



MOwner APP User Manual (V1.0)

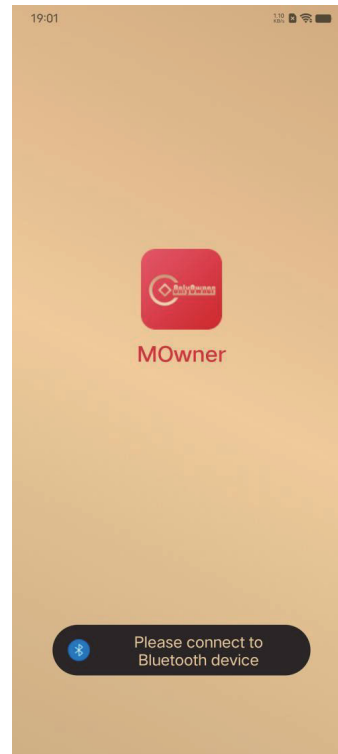
Update Date: October 20, 2025

Catalogue

1. About MOwner	17
2. Login operation (including Bluetooth device binding)	18
3. Core module function description	20
3.1 [File] section (core functional area)	20
3.2 [Address Book] section	22
3.3 [Basic Settings] section	23
4. Function usage (encryption, decryption, and sharing)	24
4.1 Encryption Operation	24
4.2 Decryption Operation	26
4.3 File Sharing and Receiving Management	28
5. Precautions	31

1. About MOwner

MOwner is a mobile file encryption application that requires the use of a dedicated Bluetooth hardware device called "MOwner". Its core functions include encrypted storage, secure management, and targeted encryption sharing of mobile file data. Similar to OnlyOwner's computer encryption product, all operations rely on Bluetooth hardware MOwner verification to ensure information security.

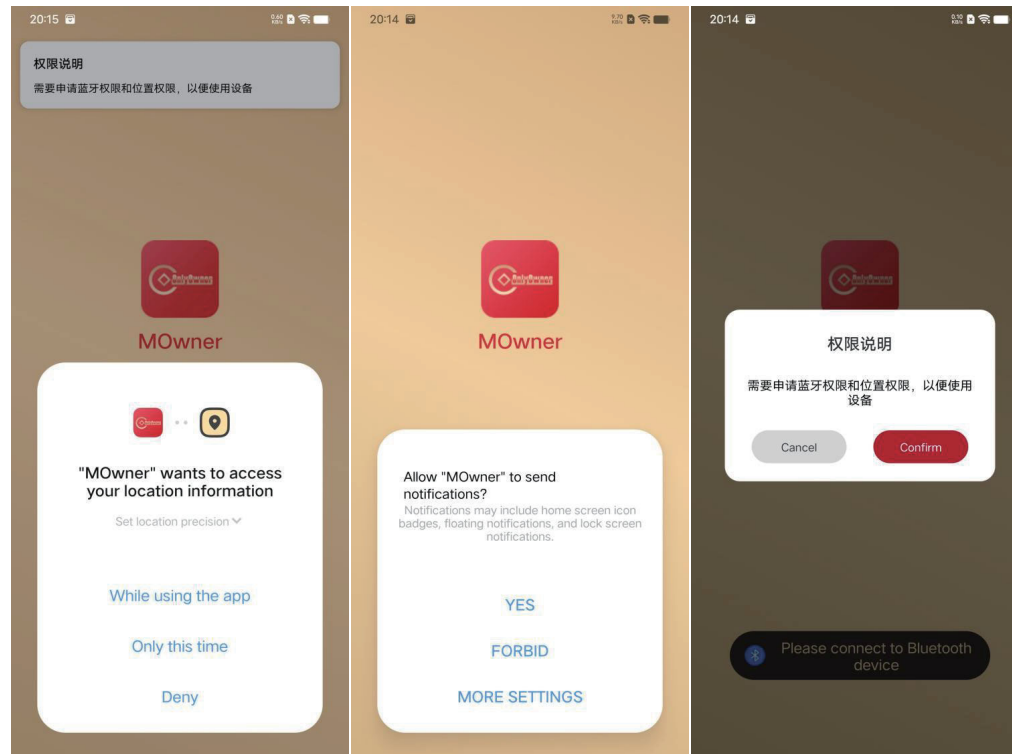


2. Login operation (including Bluetooth device binding)

Login requires completing four steps: Bluetooth connection → device selection → PIN code verification → device binding. The specific process is as follows:

2.1 Bluetooth Authorization:

After opening the app, click the "Please Connect Bluetooth Device" button. When the system pops up a request for "Bluetooth Authorization", "Location Search Authorization", and "File Access Authorization", select "Agree" or "Yes" for all options.



2.2 Hardware startup and device selection:

> Press the "OK" button on the Bluetooth hardware "MOwner" to start the Bluetooth device (the device automatically enters Bluetooth pairing mode after startup).

> Ensure that the phone is in close proximity to the hardware (recommended within 1 meter), and the app interface will display the hardware device name "MOwner01". Click to select the device

> Attention: When Bluetooth is disconnected, the app is closed, or the software is logged out, the device MOwner will automatically enter sleep mode after 2 minutes without shutting down. To start the Bluetooth device from sleep mode to use, press the [OK] key.

2.3 PIN code verification:

After selecting "MOwner01", the APP will pop up a PIN code input box. The default initial PIN code is "123456". Note that the initial PIN code will be forcibly guided to modify the PIN code after logging in. After modifying the PIN code, you can also modify it again in the APP settings to ensure information security. After modification, remember to keep it in mind, forgetting can not retrieve it.

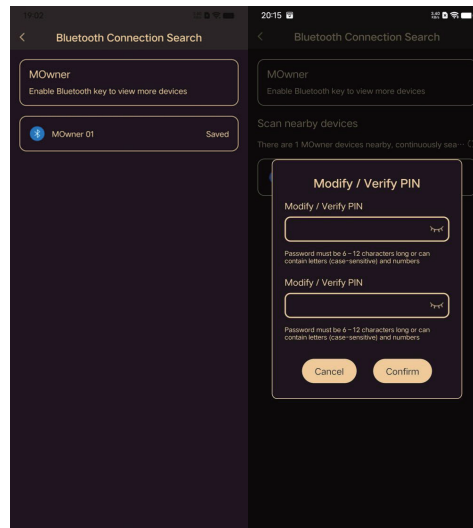
2.4 Bluetooth device binding:

> After verification, the APP automatically binds to the current Bluetooth hardware, and subsequent login only supports this bound hardware, including the master device and slave device.

> PIN code verification is completed locally, without the need for cloud registration;

> After uninstalling and reinstalling the app, the binding relationship can be released.

Attention: When switching between master or slave devices in a set of devices and logging in, you need to long press the saved device "MOwner01" on the login selection device interface, delete the device according to the prompts on the interface, and then try to connect to another device in the set of devices.



3. Core module function description

At the bottom of the app, there are three fixed resident sections: [File], [Address Book], and [Basic Settings]. The functions of each section are as follows:

3.1 [File] section (core functional area)

Function positioning: Manage all regular and encrypted files, including three core areas: [Security Zone], [Local Archives], and [File Stack]:

3.1.1 [Security Zone]:

Unique encrypted storage space, only accessible with Bluetooth hardware binding; Support storing various types of privacy information such as images, audio and video, documents, etc; After moving the file to a Security Zone, it will be automatically encrypted and cannot be viewed directly by the mobile system.

3.1.2 [Local Files]:

Display all files stored on the phone itself (consistent with the "File Management" app function on the phone), which are unencrypted ordinary files; You can select files from this area to move to the Security Zone, or directly manage regular files.

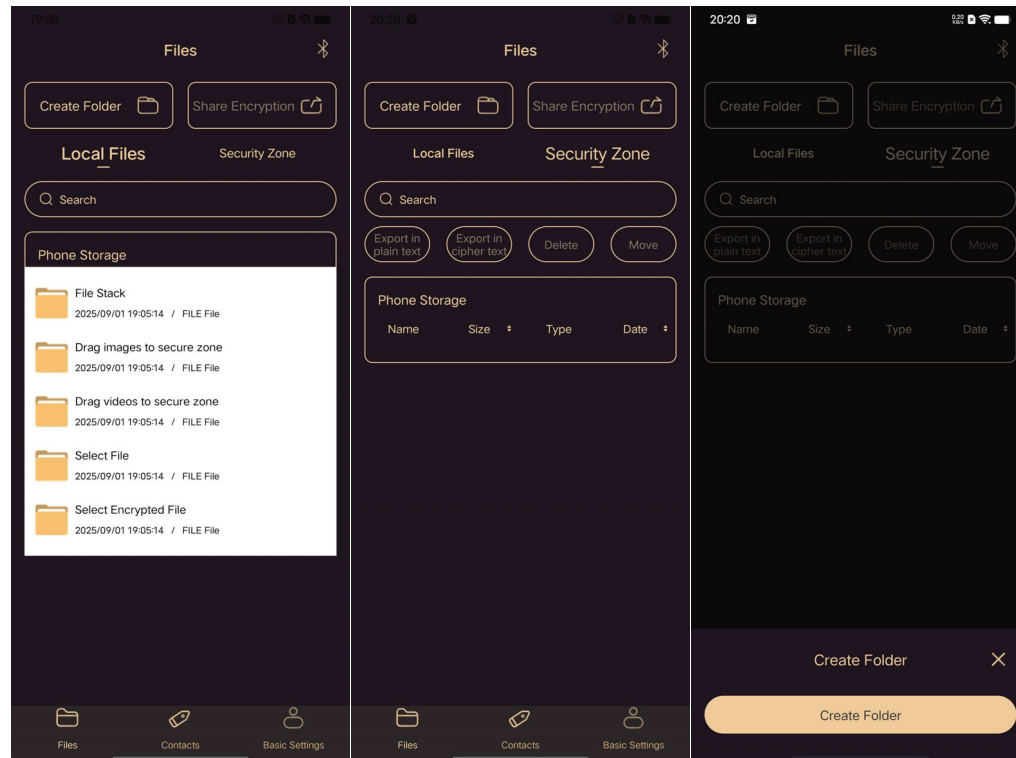
3.1.3 [File Stack]:

This folder is displayed by default in the [Local Files] interface and has the following functions:

- >Record all data related to 'plaintext export' and 'ciphertext export' operations performed in the 'Security Zone';
- >Record all encrypted package files generated after sharing with oneself;
- >Record the file information of all encrypted package files received from a friend's targeted sharing that have been successfully decrypted;
- >Long press the file to enter the "single/multiple selection" mode, where you can perform operations such as sharing, deleting, and moving.

Key operation: Move files into the Security Zone

1. Enter the "File" ->"Local Files" interface, and use the "Image", "Video" and other classification options in the white area of the interface, or click "Select File" to enter the "File Management" on your phone and manually select the files and materials you want to move to the "Security Zone".
2. After selecting the file, it will be automatically encrypted and stored in the 'Security Zone'.



3.2 [Address Book] section

Function positioning: Manage friend information, support "export/import", can export and save contacts to a specified path on the phone.

Core functions:

3.2.1 Adding friends:

>Path: [Contacts] → [Personal] Top of column → [Add].

>Operation: Enter the friend ID (to be obtained from the friend), set the friend nickname and group (such as "family" or "colleagues"), click confirm to add (no consent required from the other party).

>ID acquisition: You can view your own ID at the top of the Basic Settings interface, long press to copy.

3.2.2. Add Group:

>Path: [Address Book] → [Group] Top of column → [Add].

>Operation: Enter the custom group name and click confirm to create it.

3.2.3. Friend management:

>Path: [Contacts] → Friend List → Select Target Friend.

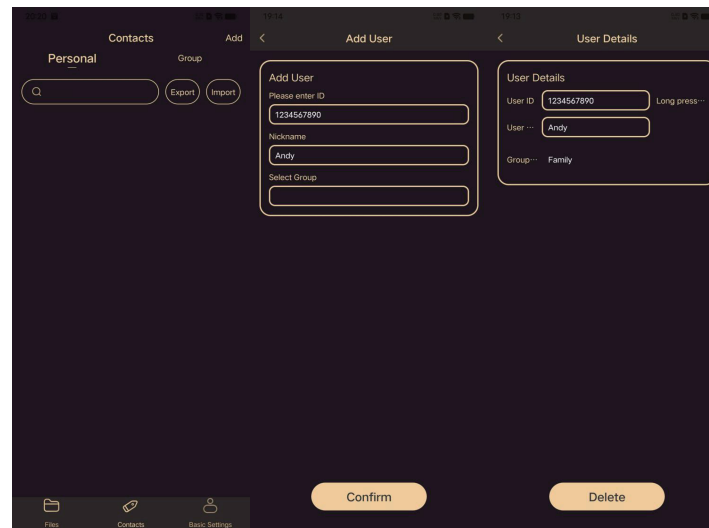
>Operation: You can view friend IDs, modify friend nicknames, adjust friend groups, and delete friends.

3.2.4. Address book backup (import and export):

>Path: [Address Book] → [Import/Export]

>Operation: Export refers to exporting the address book to the file stack or MOwner device for storage and backup.

Import refers to restoring the backed up address book file to the current software address book list.



3.3 [Basic Settings] section

Functional positioning: Manage basic settings, personal key information, and device information of the APP, with the following core functions:

3.3.1 Viewing Device ID:

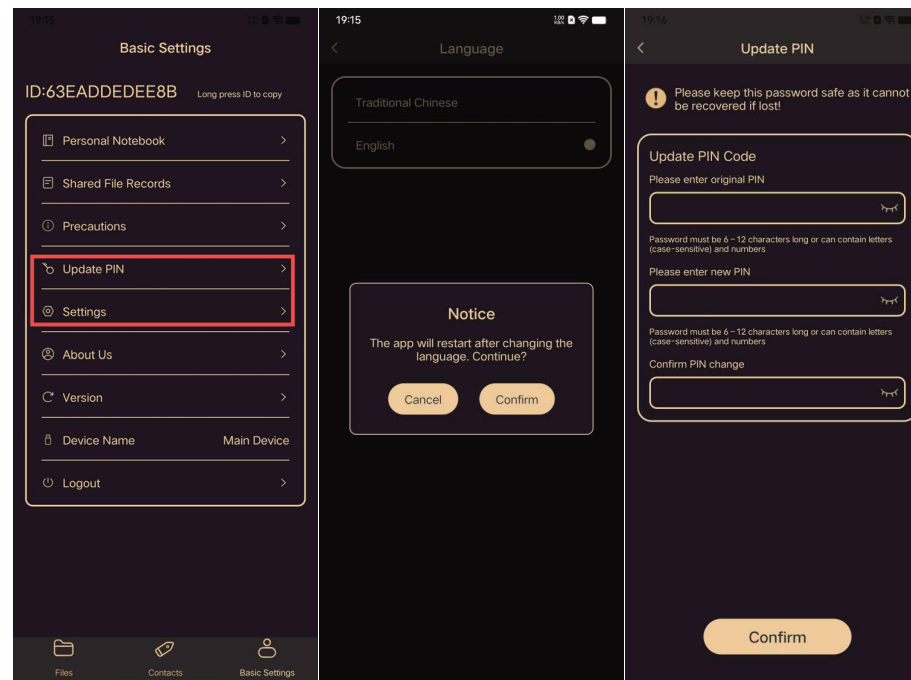
The top of the interface displays the user's ID (for adding friends) and supports long press copying.

3.3.2 Personal notepad:

Edit and encrypt key information (such as privacy information, account passwords, etc.), support uploading up to 9 images; After saving, it will be automatically encrypted and can only be viewed/edited when connected to Bluetooth hardware.

3.3.3 Other settings:

Modify APP display language, modify device PIN code, check for version updates, log out, delete all Security Zone data with one click, etc.



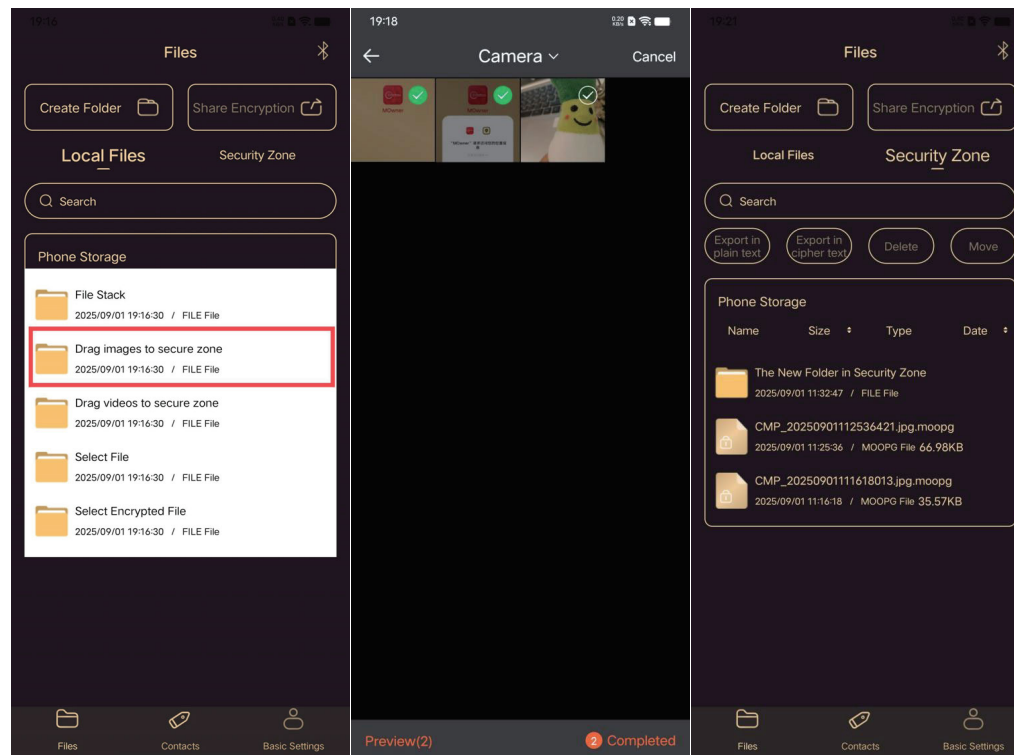
4. Function usage (encryption, decryption, and sharing)

4.1 Encryption Operation

4.1.1 Ordinary file encryption (move to Security Zone)

>Path: [File] ->[Local Files] ->Select File ->"Move to Security Zone".

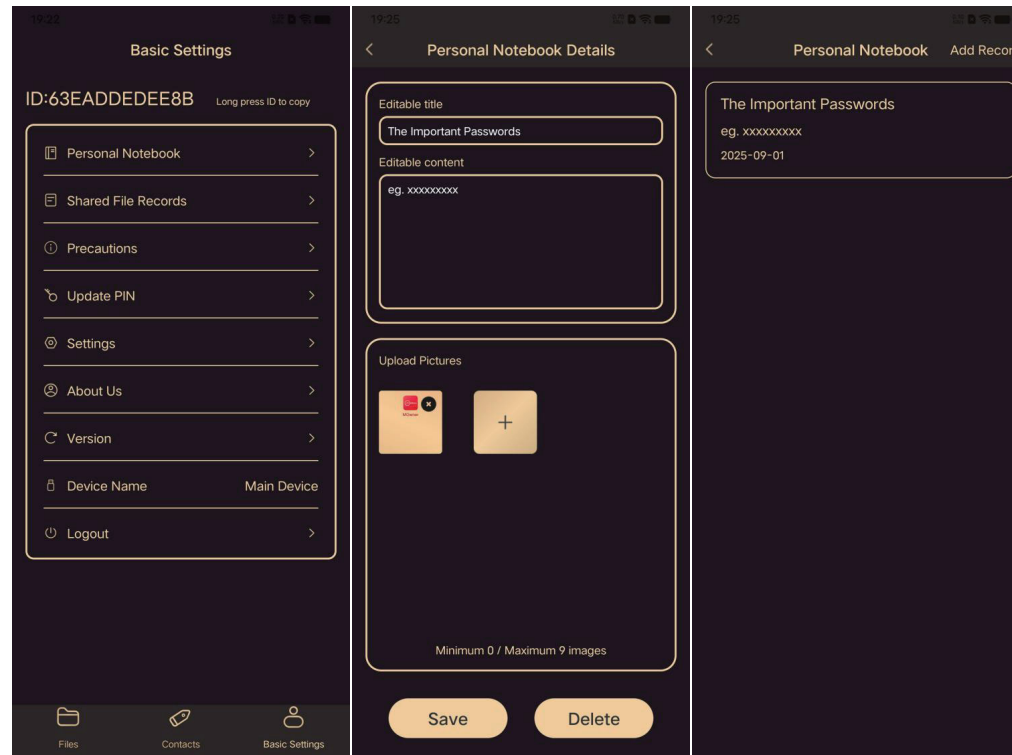
>Description: After the file is moved in, it is automatically encrypted and stored independently. Only Bluetooth hardware can be connected to view it in the 'Security Zone'; The original regular files can be manually deleted without affecting viewing within the Security Zone.



4.1.2 Personal Notebook Information Encryption

>Path: [Basic Settings] → [Personal Notebook] → Edit Information/Upload Images → Click "Save".

>Description: After saving, the information is automatically encrypted and can be accessed for viewing or editing management at any time. It cannot be accessed without Bluetooth hardware.

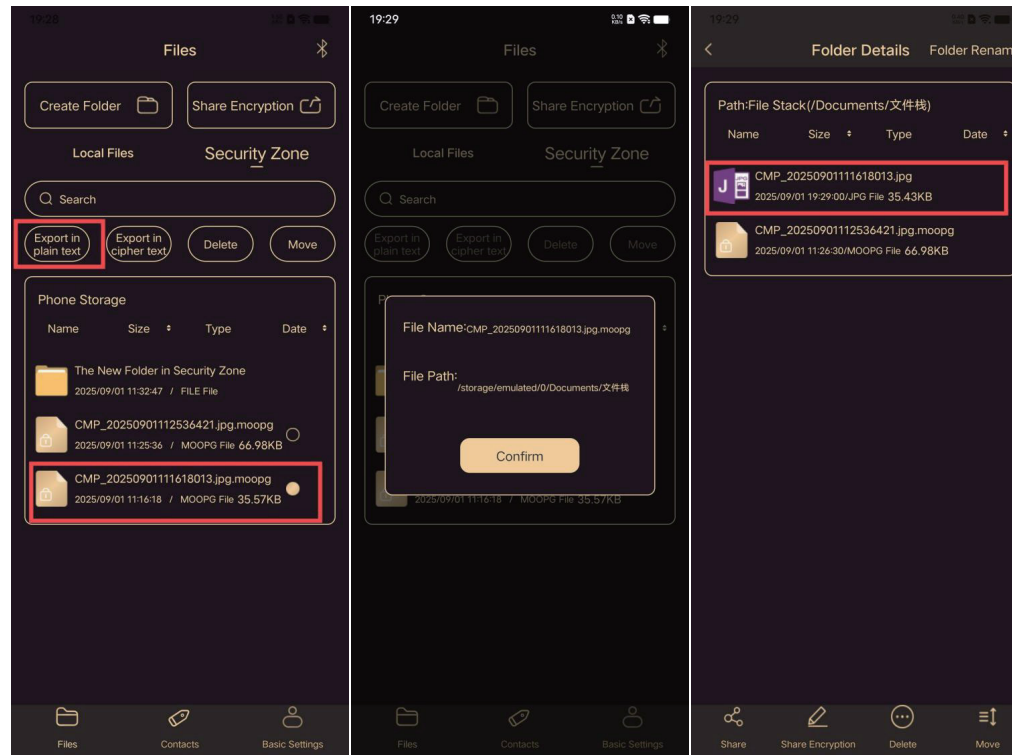


4.2 Decryption Operation

4.2.1 Security Zone File Decryption (Clear Text Export)

>Path: [File] → [Security Zone] → Long press to select encrypted file → Click [Clear Text Export].

>Explanation: The decrypted regular file is automatically stored in the File Stack and can be viewed/used normally.

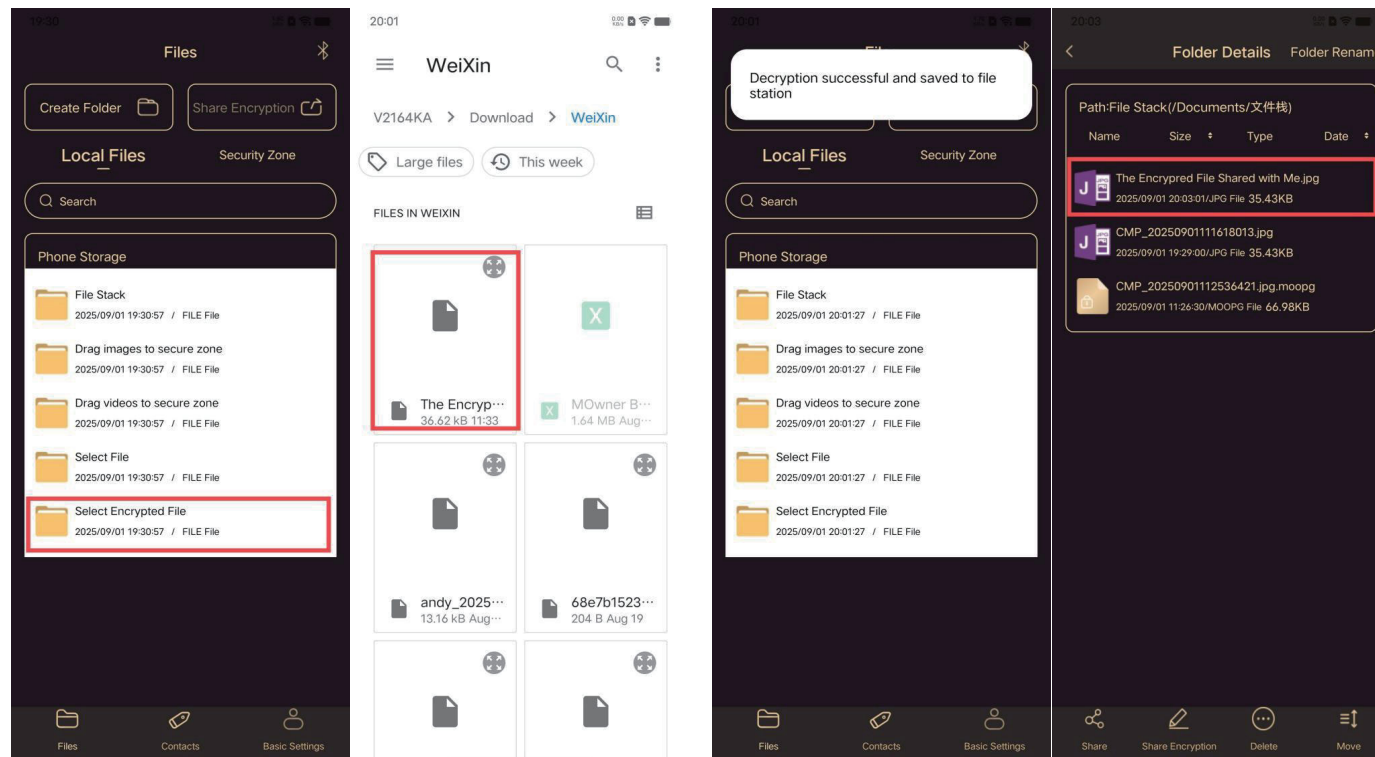


4.2.2 Decryption of encrypted files shared by friends

>Prerequisite: Download the received encrypted file to the local phone.

>Path: [File] ->[Local File] ->[Select Encrypt File] ->Find and click on the received shared file.

>Explanation: Decryption is only allowed for files shared with you by friends who have specified encryption, and can be successfully decrypted using the bound MOwner hardware. After decryption, the file will be displayed in the 'File Stack'. Files shared with you without specified encryption cannot be decrypted.



4.3 File Sharing and Receiving Management

4.3.1 Ordinary file sharing

>Path: [File] → [Local Files] → [File Stack] → Long press to select normal/encrypted files (supports single/multiple selection) → Click on the bottom of the interface [Share].

>Operation: Select the sharing medium (such as WeChat, email, etc.) and send it to the target recipient.

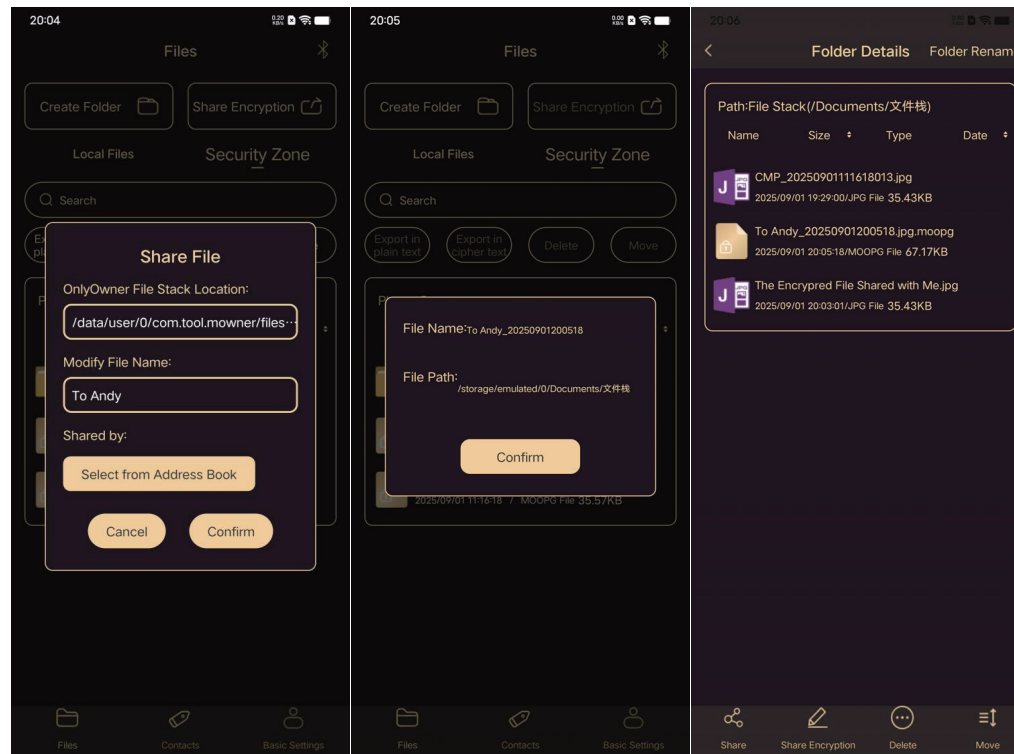
4.3.2 Targeted encryption sharing (only friends can decrypt)

Please create an "encrypted sharing package" and send it through regular sharing. Specific steps:

1. Generate encrypted sharing package:

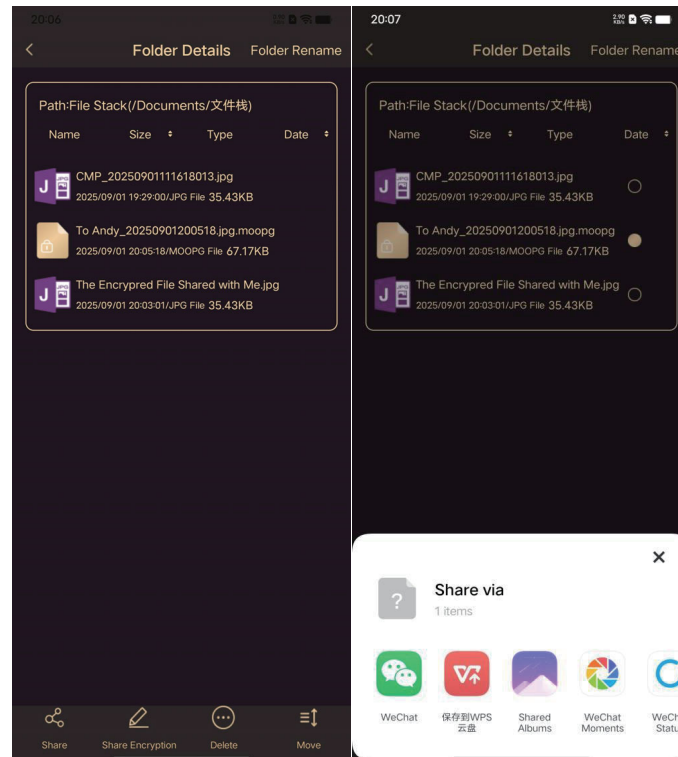
>Path: [File] ->[Local Files] ->[File Stack] ->Long press to select the file to share ->Click [Share Secret].

>Operation: Rename the shared file, select the target friend from the address book (supports single, multiple friends, or group selection), and click "Confirm Generation"; The generated encrypted package is automatically stored in the File Stack.



2. Send encrypted package:

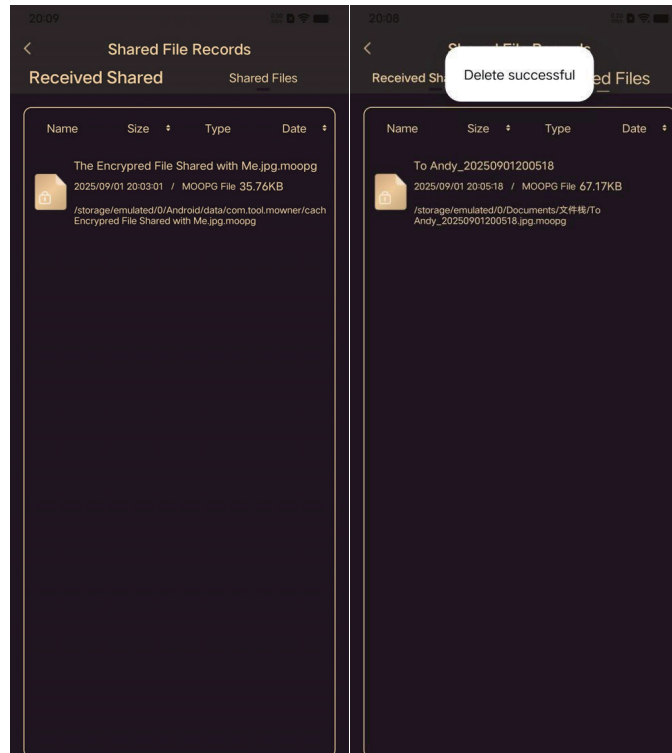
>Path: Find the encrypted package in the 'File Stack' ->Long press ->Click on 'Share' ->Select media to send to friends.



4.3.3 File Sharing Management

>Path: [Basic Settings] → [Share File Records].

>Function: You can view all "received encrypted shared files" and "encrypted shared files", and support direct clicking to view.



5. Precautions

5.1. Data security: APP updates (app marketplace or APK package updates) will not result in user data loss, damage, or inability to decrypt.

5.2. Privacy Protection: [Security Zone] Files will not be associated and displayed by the phone's built-in software (such as gallery, music player) to avoid privacy leakage.

5.3. File backup: It is recommended to back up important files through the "plaintext export" or "ciphertext export" function in the "Security Zone" to prevent accidental deletion.

5.4. Transmission security: When Bluetooth devices are connected, all communication data is encrypted to ensure the security of the transmission process.

5.5. Prevent accidental deletion: Cleaning software such as Mobile Manager may accidentally delete encrypted files. Please carefully check the "Clear List" when cleaning to avoid checking files related to MOwner.

5.6. Hardware dependency: All encryption, decryption, and login operations must be bound to MOwner Bluetooth hardware. Do not lose or damage the hardware.

FCC Warning:

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.

Caution: Any changes or modifications to this device not explicitly approved by manufacturer could void your authority to operate this equipment.

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, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 0cm between the radiator and your body.

傲然技術有限公司
使用者手冊