



Wireless Fingerprint Mouse A3

User Manual



No more memorizing any account passwords-ever

Password Management

Fingerprint Unlock System

File Encryption

Product Exterior Introduction

- ① Left button
- ② Scroll ball
- ③ Fingerprint
- ④ DPI button
- ⑤ Right button
- ⑥ Middle button
- ⑦ Colorful glow
- ⑧ Fingerprint Light
- ⑨ Mode button
- ⑩ USB mode (R)
- ⑪ 2.4G mode (G)
- ⑫ USB Type-C
- ⑬ Power switch
- ⑭ 2.4G dongle
- ⑮ USB cable



1 Mouse Functions

1.1 Power Switch

Before using the mouse, you must first turn on the power switch⑬. The mouse can also be charged when the power switch is turned off.

1.2 Mode Selection

>2.4G Mode (Recommended)

a. Remove the 2.4G receiver ⑭ from the bottom of the mouse and insert it into the USB port of your computer.

b. Press the mode button ⑨ until the right green light ⑪ flashes rapidly (indicating a waiting-for-connection state); afterward, a slow flash indicates successful connection to the receiver.

>USB Mode

a. Insert the Type-C end of the USB adapter cable ⑮ into the mouse port ⑫, and plug the other end into the computer's USB port.

b. Press the mode button ⑨ until the left red light ⑩ flashes (indicating successful connection).

1.3 DPI Adjustment (Defines Mouse Movement "Sensitivity")

a. Press the DPI button ④ once; the breathing light will cycle through colors to set DPI as follows: 1000 (red) → 1600 (blue) → 2400 (green). The higher the DPI, the higher the cursor sensitivity.

b. Long-press the DPI button to turn off/on the breathing light ⑦ and

e. Password pops up Settings

You can customize how to pop up the password autofill window. The default method is the middle mouse button. You may also choose a keyboard shortcut instead.

Go to Toolbox → Mouse/Keyboard pops up Settings, select your preferred method, and click OK to save.

f. Auto Start & Breathing Light

Auto Start: Enabled by default. You can choose to enable or disable automatic startup with the system.

Breathing Light: Enabled by default, and can be turned on or off as desired.

3.4 File Encryption

Both encryption and decryption functions require the device to be connected and are executed via the right-click context menu.

a. File Encryption

Select any file on your computer, right-click, and choose "Kika Doc Encrypt". The system will automatically create an encrypted file with the extension .kik in the same directory as the original file.

b. File Decryption

Select an encrypted file, right-click, and choose "Kika Doc Decrypt". After clicking, the system will generate a decrypted file in the same directory, restored to its original format.

4 Frequently Asked Questions

4.1 System Installation Issues

a. Which devices and systems are supported?

The device supports all Windows systems, enabling fingerprint authentication login through CP technology.

It is compatible with both desktop computers and laptops. Additionally, it also supports Ubuntu 20–23. For detailed setup instructions, please refer to the official website guide.

b. How to use with Windows 7 or Windows 8?

You need to download the management software. After installation, click [Bind to Windows System Login] in [Fingerprint Management], enter your Windows account password, and click OK to test the fingerprint login function.

4.2 Product Usage Issues

a. How many passwords and fingerprints can be stored?

The device can store more than 500 passwords and 20 fingerprints.

b. How to record and use passwords?

Please refer to Sections 3.1 (Password Management) and 3.2 (Fingerprint Management) for detailed instructions.

c. Why does fingerprint recognition become less sensitive after

the fingerprint's seven-color light effect ⑧.

1.4 Charging

- When the breathing light ⑦ flashes red once every 2 seconds, it indicates a low battery warning (below 25%).
- When a USB cable is connected, the red light on the top of the mouse will turn on to indicate charging; the red light will turn off once charging is complete.

2 Software Installation

2.1 Windows Hello Automatic Installation

If your computer is running a genuine Windows 10 or later operating system and the logged-in account is not the Administrator account, refer to the content here; for other operating systems, please refer to section 2.2.

a. **Automatic Installation:** After connecting the hardware to your computer, the system will automatically download the driver from Microsoft. (Note: Some early versions of Windows 10 do not support this feature—please refer to 2.2.)

b. **Fingerprint Setup:** Open your computer's [Settings] > [Accounts] > [Sign-in options] > [Sign-in method], select [Windows Hello Fingerprint], and click [Set up].

c. **Fingerprint Enrollment:** Click [Start], enter your user password [PIN] to verify your identity, then start enrolling your fingerprint. Adjust your finger repeatedly until enrollment is successful.

d. **Authorization Configuration:** Go to [Accounts] > [Sign-in options] > [Additional settings] in the system, and enable [Sign in using an external camera or fingerprint reader]. (This feature was added in Windows updates after July 2025; if it is not available on your version, no configuration is required.)

e. **Unlock Test:** Lock your screen (you can use the shortcut key WIN+L), select the [Fingerprint] sign-in option on the screen, place your finger on the device's fingerprint sensor, and experience instant screen unlocking.

2.2 KikaID Management Software Installation

The KikaID management software provides local fingerprint and password management, as well as file encryption features. (For systems that do not support Windows Hello, this software can also enable fingerprint login.)

a. **Download the Software:** Enter [www.ad2cd.com] in your browser and download the KikaID Management Tool from the download page (please distinguish between the 32-bit and 64-bit versions).

b. **Install the Software:** Extract the files and install the .exe program. (It is recommended to temporarily disable antivirus software during

long periods of inactivity?

The device features an auto-learning function, which improves accuracy over time and stabilizes after frequent use.

If the fingerprint is not used for a long time, environmental factors or changes in the fingerprint texture may affect recognition accuracy. For the best experience, it is recommended to re-enroll your fingerprint periodically.

d. Forgot KikaID login password?

Use fingerprint to log in to KikaID. An KikaID account exists in the password vault; its password is the login password and can be copied.

4.3 Product Security

a. Will account passwords be leaked?

The product uses EAL4+ level encryption—hardware attacks cannot extract usable data. If incorrect passcodes are entered repeatedly, the device will lock. The management software never connects to the internet; all passwords are stored locally on the device, eliminating network-based leakage risk. Each device has a unique encryption key, so devices cannot unlock each other unless the user explicitly imports the same key into another device.

We recommend regular backups (both passwords and keys) so data can be recovered if the device is lost or damaged.

b. What if the device is lost or broken?

Physical damage or loss is possible; therefore, regular backups of passwords and keys are strongly recommended to prevent permanent data loss. If the device is lost, purchase a replacement device and import your backed-up key to synchronize and restore data. For higher security/availability requirements, consider purchasing two devices to serve as mutual backups and recovery options.

c. What if the device cannot recognize fingerprints?

If the device fails to recognize fingerprints, check whether the sensor area is dirty—clean the fingerprint module and try again. If repeated attempts fail, the device may be damaged; please contact official after-sales support.

d. Can identical devices unlock each other?

Each device contains a randomly generated master key stored in the device's secure chip. The master key does not leave the chip by default, and fingerprint verification is performed inside the secure chip—external interference is not possible. To enable cross-device unlocking, back up the key from one device and import it into the other device. (Note: both devices must have the same login password when importing the key.)

4.4 Software Update

a. Software Download

installation, as security warnings may appear.)

c. **Enroll Fingerprint and Set Password:** After successful installation, open the software, enroll your fingerprint, and then set your login password.

d. **Reminder:** Please keep your password safe in case your fingerprint becomes invalid or for future backup management needs.

3 Usage Instructions

3.1 Password Management

The management software Password Box supports storing and managing more than 500 passwords, allowing you to add, edit, or delete entries easily.

a. Add a Password:

Open the software and log in, then go to the Password Box section; Drag an application icon from the desktop into the box page or click Add, then enter the title, website, username, and password; Select the autofill rule: fill in both the username and password, or fill in the password only. After confirmation, click [OK] to save the password.

b. Use a Password:

Open a website or PC application, place the cursor in the username or password field, and press the middle mouse button; In the pop-up window, select the correct account; The software will automatically fill in the credentials for quick login.

c. Manage Passwords:

Edit a Password: Double-click the password entry and modify the details in the pop-up window.

Delete a Password: Select a password entry, view its details at the bottom of the window, and click Delete. Confirm to permanently remove the password.

3.2 Fingerprint Management

a. Enroll Fingerprint

Open the software and log in, then go to the Fingerprint Management section. Click Add Fingerprint, verify your login password, and place the desired finger on the device. Follow the on-screen instructions to complete the fingerprint enrollment.

b. Delete Fingerprint

In the Fingerprint Management page, click the X icon at the top right corner of the fingerprint entry. A confirmation window will appear—click Confirm to delete the fingerprint. Note: once deleted, the fingerprint cannot be recovered.

Delete all fingerprints using the "Clear All Fingerprints" function below.

c. Verify Fingerprint

In the Fingerprint Management page, click Verify Fingerprint, then place your finger on the sensor. The software will identify the fingerprint

and display its corresponding ID number.

d. Fingerprint Login to System

For computers running Windows 10 or later: Automatically check the box next to "Enable/Disable Log in Combine Function", click "Combine Fingerprint with Log in MS account", and enter your system login password to enable fingerprint login or screen unlock. Uncheck "Enable/Disable Log in Combine Function" and only Windows Hello fingerprint login will be available for the system.

For computers running Windows versions earlier than 10: Check the box next to "Enable/Disable Log in Combine Function" and bind your Windows login account to enable fingerprint login or screen unlock.

3.3 Toolbox

a. Backup / Restore / Clear Password Box

Backup Passwords: Back up the passwords stored in the device to your local computer. Go to Toolbox → Backup Passwords, choose the save location, enter a backup name, and click Start to generate a backup file.

Restore Passwords: Import a previously saved backup file into the device. Go to Toolbox → Restore Passwords, select the local backup file, and click Start to import the passwords.

Clear Password Box: Click Clear Password Box, confirm the operation, and all stored passwords will be permanently deleted and cannot be recovered.

b. Import Browser Passwords

Go to Toolbox → Import Browser Passwords, select a local CSV file, and click Start to import the passwords into the device.

Note: The total number of passwords cannot exceed capacity limit.

c. Change Login Password

While logged in, go to Toolbox → Change PIN, enter the current PIN and the new PIN twice, then click Confirm to save changes.

The password must contain at least 6 characters. It is recommended to use a combination of letters + numbers + symbols.

The login password is a critical credential for fingerprint verification and data backup/recovery—please keep it safe.

d. Manage master Key

The master key is the device's unique security lock. It can be backed up or imported to synchronize encryption/decryption keys between devices.

Backup Key: Go to Toolbox → Backup master Key, select the storage location, enter a name, and click Start to create a backup file.

Restore Key: Go to Toolbox → Restore master Key, select the local key file, and click Start to import it into a new device.

You can visit the official website www.ab2cd.com to download the product management software.

b. How often and how to update the software

To protect user privacy and data security, the software does not update automatically. Please manually visit the official website to download and install the latest version when updates are available.

4.5 Other Issues

a. Supported languages

Currently, the software supports both Chinese and English. You can download the corresponding installation package.

b. Fingerprint recognition is slow or fails

Make sure your finger is clean, dry, and free of oil. If recognition remains inaccurate, re-enroll the fingerprint — capturing it from different angles helps improve accuracy.

5 Precautions

5.1 Fire, Water and Liquid Protection

Keep the product's touchpad clean and dry. Avoid exposing it to high temperatures, humidity, or sharp objects.

5.2 Child Safety

Contains small parts. Keep away from children; do not touch or ingest. Risk of choking due to swallowing.

5.3 Data Backup

Regularly back up important data while using this product.

6 After-Sales Service

6.1 Device Warranty

The device is covered by a one-year limited warranty. For issues not caused by human damage, the device will be replaced, not repaired.

If the device becomes unusable due to product performance or other reasons, please contact our customer service promptly at: support@ab2cd.com.

6.2 Company Statement

KikaID is not responsible for any loss or damage resulting from the use of our fingerprint recognition device, including direct, indirect, incidental, or consequential damages. Users are responsible for the proper use and maintenance of the device. By using this product, you acknowledge that KikaID assumes no liability for any resulting losses.

6.3 Contact Us

If you have any questions or suggestions regarding the product, please contact us via the following email: support@ab2cd.com

FCC WARNING :

NOTE: 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. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation

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.

Warning: changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment

The device has been evaluated to meet general RF exposure requirement, the device can be used in portable exposure condition without restriction