Comprehensive Guide to Sovereign Recovery of Theya Wallet

Version: 1.0

Introduction

This guide offers step-by-step instructions for recovering your multisig vault independently using an open-source bitcoin wallet like Sparrow or Electrum. By following this guide, you'll be able to access and manage your funds without relying on Theya's app or services. The most updated version of this guide can also be found on our website.

Prerequisites

Before starting, ensure you have:

- Access to at least two of the three private keys associated with your vault. Please refer to the guide below for instructions on how to export your mobile keys from your Theya vault.
- Access to your wallet's output descriptor. Please refer to the guide below for instructions.
- Latest version of an open-source wallet like Sparrow or Electrum installed on your computer.

Gathering Essential Information

Your output descriptor:

- Open the Theya app on your phone and select the vault you want to transfer from the vault switcher on the top right hand corner.
- Expand the 'More Actions' card on your vault home and select 'Vault settings'.
- Locate and tap on the 'Export Vault Descriptor' menu option.
- You'll be asked to provide your Biometrics for authentication. Post that you will be able to view your vault's descriptor file and copy it. Your descriptor holds crucial information about your vault including your public keys and derivation paths.
- Store this descriptor text securely - you'll need it to re-create your vault using Sparrow wallet.

Export Mobile Private Key:

Note: Exporting your mobile key will deactivate your vault and prevent you from using the Theya vault thereafter. This is done to maintain the security and integrity of your vault.

- Open the Theya app on your phone and select the vault you wish to transfer from using the vault switcher located in the top right-hand corner.
- On the vault home page, expand the 'More Actions' card and select 'Key Management'.

- Choose 'Mobile Key', then select the 'Export Mobile Key' option on the following screen.
- Follow the on-screen instructions to securely export your mobile private key. You will be prompted to provide your biometrics and choose a password for the file containing the mobile key.
- An encrypted document containing your key will be generated which you can save or share from your phone. It's crucial to store this key information securely.

Prepare hardware key (if applicable):

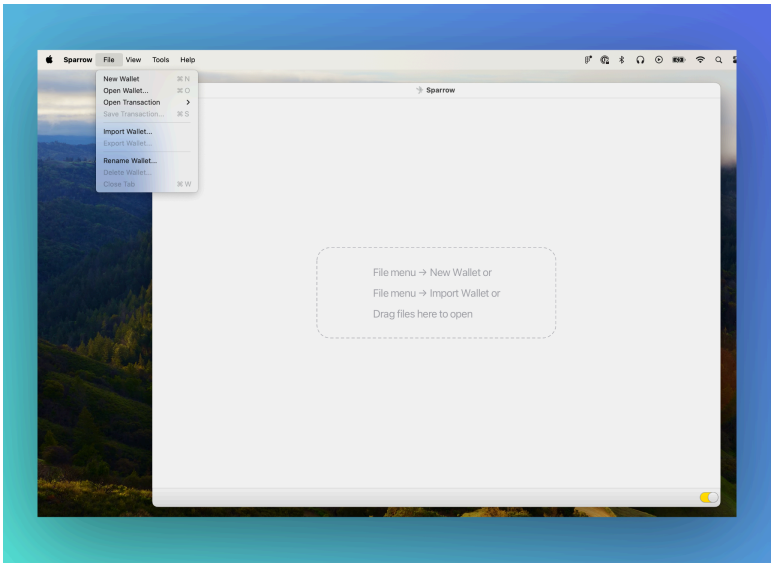
- If you used a hardware key for your vault, make sure that the device is accessible.
- Make sure you have the Ledger Live software installed on your computer to interact with your Ledger device. Update your firmware to the latest version before moving forward.

Recovery Steps

In this section, we will walk you through the detailed steps on how to import the output descriptor and private keys into Sparrow wallet and recreate your multisig Vault.

Recovery Steps

1. Launch Sparrow Wallet:

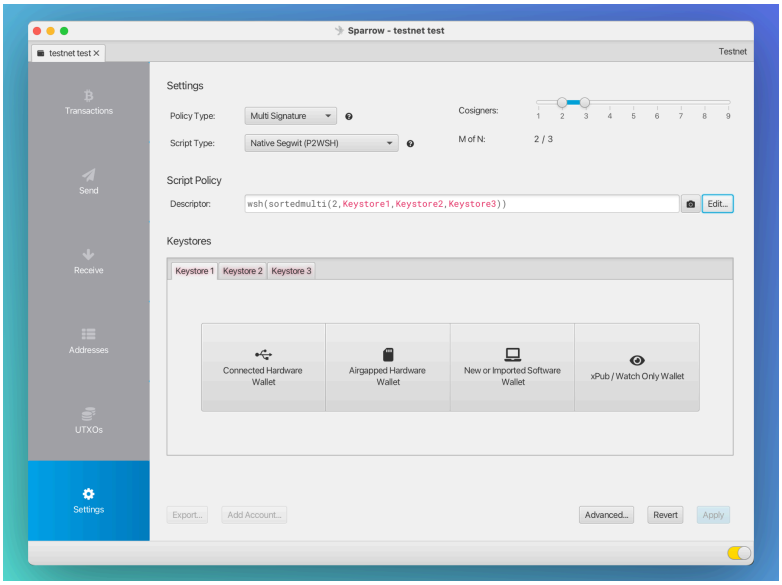


- Double-click the Sparrow Wallet icon on your desktop to open it.
- If it's your first time using Sparrow Wallet, you may be prompted to set up a new wallet.
- Alternatively, you can go to File -> New Wallet to create a new wallet.
- Choose a name for your wallet. This name can be anything you like, it doesn't have to match your Theya vault name.

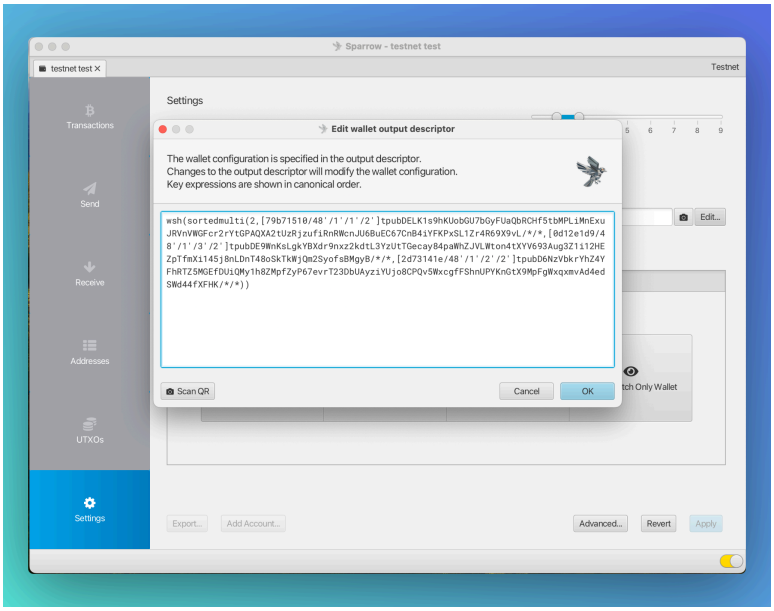
PLEASE NOTE: If you want to recover a *testnet* vault - please go to Menu Bar, find Tools -> Restart in Testnet command. This will relaunch the wallet in testnet mode.

2. Import Output Descriptor:

- On the next screen, navigate to the settings section on the left pane as shown below.

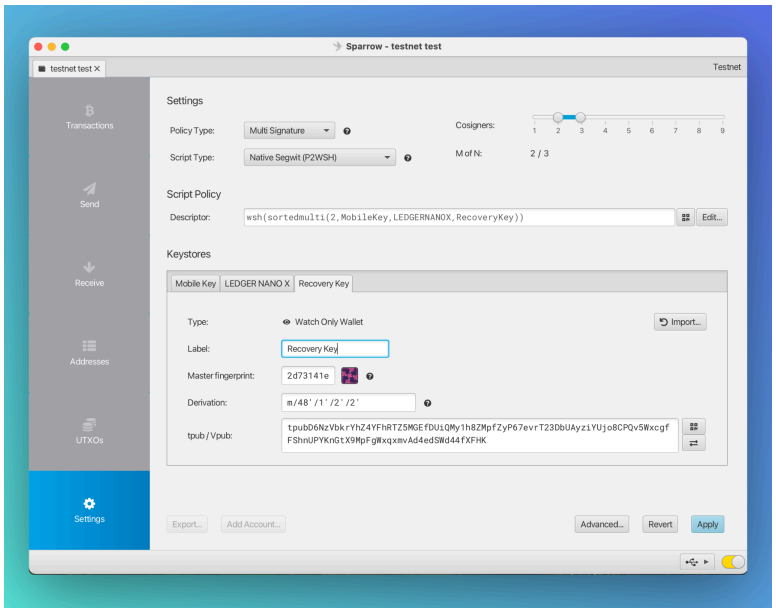


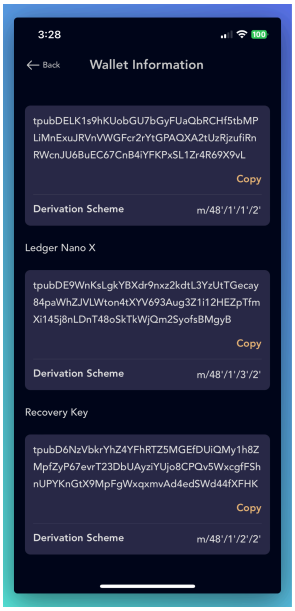
- Select 'multi-signature' as the policy type and make sure to choose the same script type as indicated in your vault settings page, likely P2WSH.
- Paste your output descriptor that you exported from theya's app in the descriptor field under the Script Policy section



- Upon entering your output descriptor, the three keystore sections should automatically populate with your derivation paths and public keys.

- Ensure that the public keys (xpub etc.) and derivation paths match with the values shown on your vault settings page. To avoid any confusion, please rename your keys appropriately by mapping the public key values to the values shown in Theya's app.

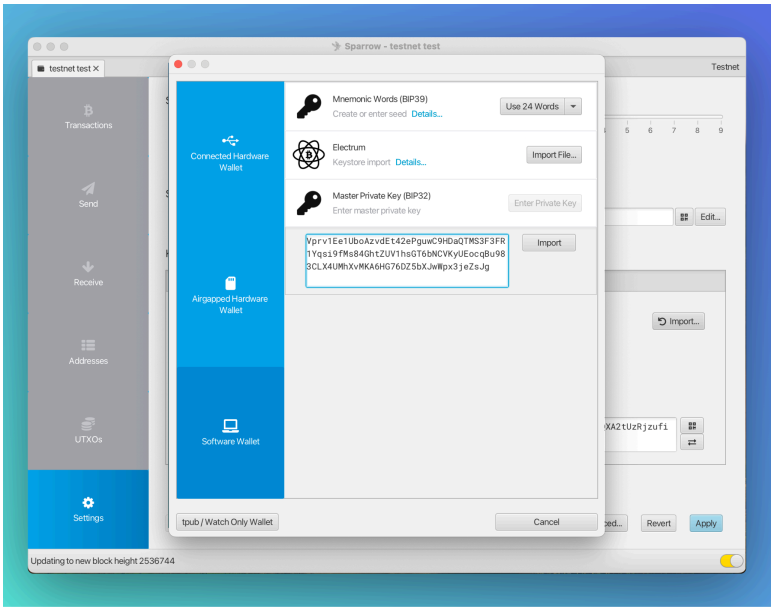


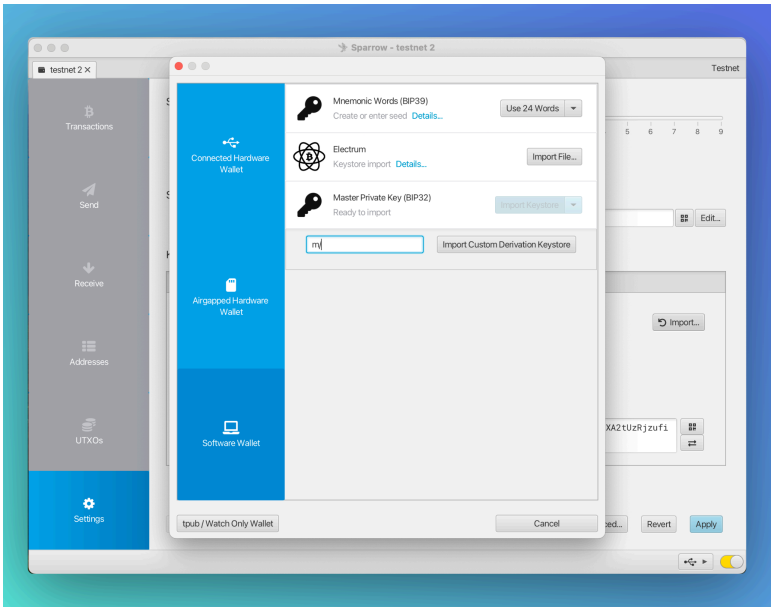


3. Import Private Keys:

Now it's time to import your private keys.

- Go to keystore 1 (your mobile key) and then click on the import button next to Type.
- You'll be prompted to select from three key types. Opt for the 'software key' option, then click on the 'Enter Private Key' button adjacent to the Master Private Key option. Paste your Mobile key that you exported from your Theya vault. Click import and then modify the derivation path to the one shared in your mobile key export file.

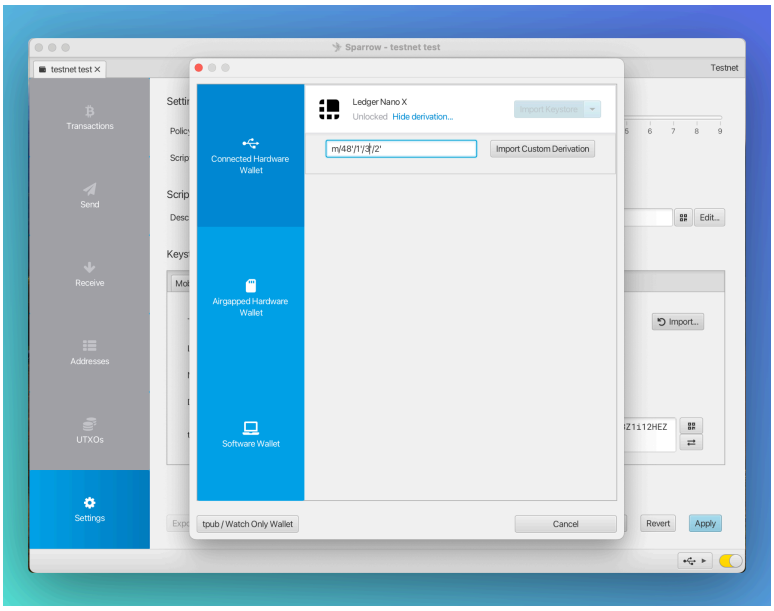




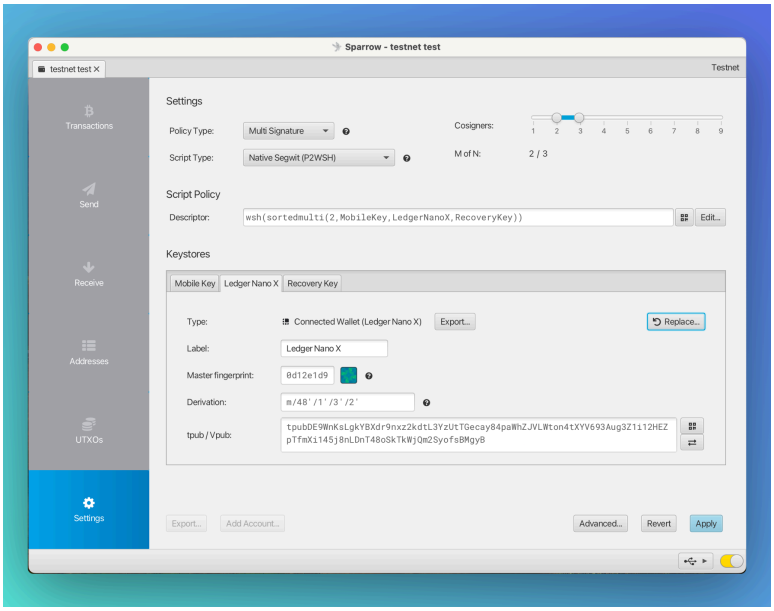
- Depending on your cosigning key type, follow the instructions below:
  <u>For mobile Cosigning key:</u>
  - Navigate to 'keystore 2', select the 'software key' option, and then click on the ‘Enter Private Key’ button next to the Master Private Key option, similar to the previous step.
  - Copy and paste your Cosigner Private Key that you exported from your co-signer’s Theya app into the provided field.

  <u>For Hardware Cosigning key:</u>
  - Turn on your hardware device and connect it to your computer using a USB cable. Enter your PIN and open the Bitcoin app on the device.
  - In Sparrow Wallet, go to 'keystore 2', select 'Connected hardware wallet'. Use the scan feature to locate your hardware key. Sparrow wallet should display your device in the list.

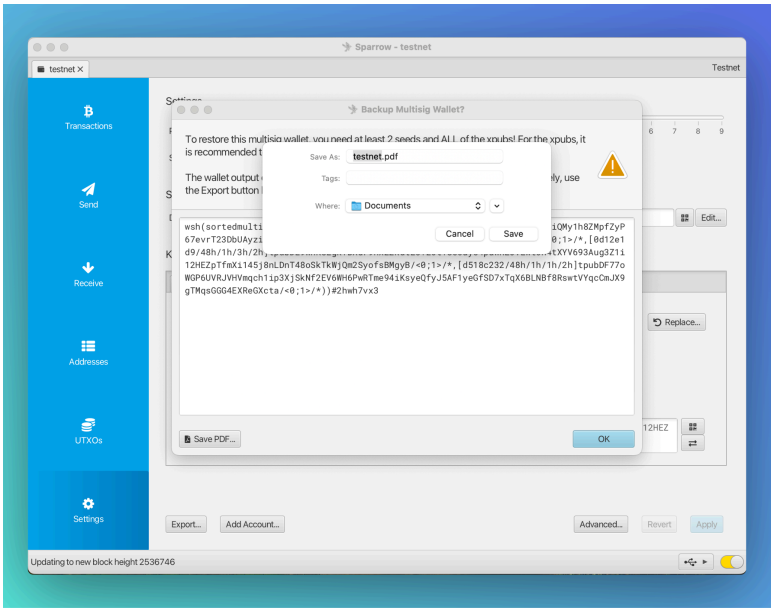
- Locate your device and edit your derivation path to the same one as listed on your hardware public key on Theya's app. Click on import custom derivation to import this key to your Sparrow Wallet.



- Once your two keys are added, click on apply on the bottom right section of your sparrow wallet.



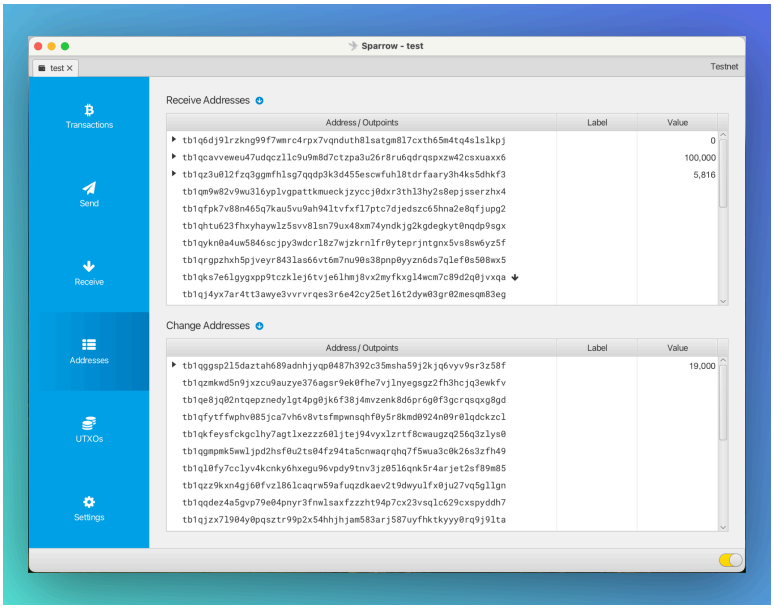
- Sparrow will prompt you to select a password to protect your wallet. You can leave these fields blank if you don't want to set a password.
- Sparrow wallet will prompt you to save a backup copy of your wallet. If you choose to do this, please store this file somewhere safe and private.



- After you proceed, Sparrow Wallet should automatically reconstruct your multisig wallet.
- Once the wallet syncs, you would be able to see all your transactions and your balance in the Sparrow app.

4. Verify Your Multisig Wallet:

- Ensure all wallet addresses and transaction history match the records from our app.



- You now have full control over your funds and can manage your multisig wallet independently through Sparrow Wallet. Your software keys on Sparrow plus (optionally) your hardware keys can be used to send funds out of your wallet if you choose to.

5. Secure Your Recovery Information:

- It's crucial to store your Output Descriptor file, private keys, and your wallet back up (optional) securely.
- Consider using a secure offline storage medium like a safety deposit box or a secure USB flash drive stored in a safe location.

For any additional support or inquiries, you can refer to the Sparrow Wallet documentation or contact our support team.