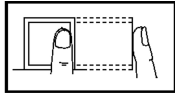
You should press your finger on the scanner horizontally. The center of your scanned finger should align with the scanner center.

Incorrect Scanning

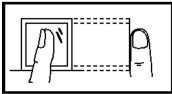
The figures of scanning fingerprint displayed below are incorrect:



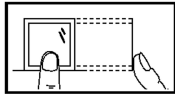
Vertical



Edge I



Side



Edge II

Environment

The scanner should avoid direct sun light, high temperature, humid conditions and rain.

When it is dry, the scanner may not recognize your fingerprint successfully. You can blow your finger and scan again.

Others

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

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

C. 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 C-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 C-2 Device Command