# #

Keys Migrate

The keyfile (private key) of irishub v0.16.x uses db storage. The new version v1.0+ will offer a new way to store user private keys. In order to support the migration of the old keyfile to the new version, there are two solutions provided.

# #

Mnemonic

This way is suitable for users who have mnemonic words. When creating a new account, the system will randomly assign a mnemonic phrase to the user, and use this mnemonic phrase to recover the user's private key. Regardless of the v0.16.x version, or v1.0+, the mnemonic phrase remains unchanged. You can use theadd command with the--recover flag to restore the account, for example:

iris keysadd n2--recover

# #

Keystore

This way is suitable for users who have lost the mnemonic but saved the db file of the keys, or the keystore file of the keys. The format of the keystore file of irishub v0.16.x is similar to that of Ethereum, and v1.0+ is also fully compatible with a new format. Therefore, the user can export the old private key using the keystore, and then use the v1.0+ version of irishub to import the keystore to complete the key migration.The operation process is as follows:

1. Use irishub v0.16.x to export keystore file

iriscli keysexport test1 --output-file= key.json--home ./iriscli_test output:

{ "address" : "iaa1k2j3ws7ghwl9qha36xdcmwuu4rend2yr9tw05q" , "crypto" : { "cipher" : "aes-128-ctr" , "ciphertext" : "b5e586baf1126f982ee89ffa9fd23fc68e0a25e1d561d6d59896a0b4878a4d5f" , "cipherparams" : { "iv" : "d02a7b40ce35b6e87f9a395850372bbc" } , "kdf" : "pbkdf2" , "kdfparams" : { "c" : 262144 , "dklen" : 32 , "prf" : "hmac-sha256" , "salt" : "8c77a3a8a75a76da203b262e7fa0187bafbd2ab8bfd3b21ba99f88dcc550d1a6" } , "mac" : "4bdf3fd116a4b9d7eb8846d078399f41a6e271a80678ce8979e4fa86f793cdeb" } , "id" : "c63bdcd2-c470-4c9a-90eb-a4ef6d3d5937" , "version" : "1" } ```

2 . Use irishub v1.0.1 to import keystore file

```bash iris keys import n2 key.json --keyring-backend file 3. Verify the imported key information

iris keys show n2 --keyring-backendfile output:

Enter keyring passphrase: - name: n2 type: local address: iaa1k2j3ws7ghwl9qha36xdcmwuu4rend2yr9tw05q pubkey: iap1addwnpepqgrj4yshwmq7v7akp04empq9rrn6w26e8q6gpl7jkfjaexk93deq2pwa3m6 mnemonic: "" threshold: 0 pubkeys: []
The output account address is consistent with the address in the keystore file, and the migration is successful.
```