**1 Appearance**

![Fingerprint Time Attendance Terminal](Image)

**UD12120B-C**

- **USB Interface**
- **Fingerprint Recognition Area**
- **Power Interface**
- **Network Interface**
- **Keypad**
- **Display Screen**
- **Card Swiping Area**
- **Exiting Key**
- **Direction Keys**
- **Editing Key**
- **Deleting Key**

**Keypad Descriptions**

- **OK Key:** Press the key and confirm operations. Hold the key for 2 s to enter the login interface.
- **Deleting Key:** Press the key to delete the entered letter or number. If the device supports connecting lithium battery, long press the key to power off the device.
- **Direction Keys:** Press the key to move the cursor on the screen.
- **Exiting Key:** Press the key to exit the menu.
- **Numeric Keys/Letter Keys:** Press the key to enter numbers or letters. Key 0 can also represent a space key except you are using the number/layout method.
- **Editing Key:** Press the key to enter the editing status. You can shift among numbers/lowercases, numbers/uppercases and symbols.

**Notes:**

1. The pictures here are for reference only. Some models do not support card swiping function. For details, refer to the actual products.
2. If you enable the attendance status function, the OK key, the direction key, and the exiting key can be the shortcut key of the attendance status.

**2 Installation**

The additional force shall be equal to three times the weight of the equipment but not less than 50 N.

The equipment and its associated mounting means shall remain secure during the test. After the test, the equipment, including any associated mounting plate, shall not be damaged.

**Steps:**

1. Stick a mounting template on the wall at a required height, and drill 4 holes according to the mounting template on the wall.
2. Insert 4 supplied expansion sleeves of the setscrews (4_KA4×22-SUS) in the fixed screws and hang the device on the wall.
3. Align four holes of the device rear panel with the fixed screws and hang the device on the wall.
4. Reserve 5.2 mm to 5.5 mm of expansion bolts outside the wall for hanging the device.

©2019 Hangzhou Hikvision Digital Technology Co., Ltd.

It includes instructions on how to use the Product, the software embodied in the Product is governed by the user license agreement covering that Product.

About this Manual:

This Manual is subject to domestic and international copyright protection. Hangzhou Hikvision Digital Technology Co., Ltd. ("Hikvision") reserves all rights to this Manual. This manual cannot be reproduced, changed, translated, or distributed, entirely or wholly, by any means, without the prior written permission of Hikvision.

**Trademarks**

Hikvision and other Hikvision marks are the properties of Hikvision and are registered trademarks or the subject of applications for the same in Hikvision and/or other countries. Other trademarks mentioned in this manual are the properties of their respective owners. No right of license is given to use such trademarks without express permission.

**Legal Disclaimer**

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE PRODUCT IS PROVIDED "AS IS," WITH ALL FAULTS AND ERRORS, AND HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF THIRD PARTY RIGHTS, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, HIKVISION SHALL NOT BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTIONS, LOSS OF BUSINESS INFORMATION, OR LOSS OF BUSINESS OPPORTUNITY, IN CONNECTION WITH THE USE OF THIS PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

REGARDING TO THE PRODUCT WITH INTERNET ACCESS, THE USE OF PRODUCT SHALL BE AT YOUR OWN RISK. HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR PRIVACY LEAKAGE DUE TO THE FOLLOWING CAUSES, INCLUDING, AMONG OTHERS, ACCESS TO INTERNET FROM CYBER ATTACK, HACKER ATTACK, VIRUS/INFECTION, OR OTHER INTERNET SECURITY RISKS. HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

SURVEILLANCE LAWS VARY BY JURISDICTION. PLEASE CHECK ALL RELEVANT LAWS IN YOUR JURISDICTION BEFORE USING THIS PRODUCT FOR SURVEILLANCE.

**Data Protection**

During the use of the device, personal data will be collected, stored and processed. To protect the development of Hikvision devices recruited 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 a 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, periodic reviews and assessments of the effectiveness of your security controls.
3 Basic Operation

1 Activation

- Activating via Device
  - Power on and wire the network cable after installation.
  - You should activate the device before the first login.
  - After powering on, the interface will be displayed as follows.
  - You can create the device password and confirm the password to activate.
  - The default values of the terminal are as follows:
    - The default IP address: 192.0.0.64
    - The default port No.: 8000
  - The default user name: admin

2 Parameters Configuration

- Schedule Shift by Department Flow:
  - Add User (select department when adding new user): Department Management > Shift Management > Add Holiday > Shift Schedule Management (Schedule Shift by Department)
  - Schedule Shift by Individual Flow: Add User > Management Tool > Add Holiday > Shift Schedule Management (Schedule Shift by Individual)

  - Add User: Edit the ID No. and the user name. Press the OK key to confirm. Enter the card No., register the fingerprint, set the password, select the department, select the role and select the authentication mode. Save the parameters to confirm adding.
  - Edit Department: Select the department in the department list and select “Edit”. Edit the department name. Save the parameters to confirm editing.
  - Shift Management:
    - Manual Shift (Normal (Normal Shift) interface under the Shift Management menu. Configure the shift rule and the normal shift. Save the parameters to confirm editing.
    - Man-Hour Shift: Edit the Man-Hour (Man-Hour Shift) interface under the Shift Management menu. Configure the man-hour parameters and save the parameters.
  - Add Holiday: Enter the New (Add New Holiday) interface under the Holiday menu. Enter the holiday name, the holiday type, the holiday start date and the holiday end date. Save the parameters to confirm configuration.
  - Shift Schedule Management:
    - Schedule Shift by Department: Select a department to configure in the By Dept. (Schedule by Department) interface. Configure the shift, the start date, the end date and the holiday. Save the parameters to confirm configuration.
    - Schedule Shift by Individual: Select New Individual Shift in the By Indiv. (Schedule by Individual) interface. Select a person to schedule in the New Individual Shift interface. Configure the shift, the schedule start date and the end date. Save the parameters to confirm editing.
  - Attendance Report:
    - Plug the USB flash drive in the device. In the Report interface, select a table type, create a device ID, select start date and end date. Press OK to export the attendance report to the USB flash drive.

- View License: You can view the license via the website: http://opensource.hikvision.com/Home/List?id=46

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 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 product is a Class B digital device. This product is designed and manufactured to meet the latest possible level of electromagnetic emissions and immunity standards. However, no equipment can provide 100% immunity to electromagnetic interference. 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 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.

- FCC Conditions
  - This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:
    - This device may not cause harmful interference.
    - This device must accept any interference received, including interference that may cause undesired operation.

- EU Conformity Statement
  - This product is in conformity with the protection requirements of EU Council directive 2014/30/EU on the approximation of the laws of the Member States relating to electromagnetic compatibility, 2014/35/EU on the harmonization of the laws of Member States relating to the access of electricity端末 users, 2011/65/EU (RoHS directive) on restriction of the use of certain hazardous substances in electrical and electronic equipment, 2009/125/EC (WEEE directive) on waste electrical and electronic equipment, for the harmonized EN standard EN 55032:2015 (EMC), EN 50155:2008 (EN), EN 61010-1:2010 (safety). For more information, see: www.recyclight.info

- Industry Canada ICES-003 Compliance
  - This device meets the ICES-003 (B)/NMB-3(B) standards requirements.
  - This device complies with Industry Canada licence-exempt RSS standards 049.

- Use Only power supplies listed in the following model and manufacturer standards:

<table>
<thead>
<tr>
<th>Model</th>
<th>Manufacturer</th>
<th>Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADS-MA-06 05050EFG</td>
<td>Dow Van Enterprise Co., Ltd.</td>
<td>CE</td>
</tr>
<tr>
<td>ADS-MA-06 05050FCU</td>
<td>Dow Van Enterprise Co., Ltd.</td>
<td>NEMA</td>
</tr>
<tr>
<td>ADS-MA-06 05050PB</td>
<td>Dow Van Enterprise Co., Ltd.</td>
<td>BS</td>
</tr>
</tbody>
</table>

Activating via SADP

1. Download SADP Software
   - Get the SADP software from the supplied disk. Install and run the software.

2. Activate Device
   - Check the inactive device from the device list. Create a password in the right side of the interface and confirm the password.

3. Edit Device IP Address
   - Check the device and manually edit the device IP address, Port No., Subnet Mask, Gateway, etc.

Activating via Client Software

1. Get the client software from the supplied disk. Install and run the client software.
2. Enter the Device Management page.
3. Select an inactive device from the Online Device list.
4. Click Activate to pop up the Activation page.
5. Create a password and confirm the new password.
6. Click OK to activate the device.
7. Click Modify Netinfo to set the device IP address, mask address, gateway address, and port No.