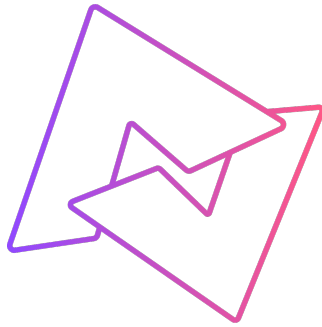




Stashi Wallet

User guide

Setup, recovery, payments, privacy, key management, verification, and troubleshooting.

Mobile and desktop

Pirate Chain Foundation

Contents

Stashi Wallet user guide	5
Mobile and desktop layouts	5
Getting help	5
Install and set up Stashi Wallet	6
Download the file	6
Open Stashi Wallet	6
Create a new wallet	7
Import an existing wallet with a seed phrase	9
Create a view-only wallet	11
After setup	12
Wallet basics	13
Home	13
Wallets	14
Activity	14
Settings	15
Navigation on different screen sizes	16
Receive and send ARRR	17
Receive ARRR	17
Send ARRR	18
Source selection and available funds	18
Multiple recipients	19
Auto consolidation	19
Sweep a spending key	19
Seed accounts, keys, and addresses	20
Seed accounts	20
Imported spending keys	21
Imported viewing keys	22
Sapling and Ironwood	23
Diversified addresses	23
Spending key details and export	24
Seed account controls for imported keys	24
Move from Treasure Chest or Pirate Wallet Lite	25
Before you begin	25
Import the seed phrase	25

Find funds in higher seed accounts	25
Import separate keys	26
If the previous wallet shows more history	26
Finish moving the wallet safely	27
Network privacy and synchronisation	28
Transport choices	28
Node selection	29
Synchronisation stages	29
Cached blocks and rescans	30
If Preparing sync does not finish	30
Rescan the wallet	30
Backups and wallet security	31
What protects the funds	31
Back up the seed phrase	31
Back up imported keys	31
Local passphrase	31
Biometrics	32
Duress passphrase	32
Before deleting or resetting anything	32
Settings and release verification	33
Settings map	33
Outbound API Calls	33
Currency, language, and theme	34
Birthday height	34
Verify the Stashi Wallet installation	35
Verify the downloaded release files	37
Debug logging	37
Troubleshooting	39
Missing balance or transaction	39
Stuck on Preparing sync	39
Fiat value is blank	39
Insufficient funds when the total balance is larger	40
Verify build cannot download files	40
AppImage does not open	40
Interface looks too large on a laptop	40
Send failed	41
Information for a support report	41

Advanced use	42
Manage several wallets	42
Exact birthdays and controlled rescans	42
Manual light-server configuration	42
SOCKS5 and I2P details	42
Address management	42
Seed accounts and sparse account layouts	43
Payment disclosure	43
Swaps	43
Local privacy data	43
Independent release verification	44

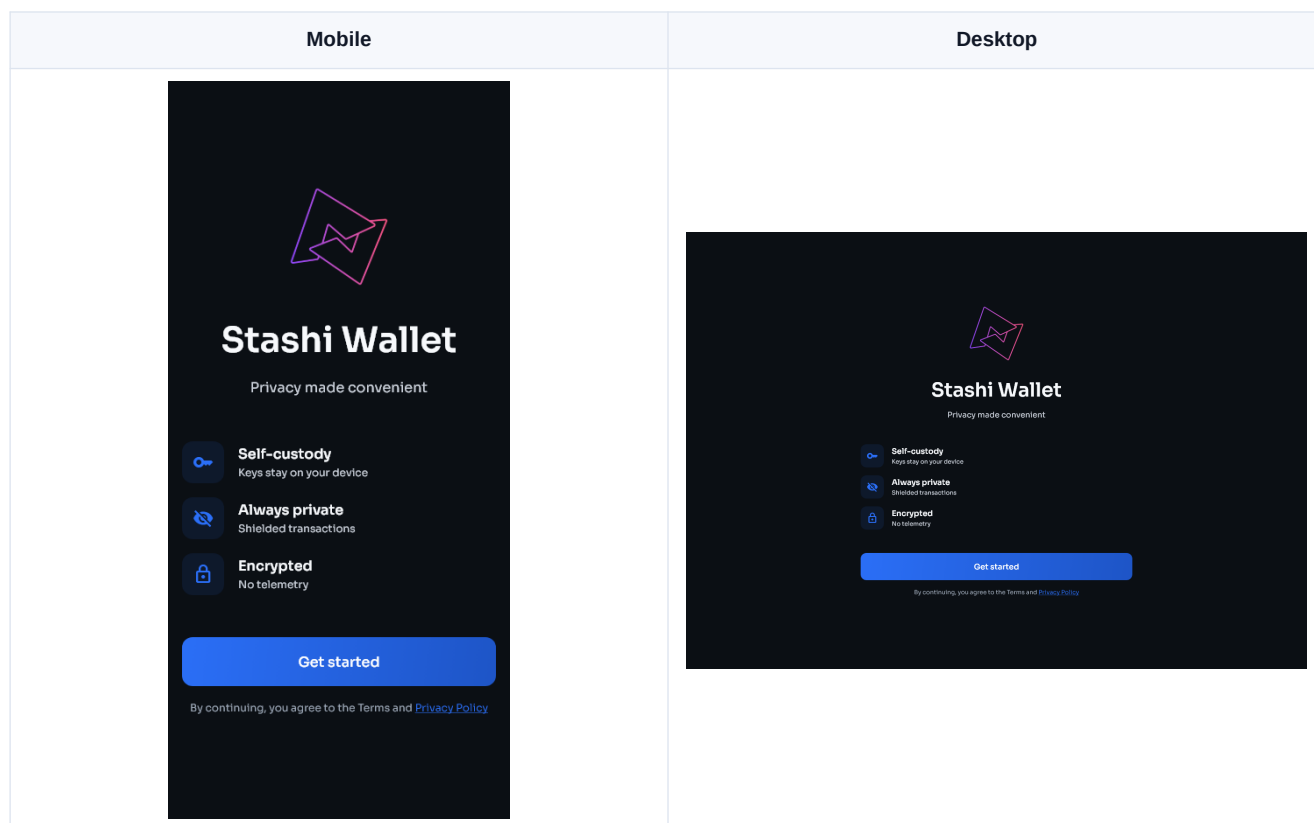
Stashi Wallet user guide

This guide explains how to set up and use Stashi Wallet for ARRR, recover a wallet, manage privacy settings and keys, verify a release, and resolve common problems.

If you are moving from Treasure Chest or Pirate Wallet Lite, start with [Moving from another Pirate Chain wallet](#).

Mobile and desktop layouts

The same controls are available on mobile and desktop devices. Information is arranged vertically on a mobile device, so some pages require scrolling. Related information may appear side by side in a wide desktop window.



Getting help

Read [Troubleshooting](#) before asking for help. It explains which details are safe to share and how to create a useful debug log. Never send a seed phrase or private key to support staff.

Install and set up Stashi Wallet

[Guide contents](#) | [Next: Wallet basics](#)

Download the file

Download Stashi Wallet from the [official Pirate Unified Wallet releases on GitHub](#) or the [Pirate Chain Wallets page](#). Do not install wallet files received through direct messages or file-sharing websites.

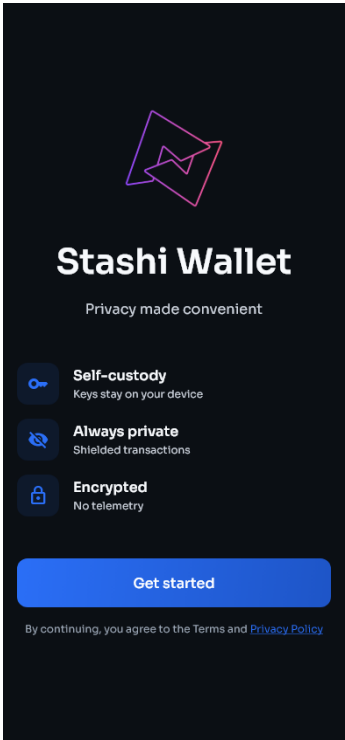
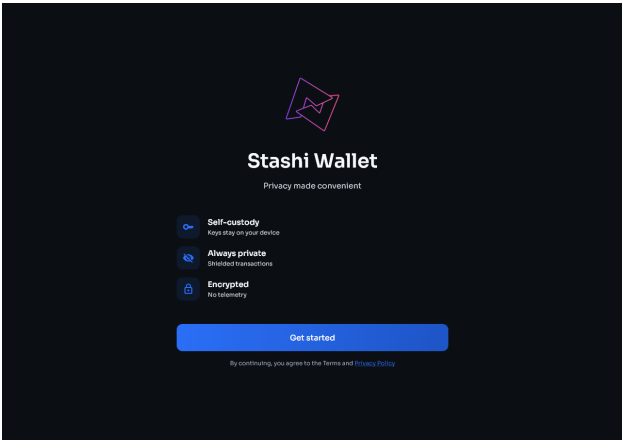
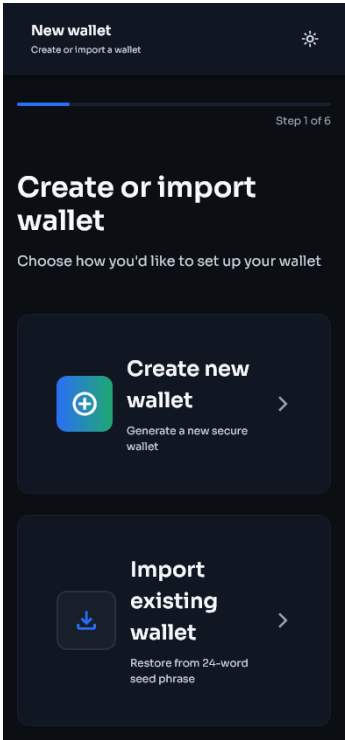
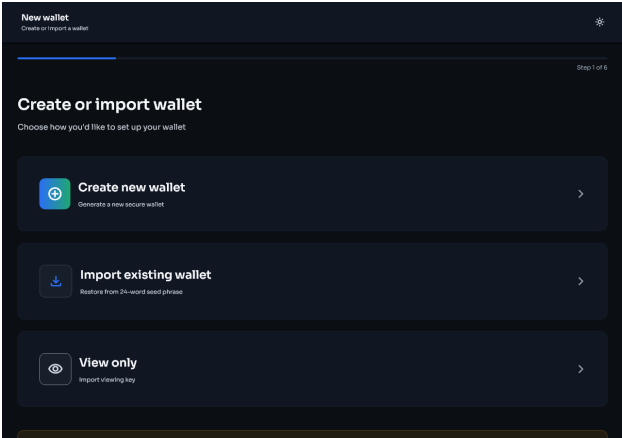
Select the package for your device:

- For Windows, download `Stashi-Wallet-windows-installer.exe`.
- For macOS, download `Stashi-Wallet-macos.dmg`. The package supports Apple Silicon and Intel Macs.
- For Linux, select the format supported by your distribution:
 - Download `Stashi-Wallet-linux-x86_64.AppImage` for a portable file that runs on most 64-bit Linux distributions without installation.
 - Download `Stashi-Wallet-amd64.deb` for a Debian-based distribution such as Debian, Ubuntu, Linux Mint, Pop!_OS, or Zorin OS.
 - Download `Stashi-Wallet.flatpak` if your distribution supports Flatpak or you normally install applications through Flatpak. Fedora, Endless OS, and many other distributions can use this format after Flatpak is enabled.
- For Android, use `Stashi-Wallet-android-V8.apk` on a current 64-bit ARM mobile device or tablet. Use `Stashi-Wallet-android-V7.apk` only on an older 32-bit ARM device that cannot install the V8 package.
- Stashi Wallet is not yet distributed for iPhone or iPad. Until an iOS version is available, use a third-party wallet with Pirate Chain support, such as Edge.

The release includes SHA-256 checksums and PGP signatures. See [Verify the downloaded release files](#) to check the files before installation.

Open Stashi Wallet

- 1 Install or open Stashi Wallet.
- 2 Confirm that the name and icon match the official release.
- 3 Select **Get started** on the welcome screen.
- 4 Select **Create new wallet**, **Import existing wallet**, or **View only**.

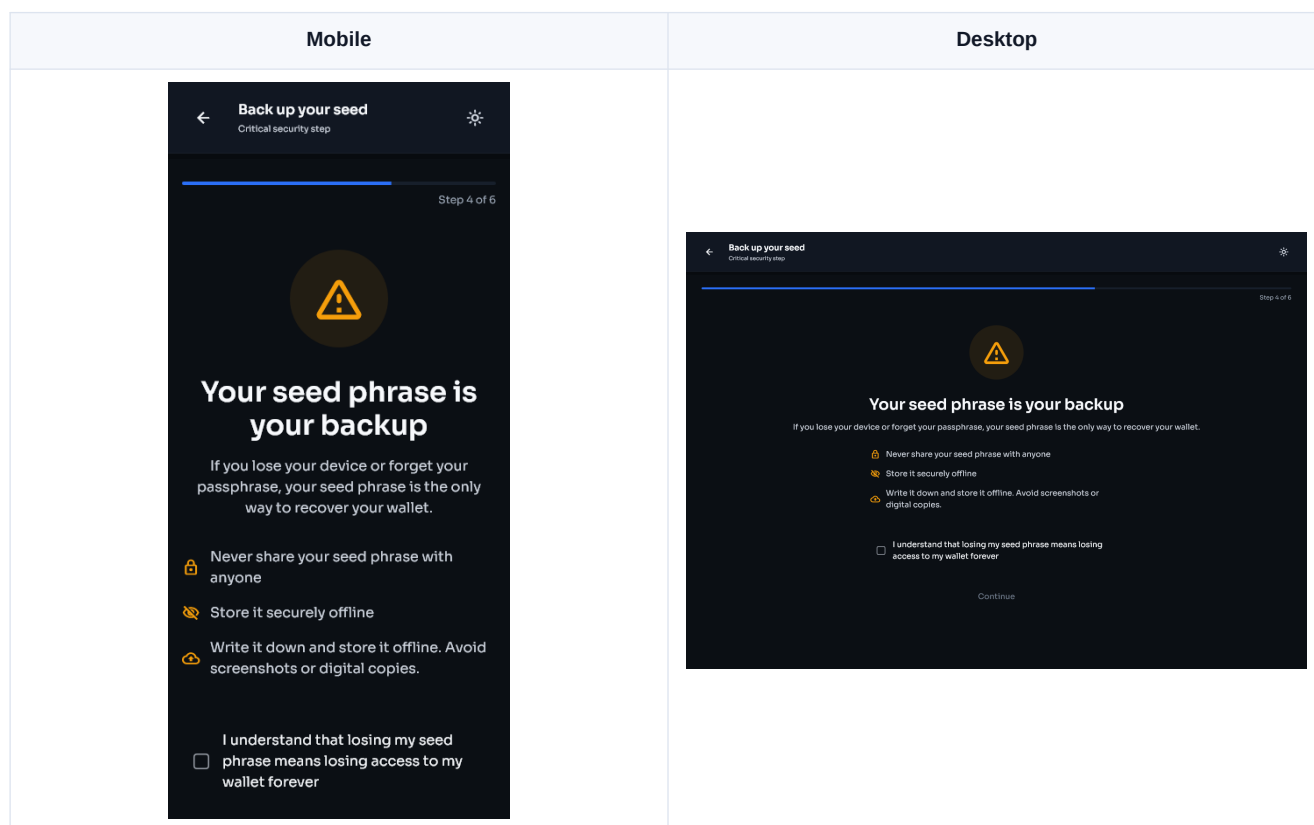
Mobile	Desktop
	
Setup choices on mobile	Setup choices on desktop
	

Create a new wallet

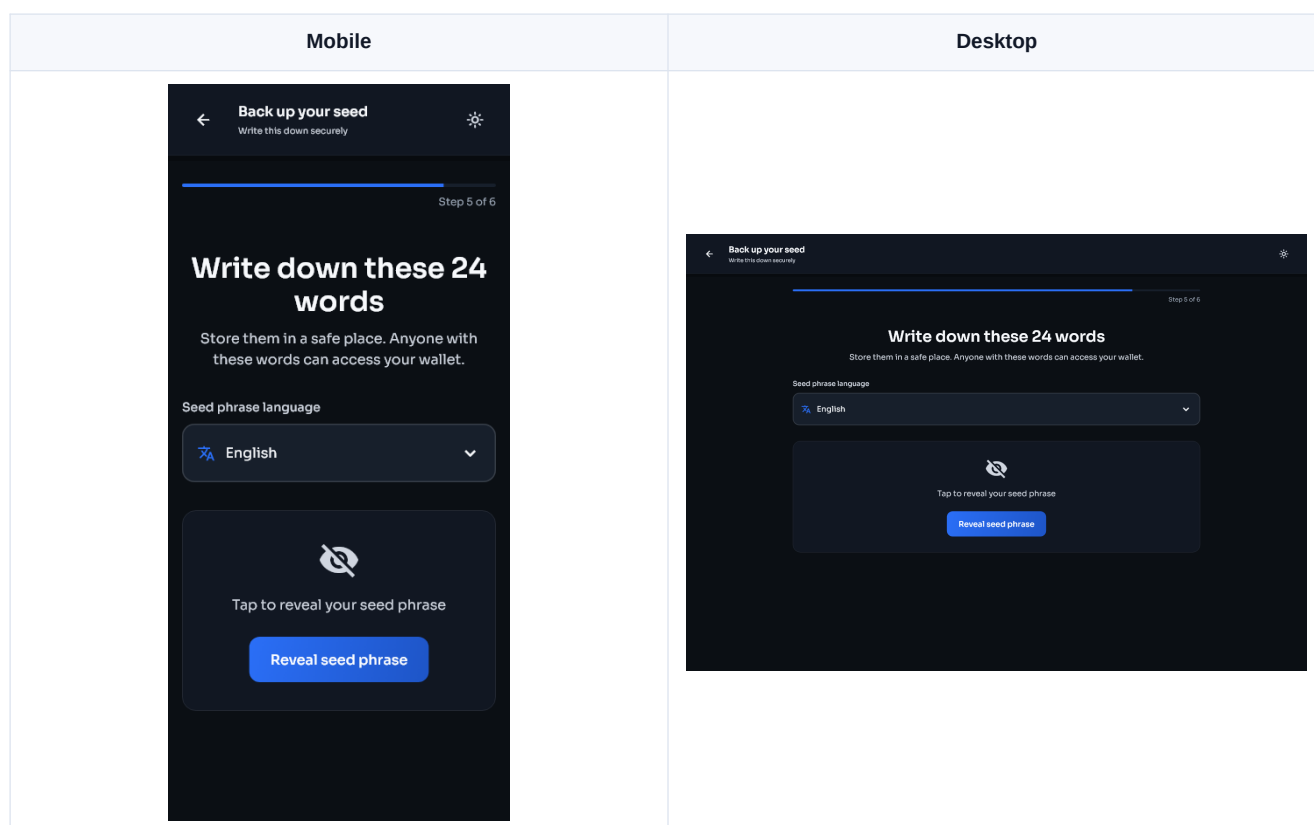
A local passphrase works like a password for Stashi Wallet on this device. It must contain at least 12 characters, including letters, numbers, and symbols. A passphrase of at least 16 characters is recommended. It cannot read the same forwards and backwards. Use a unique passphrase that you do not use for another account.

The 24-word seed phrase controls the funds in a seed-derived wallet. Anyone who obtains the words can spend the funds. The local passphrase protects the wallet on this device, but it cannot replace or recover a lost seed phrase.

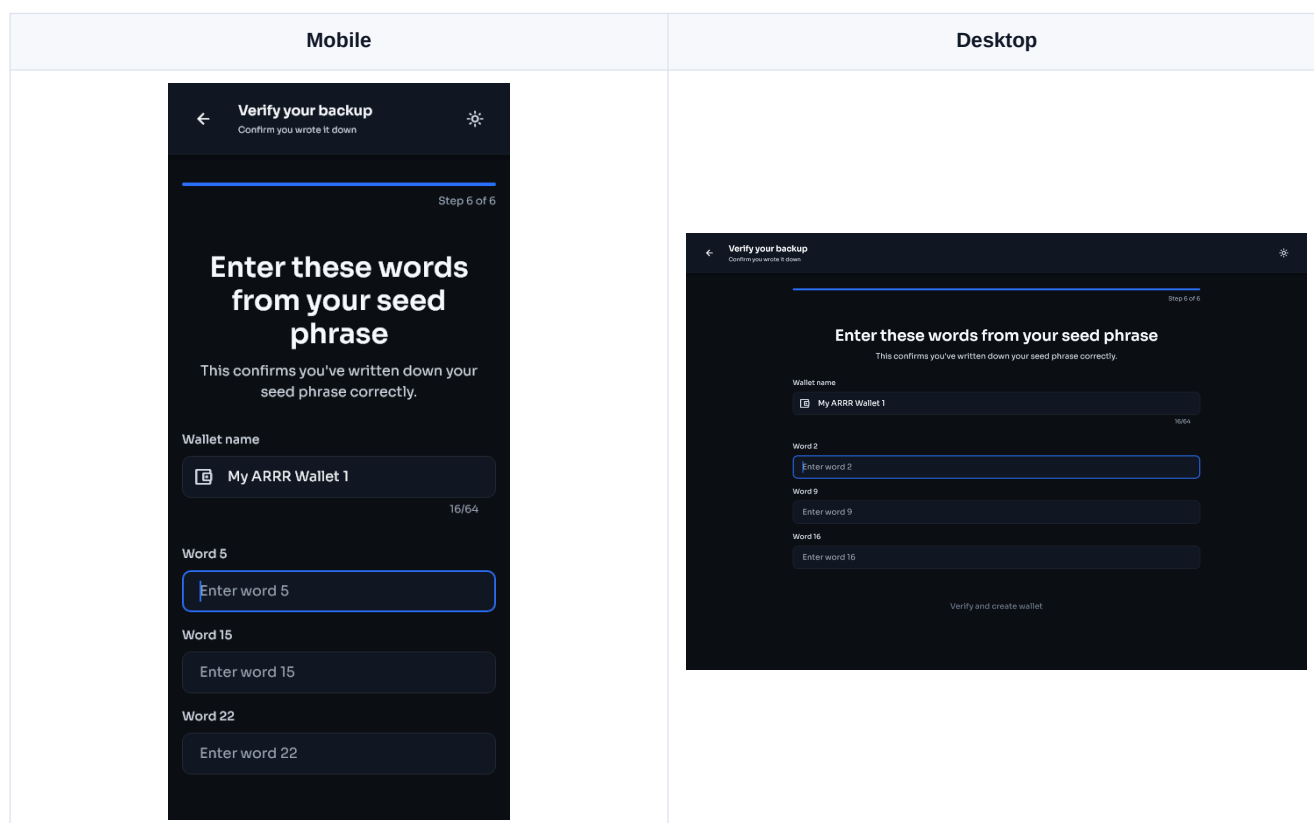
- 1 Select **Create new wallet**.
- 2 Create the local passphrase.
- 3 Enable device biometrics if you want faster unlocking. Biometrics do not replace the seed phrase.
- 4 Read the backup warning.
- 5 Write the 24 words of the seed phrase on paper or another offline medium, in the exact order shown.
- 6 Review the suggested wallet name. New wallets start with **My ARRR Wallet 1** and continue with the next number. You can edit the name before creation.
- 7 Confirm the requested words.
- 8 Store the seed phrase somewhere protected from theft, fire, and water.
- 9 Wait for synchronisation to finish before relying on the displayed balance.



The phrase language control appears above the seed words. Leave it set to the language used for the backup.



The final confirmation page allows you to name the wallet before it is created.



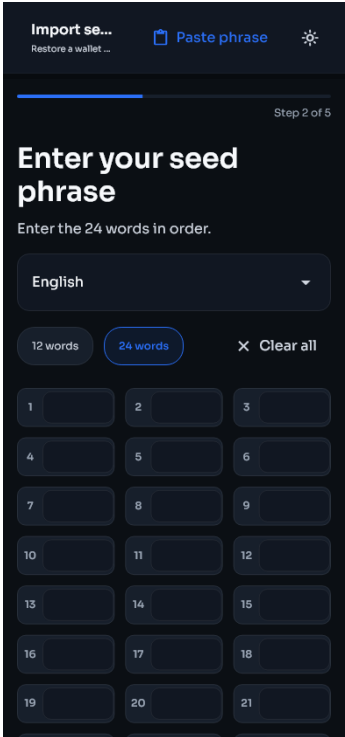
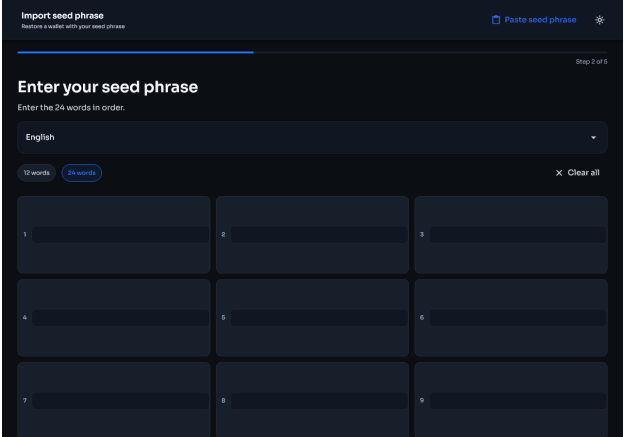
Do not photograph the seed phrase, store it in a cloud note, send it by email, or enter it into a website.

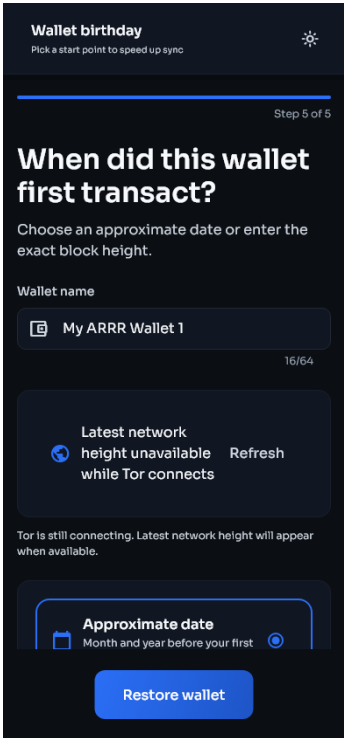
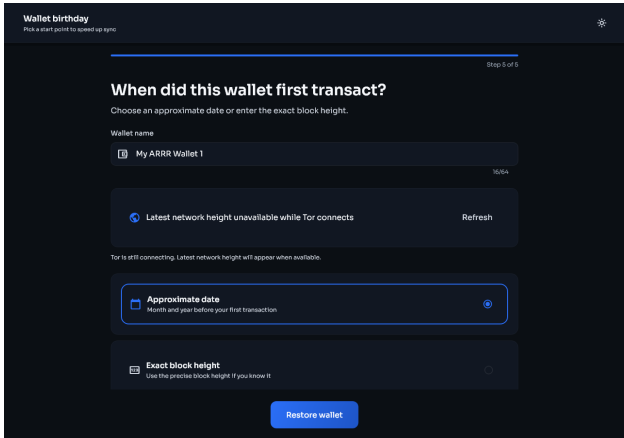
Import an existing wallet with a seed phrase

- 1 Select **Import existing wallet**.

- 2 Select the language of the seed phrase if it is not already selected.
- 3 Enter all 24 words in order. Check the spelling and language if the seed phrase is rejected.
- 4 Create the local passphrase and decide whether to enable biometrics.
- 5 Review or change the suggested wallet name.
- 6 Enter the wallet birthday height. Use a block height from before the wallet first received funds. An earlier height is safe but requires more time to scan.
- 7 Finish the setup and allow the scan to complete.
- 8 Check the balance and Activity page.
- 9 If the previous wallet used additional ZIP-32 seed accounts, follow [Find funds in higher seed accounts](#).

The birthday height is the earliest blockchain height that Stashi Wallet will inspect for this wallet. It is not the wallet creation date. Enter a height before the first expected transaction so that earlier activity is not excluded.

Mobile	Desktop
	

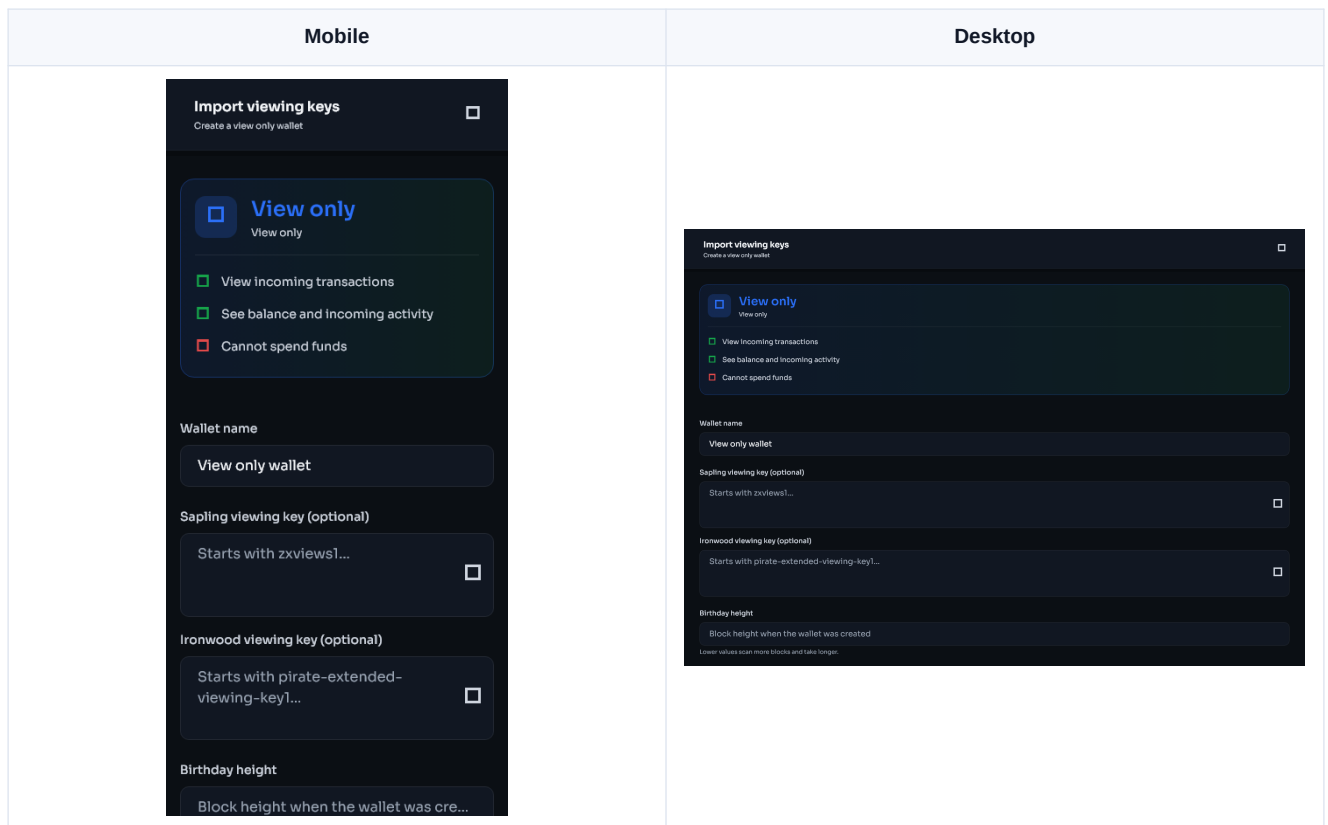
Wallet name and birthday height on mobile	Wallet name and birthday height on desktop
	

Importing the seed phrase does not restore private keys that were imported separately. Import those keys again under **Settings > Keys & addresses**.

Create a view-only wallet

A view-only wallet can monitor supported shielded activity but cannot spend the funds.

- 1 Select **View only**.
- 2 If this is the first wallet on the device, create a local passphrase and choose whether to enable biometric unlocking. If Stashi Wallet is locked, unlock it before continuing.
- 3 Enter a wallet name.
- 4 Enter a Sapling viewing key, an Ironwood viewing key, or both in the matching fields.
- 5 Enter a birthday height from before the first transaction for the viewing key.
- 6 Finish the setup and allow the scan to complete.



A Sapling viewing key begins with `zxviews1`. An Ironwood viewing key begins with `pirate-extended-viewing-key1`. Paste each key into the matching field. Keep viewing keys private because they can reveal transaction information within their scope.

After setup

Confirm the following points before receiving a payment:

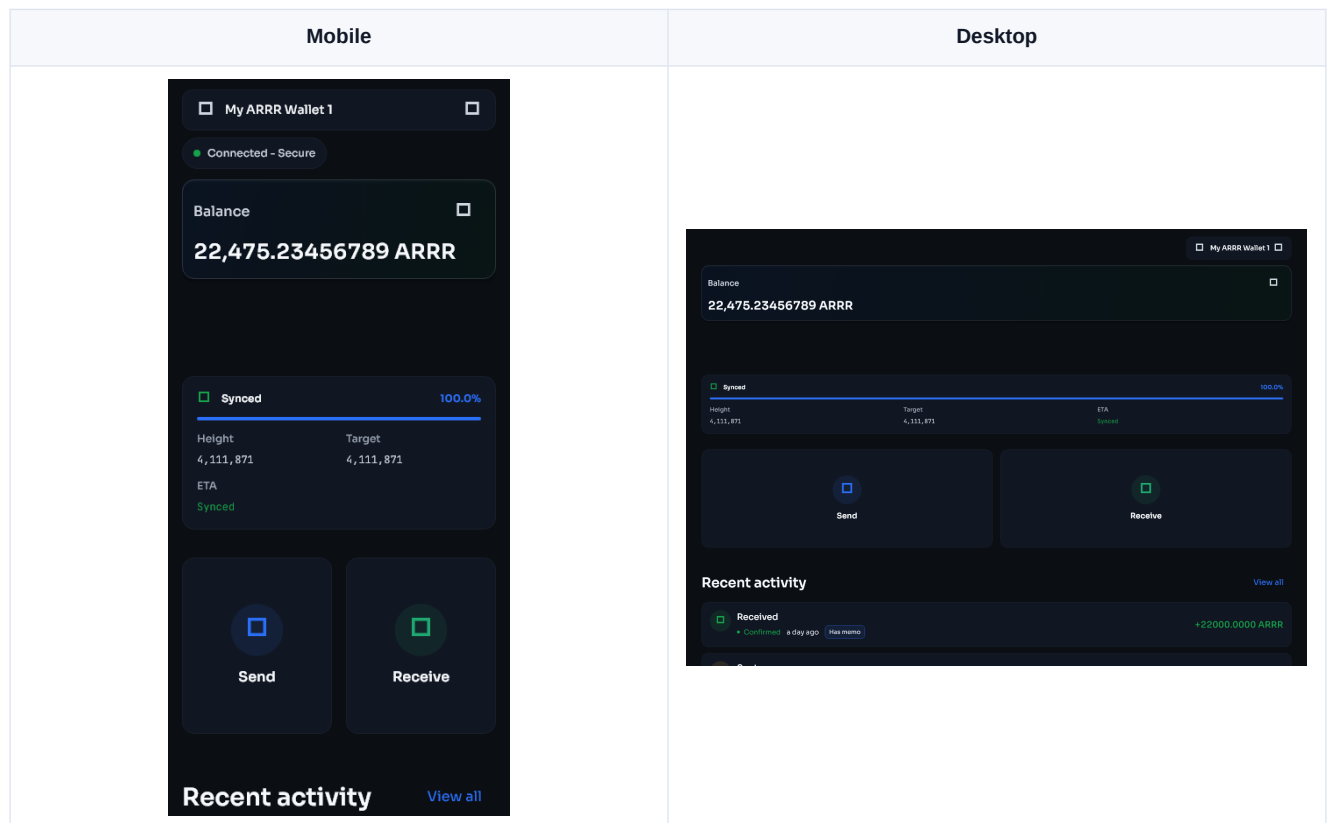
- The wallet opens with the passphrase or biometric method that you expect.
- You have checked the seed phrase backup twice.
- The network status shows a connection, and synchronisation has reached the current chain height.
- You can open **Receive**, generate an address, and copy it.
- The wallet selected at the top of the screen is the wallet that you intend to use.

Wallet basics

[Previous: Getting started](#) | [Guide contents](#) | [Next: Send and receive](#)

Home

The Home page shows the selected wallet, connection status, balance, fiat estimate, synchronisation progress, and shortcuts for common tasks.



Wallet selector

Use the wallet name at the top of the page to switch between wallets. Check the selected wallet before copying an address, importing a key, or sending funds.

Connection status

The connection status indicator reports whether Stashi Wallet is connected. When it shows **Connected - Secure**, select it to view the active privacy transport, such as Direct, Tor, SOCKS5, or I2P when available. A connection does not confirm that blockchain processing has finished. Check the synchronisation information as well.

Balance information

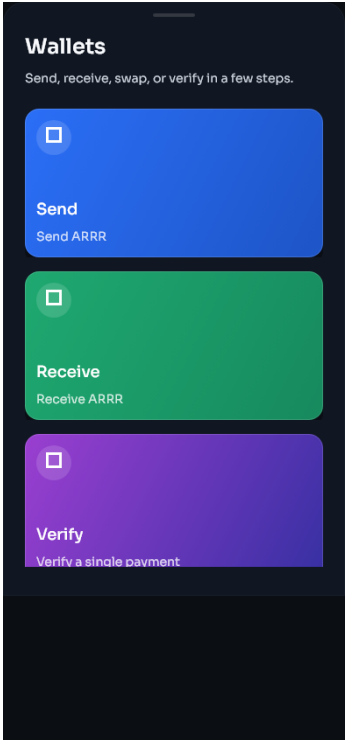
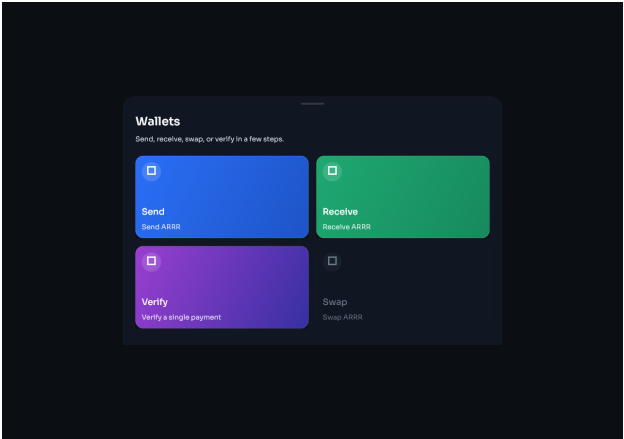
- The main balance shows the wallet's ARRR amount.
- Use the hide or show icon, represented by an eye, to hide or show the values.
- The estimated fiat value appears in smaller text and uses the currency selected under Settings.
- Use the switch icon, represented by two arrows, to exchange the positions of the ARRR and fiat values.
- Fiat prices come from an external price service and can be temporarily unavailable. This does not affect the ARRR balance.

Synchronisation information

The synchronisation area shows the current stage, blockchain height, progress, and estimated completion time when available. Common stages include **Preparing sync**, downloading, scanning, and **Synced**. Keep the application open if the operating system restricts background activity.

Wallets

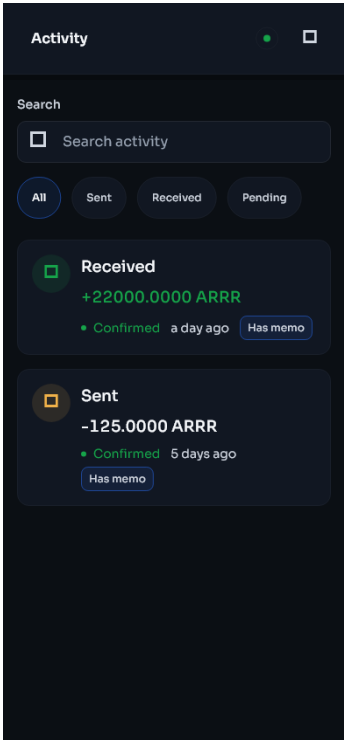
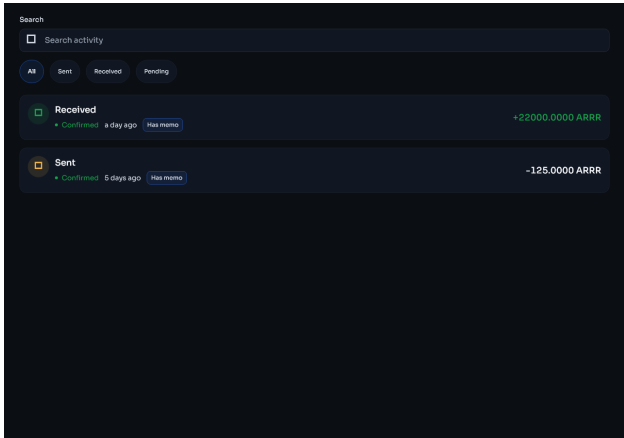
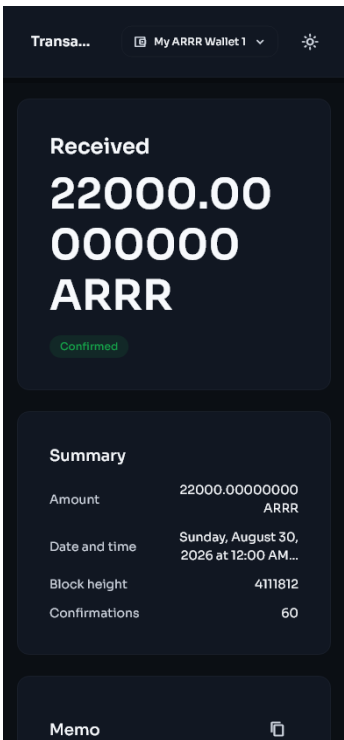
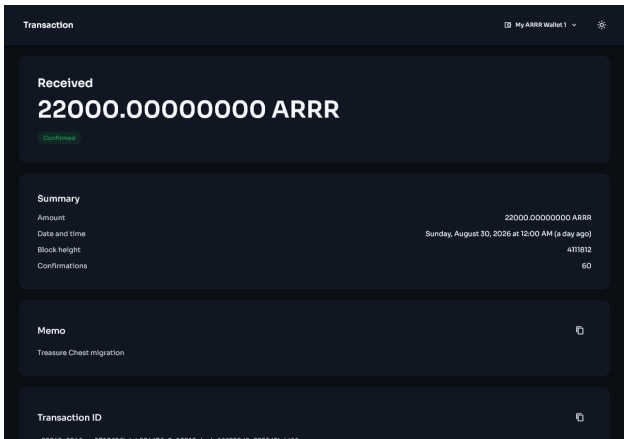
The Wallets page provides access to send, receive, swap, and payment verification tools.

Mobile	Desktop
	

Scroll on a small screen to view every available action. Depending on the selected wallet and available features, the page can include send, receive, sweep, swap, and payment disclosure tools.

Activity

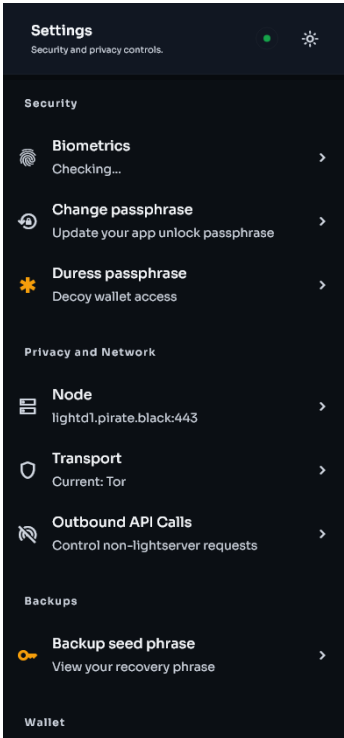
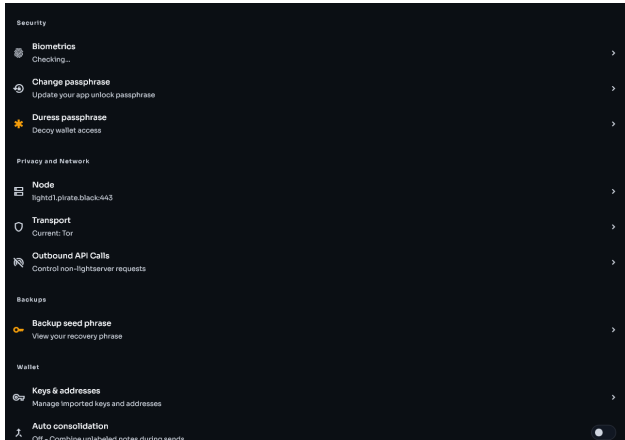
Activity lists the wallet transactions that Stashi Wallet has detected. Open a transaction to view its direction, status, amount, fee, memo, available addresses, block information, and transaction ID.

Mobile	Desktop
	
Transaction details on mobile	Transaction details on desktop
	

New transactions can appear before final confirmation. Do not treat an unconfirmed incoming payment as final. If an expected transaction is absent, wait for full synchronisation and follow [Missing balance or transaction](#).

Settings

Settings contains security, network, backup, key, appearance, synchronisation, diagnostics, and release verification controls.

Mobile	Desktop
	

Navigation on different screen sizes

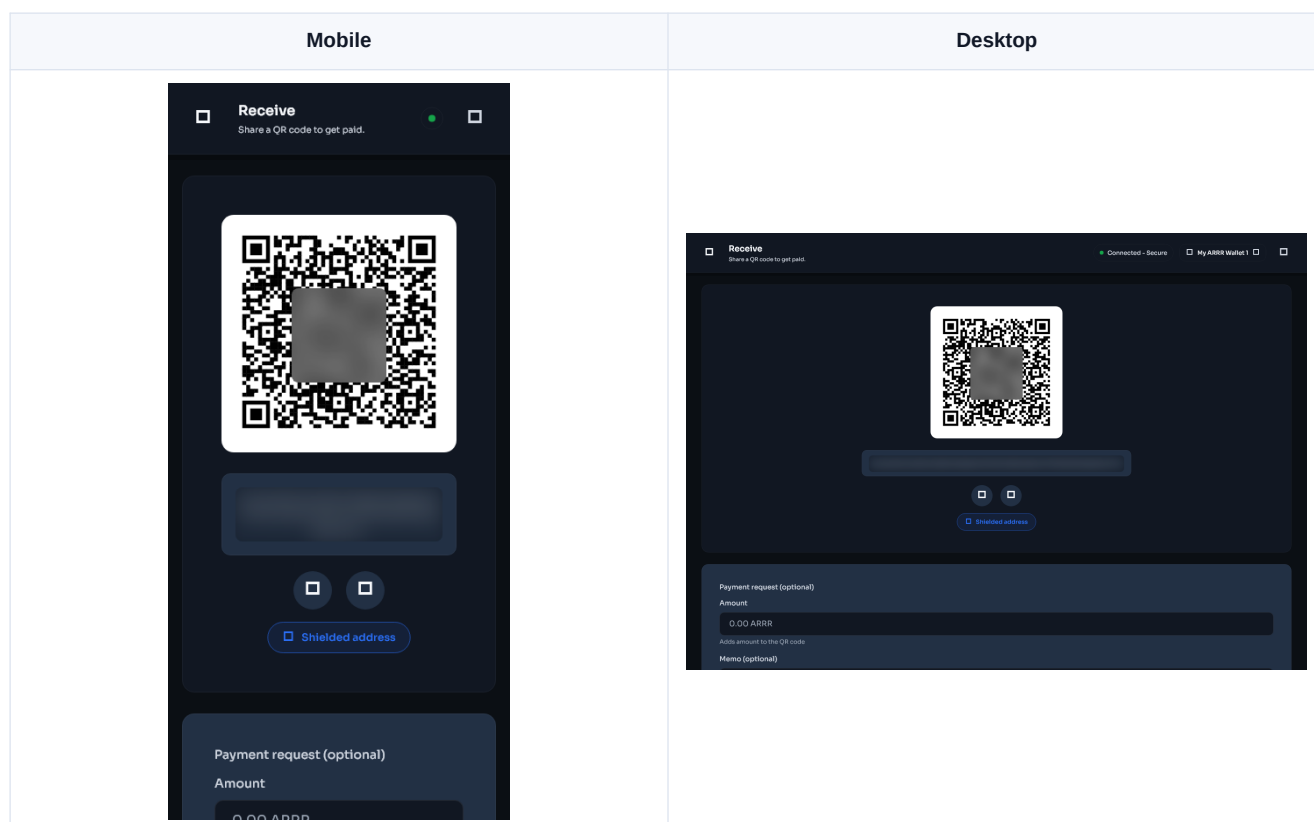
- On a mobile device, use the navigation bar at the bottom and scroll long pages vertically.
- On a desktop computer or tablet, navigation may use more horizontal space, and related information may appear in columns.
- With a keyboard, use Tab and Shift+Tab to move between controls. Use Enter or Space to activate a control, and use Escape to close a dialogue where supported.

Receive and send ARRR

[Previous: Wallet basics](#) | [Guide contents](#) | [Next: Keys and accounts](#)

Receive ARRR

- 1 Open **Receive** from Home or Wallets.
- 2 Confirm the wallet and key shown on the page.
- 3 Generate or select the address that you want to use.
- 4 Add a local label if it will help you recognise the payment later.
- 5 Copy the address or allow the sender to scan the QR code.
- 6 Check that the beginning and end of the copied address match the address shown by Stashi Wallet.
- 7 Give the sender only the payment address or payment QR code.
- 8 Wait for the transaction to appear in Activity and receive confirmations.



The operating system may hide sensitive text in screenshots or screen sharing. Use the copy button in Stashi Wallet when you need the full address.

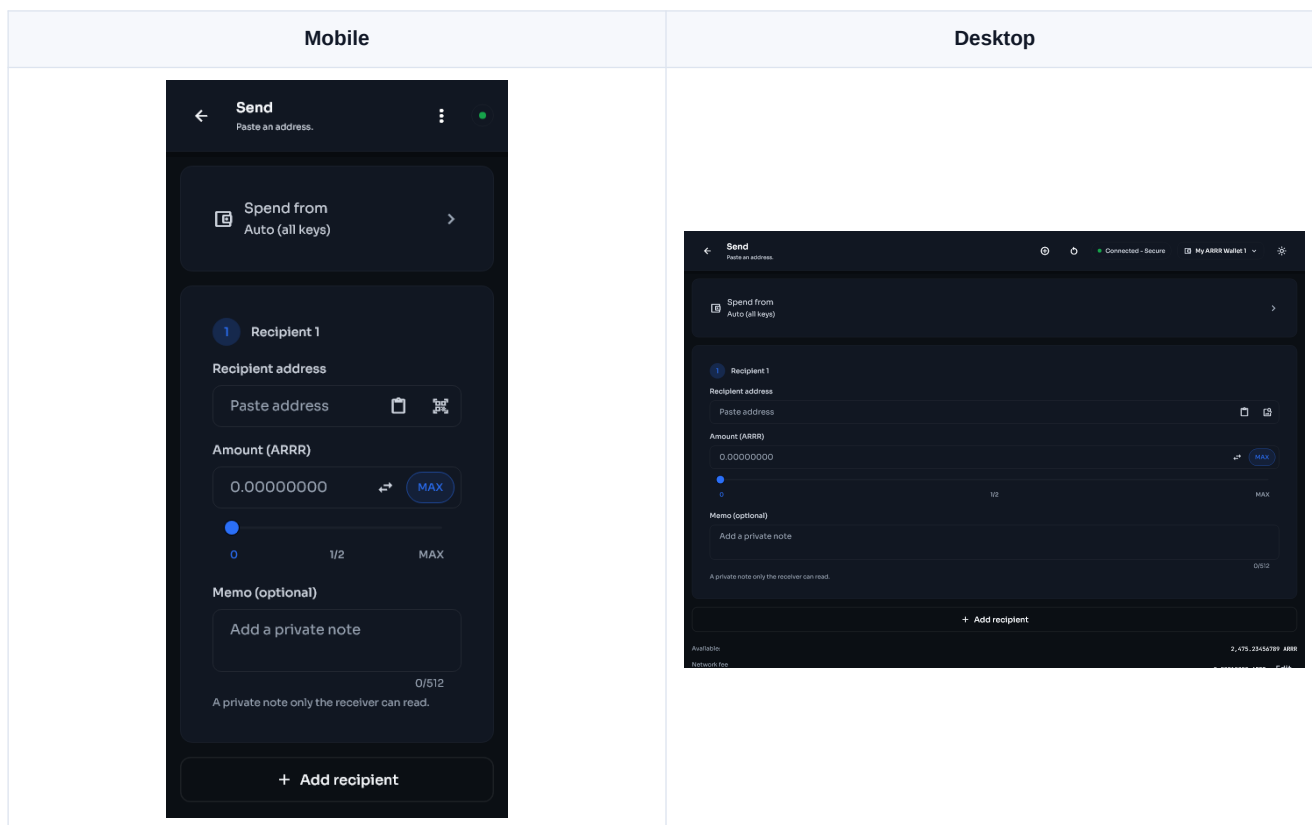
Address rotation

Stashi Wallet can generate diversified addresses for supported keys. A new address helps prevent different payments from being linked by the address alone. Previously generated addresses remain valid.

Address labels and colour tags are local organisation tools. They are not written to the blockchain and are not sent to the payer.

Send ARRR

- 1 Open **Send**.
- 2 Paste the recipient address, scan a QR code, or import a QR image where supported.
- 3 Confirm that the address is a Pirate Chain address from the intended recipient.
- 4 Enter the amount.
- 5 Add a memo only if the recipient expects you to include a message. A memo may be visible to the recipient and to anyone who later obtains the relevant viewing authority.
- 6 Review the source selector. **Auto (all keys)** allows Stashi Wallet to choose spendable notes across eligible keys. Select a specific key only when you need to control the source.
- 7 Review the network fee and total.
- 8 Continue to the confirmation screen.
- 9 Check the address, amount, memo, fee, and source again.
- 10 Approve the transaction with the requested passphrase or biometric check.
- 11 Keep the transaction ID until the recipient confirms receipt.



Blockchain transactions cannot be cancelled after broadcast. Send a small test payment first when using a new address or sending a large amount.

Source selection and available funds

The total wallet balance can be larger than the amount available to a selected key. If a specific source reports insufficient funds, select **Auto (all keys)** or select a source with enough confirmed spendable notes.

Pending funds, immature funds, and notes reserved by another transaction are not immediately spendable. The review screen includes the fee in the required total.

Multiple recipients

When the Send page supports additional recipients:

- 1 Add a separate row for each recipient.
- 2 Verify every address and amount separately.
- 3 Confirm that the displayed total includes all outputs and the fee.
- 4 Remove empty or accidental rows before confirming.

Auto consolidation

Many small notes can make transaction construction slower or exceed transaction limits. Auto consolidation can combine suitable notes during a send. It does not change wallet ownership, but it creates normal on-chain transactions and fees may apply. Review this setting under **Settings > Wallet > Auto consolidation**.

Sweep a spending key

Sweeping moves the spendable balance controlled by a selected spending key to an address that you choose. Use it when retiring a key or consolidating custody.

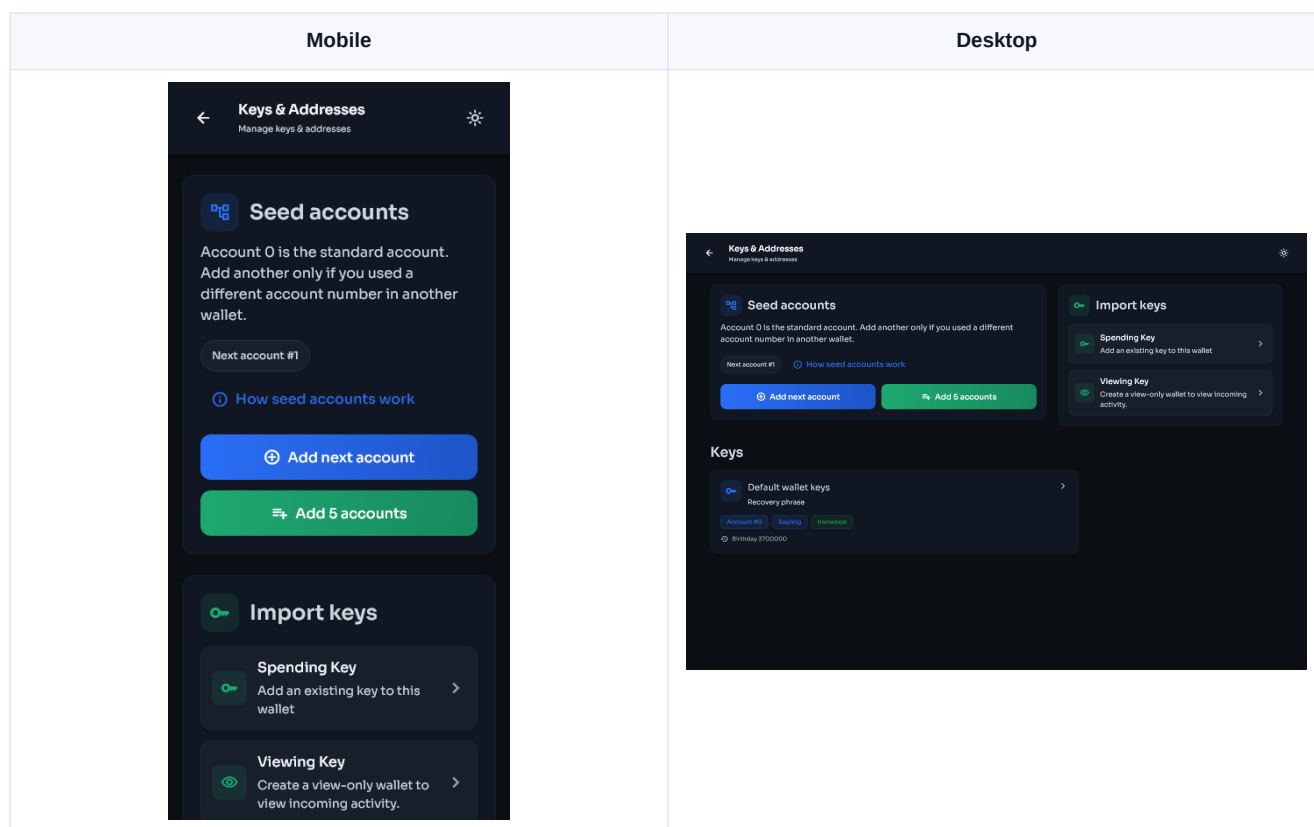
- 1 Open **Settings > Keys & addresses**.
- 2 Open the spending key.
- 3 Select the sweep action.
- 4 Select all addresses or the specific source offered by Stashi Wallet.
- 5 Enter and verify the destination.
- 6 Review the full amount and fee before approving the transaction.

Do not sweep funds to a destination until you have confirmed that its seed phrase or imported spending key is backed up.

Seed accounts, keys, and addresses

[Previous: Send and receive](#) | [Guide contents](#) | [Next: Moving from another wallet](#)

Open **Settings > Keys & addresses** to view the key groups available to the selected wallet.



Seed accounts

A seed phrase can derive many numbered ZIP-32 accounts. Account 0 is the standard account used by most wallets. Accounts 1, 2, and higher are separate account key groups derived from the same seed phrase.

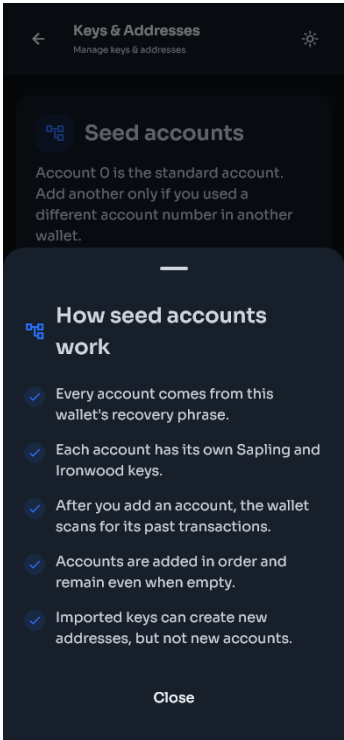
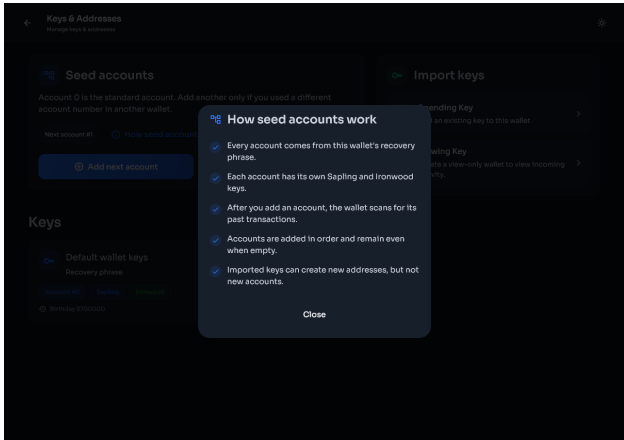
Each seed account added by Stashi Wallet includes its supported Sapling and Ironwood key material. The account number is not a diversified address number.

Use these controls only when you know or suspect that another wallet used a higher account number:

- **Add next account** adds the next consecutive seed account and starts the required scan.
- **Add 5 accounts** adds the next five consecutive seed accounts and starts the required scan.

The controls do not skip account numbers. Wait for the current account scan to finish before adding another group.

Select **How seed accounts work** to read the same explanation in Stashi Wallet.

Mobile	Desktop
	

When to add seed accounts

Add seed accounts in the following circumstances:

- You imported a seed phrase from another wallet and some transaction history is missing.
- The previous wallet allowed you to create more than one account from the same seed phrase.
- You know that a payment was sent to a higher-numbered account.

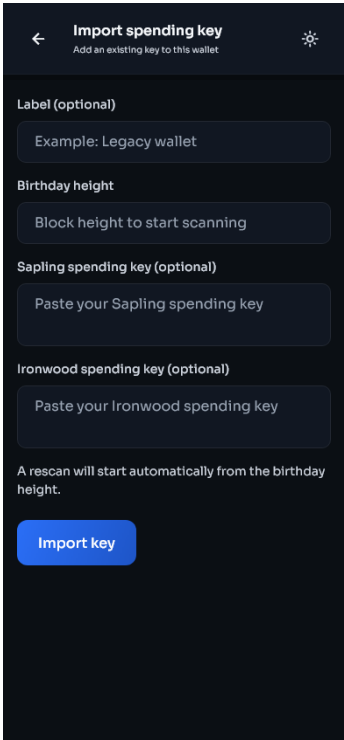
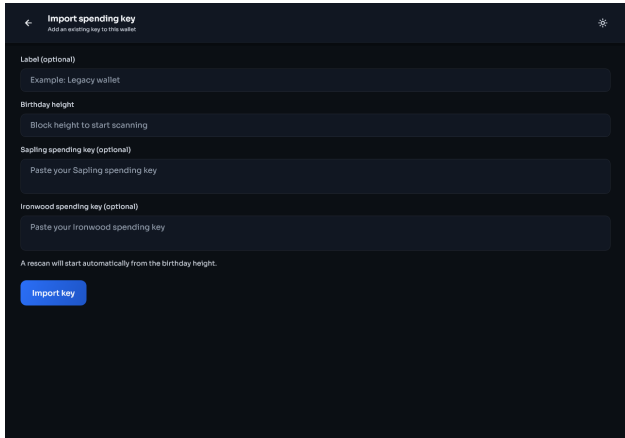
Do not add large numbers of accounts without a reason. Each added key group gives the scanner more keys to test and can increase scanning work.

Imported spending keys

An imported spending key controls a single key scope. It can spend the notes that it owns and can generate supported diversified addresses for that key. It cannot derive sibling seed accounts because it does not contain the parent seed phrase.

To import a spending key:

- 1 Open **Settings > Keys & addresses**.
- 2 Select **Spending Key** under Import keys.
- 3 Enter the spending key.
- 4 Enter a birthday height from before its first transaction.
- 5 Confirm the import.
- 6 Allow the automatic rescan to finish.
- 7 Open the imported key and check its balance and addresses.

Mobile	Desktop
	

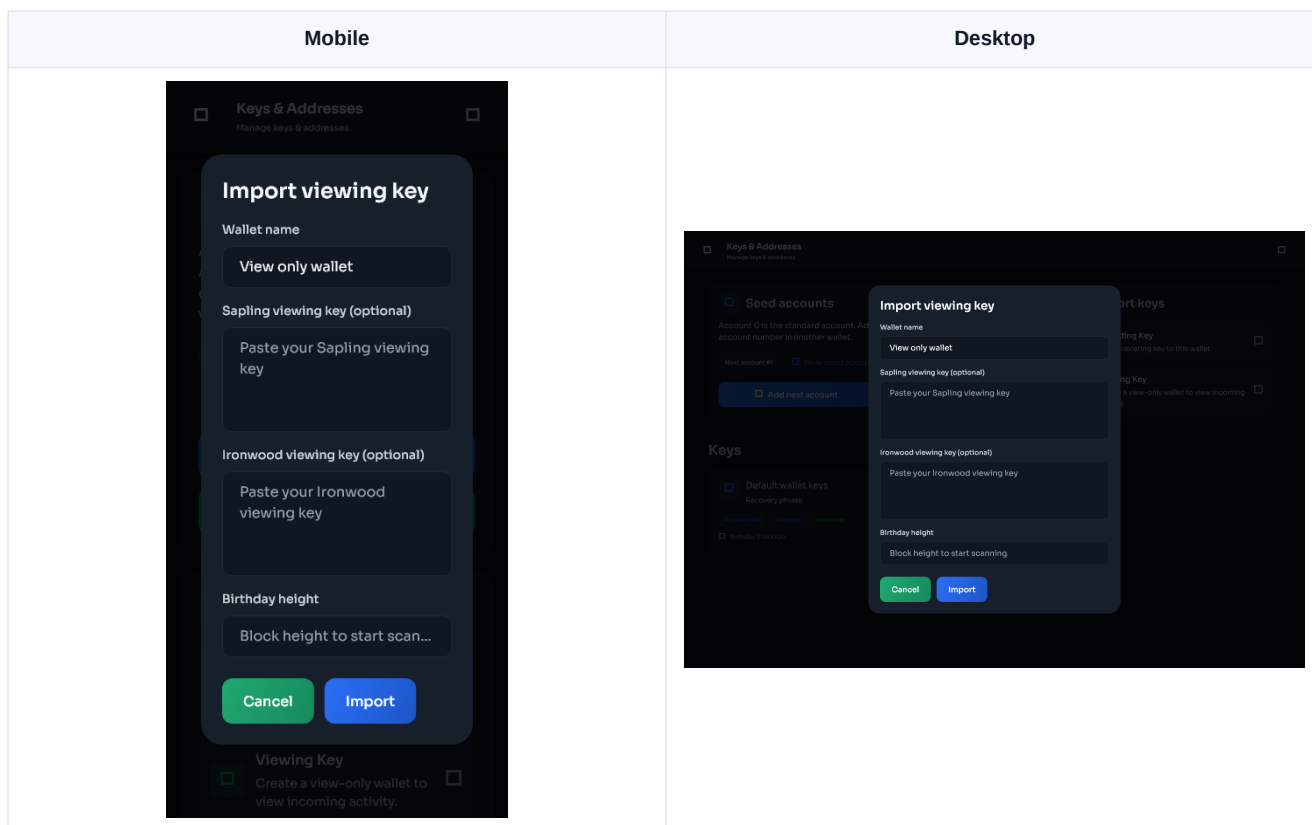
The seed account controls do not apply to imported spending keys.

Imported viewing keys

A viewing key can detect supported incoming activity and derive addresses within its key scope, but it cannot spend funds or derive sibling seed accounts.

To import a viewing key into an existing wallet:

- 1 Open **Settings > Keys & addresses**.
- 2 Select **Viewing Key**.
- 3 Enter a wallet name.
- 4 Enter the viewing key in the matching Sapling or Ironwood field.
- 5 Enter a suitable birthday height.
- 6 Confirm the import and allow the rescan to finish.



Use a separate view-only wallet when you want to monitor activity without storing spending authority on that device.

Sapling and Ironwood

Sapling and Ironwood are different Pirate Chain shielded pools. Their addresses and keys are not interchangeable.

Key type	How to recognise a viewing key	Use
Sapling	The viewing key begins with zxviews1	Monitors activity and derives addresses within a Sapling key scope
Ironwood	The viewing key begins with pirate-extended-viewing-key1	Monitors activity and derives addresses within an Ironwood key scope

The labels shown for a key indicate which shielded key types that group supports. Previous wallets and imported keys may support Sapling only. Seed accounts created by current Stashi Wallet versions can include both Sapling and Ironwood.

Funds received through one shielded pool do not make the same address valid in another pool. Use the address produced by Stashi Wallet for the selected key and payment type.

Diversified addresses

A key can produce many payment addresses. These are addresses within the same account, not new seed accounts.

- Generating a diversified address does not create a new seed phrase.
- Previous addresses remain able to receive funds.
- Address rotation reduces address reuse.
- Labels and colour tags remain local to this installation.
- A spending or viewing key can derive addresses only within the scope represented by that key.

Spending key details and export

Open a key entry to view its addresses and available actions. Exporting sensitive key material requires authentication.

Before exporting a key:

- 1 Close screen-sharing and recording software.
- 2 Confirm that no other person can see the display.
- 3 Copy the key only to the device or offline backup that requires it.
- 4 Clear the destination clipboard if the operating system does not clear it automatically.
- 5 Never send a spending key through chat or email.

Seed account controls for imported keys

Only a wallet with its seed phrase can derive the next seed account. Imported spending keys and viewing keys can create diversified addresses within their own scope, but they cannot recreate account 1, account 2, or another sibling account. This is a property of the protocol key hierarchy.

Move from Treasure Chest or Pirate Wallet Lite

[Previous: Keys and accounts](#) | [Guide contents](#) | [Next: Network and synchronisation](#)

Moving a wallet means importing its seed phrase and any separate keys into Stashi Wallet, then confirming that the expected balance and transaction history are present. Do not remove the previous wallet until you have completed these checks.

Before you begin

- 1 Open the previous wallet on a trusted device.
- 2 Confirm that you have the correct seed phrase in the correct order.
- 3 Record the approximate date or block height of the wallet's first transaction.
- 4 Record whether the previous wallet used multiple accounts from the seed phrase.
- 5 Record whether it contained separately imported Sapling spending keys or viewing keys.
- 6 Update and synchronise the previous wallet so that you have a useful comparison.

Import the seed phrase

- 1 Install Stashi Wallet from the official release.
- 2 Select **Get started > Import existing wallet**.
- 3 Select the seed phrase language if required.
- 4 Enter the 24 words of the seed phrase in order.
- 5 Set a local passphrase and optional biometrics.
- 6 Enter a birthday height from before the oldest expected transaction.
- 7 Finish the setup.
- 8 Keep the application open until the historical scan is complete.
- 9 Compare the balance and Activity page with the previous wallet.

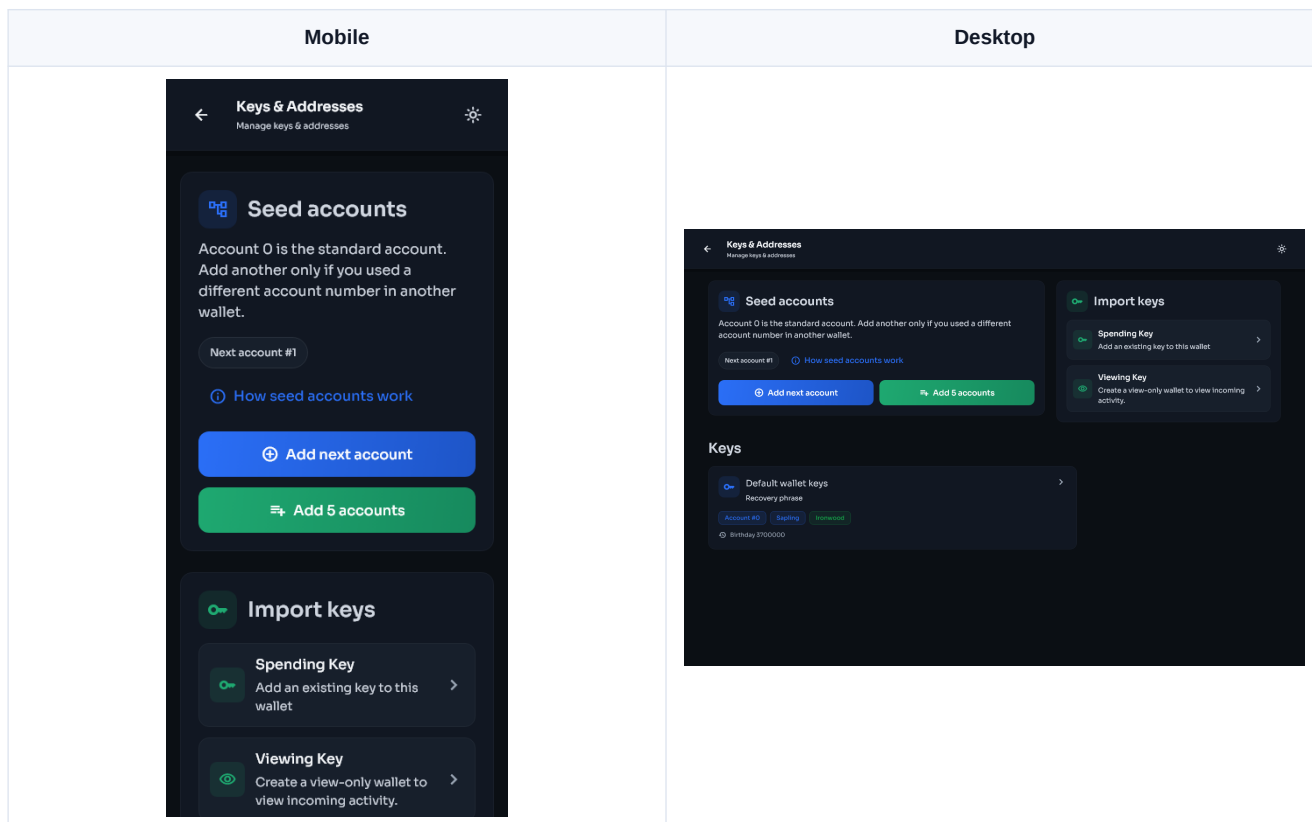
The standard seed account is account 0. During recovery, Stashi Wallet also checks the five legacy Sapling lookahead accounts, accounts 1 through 5. Unused lookahead accounts are not retained after the discovery scan. This keeps later synchronisation efficient.

Find funds in higher seed accounts

If the previous wallet used account 6 or higher, or if its account layout is uncertain:

- 1 Open **Settings > Keys & addresses**.
- 2 Find **Seed accounts**.
- 3 Read the **Next seed account** number shown by Stashi Wallet.
- 4 Select **Add 5 accounts** to extend the search in a small group, or select **Add next account** when you know the exact next index.
- 5 Confirm the account range.

- 6 Allow the scan started by Stashi Wallet to finish.
- 7 Check the balance and Activity page.
- 8 Add another group only if the expected history is still missing.



The manually added account sequence is saved. These accounts remain available even if the first scan finds no notes. Each manually added seed account includes Sapling and Ironwood support where available.

Import separate keys

A seed phrase cannot recreate a private key that was imported separately into Treasure Chest or Pirate Wallet Lite.

For each separately imported key:

- 1 Open **Settings > Keys & addresses**.
- 2 Select **Spending Key** or **Viewing Key**, as appropriate.
- 3 Enter the key and a birthday height from before its first use.
- 4 Confirm the import.
- 5 Allow the automatic rescan to finish.
- 6 Check the key entry, balance, and Activity page.

Do not use **Add next account** for an imported key. Seed accounts and imported keys use different recovery methods.

If the previous wallet shows more history

Check the following points in order:

- 1 Confirm that Stashi Wallet has reached the current block height.
- 2 Confirm that the seed phrase controls the destination address.

- 3 Confirm that the birthday height is earlier than the missing transaction.
- 4 Add any required higher seed accounts.
- 5 Import any separate spending or viewing keys again.
- 6 Confirm that Activity is not filtered to a different wallet or key.
- 7 Allow Auto node mode to select an endpoint that serves current block data.

Then run **Settings > Advanced > Rescan blockchain** from a suitable height. If the transaction is still absent, follow [Missing balance or transaction](#).

Finish moving the wallet safely

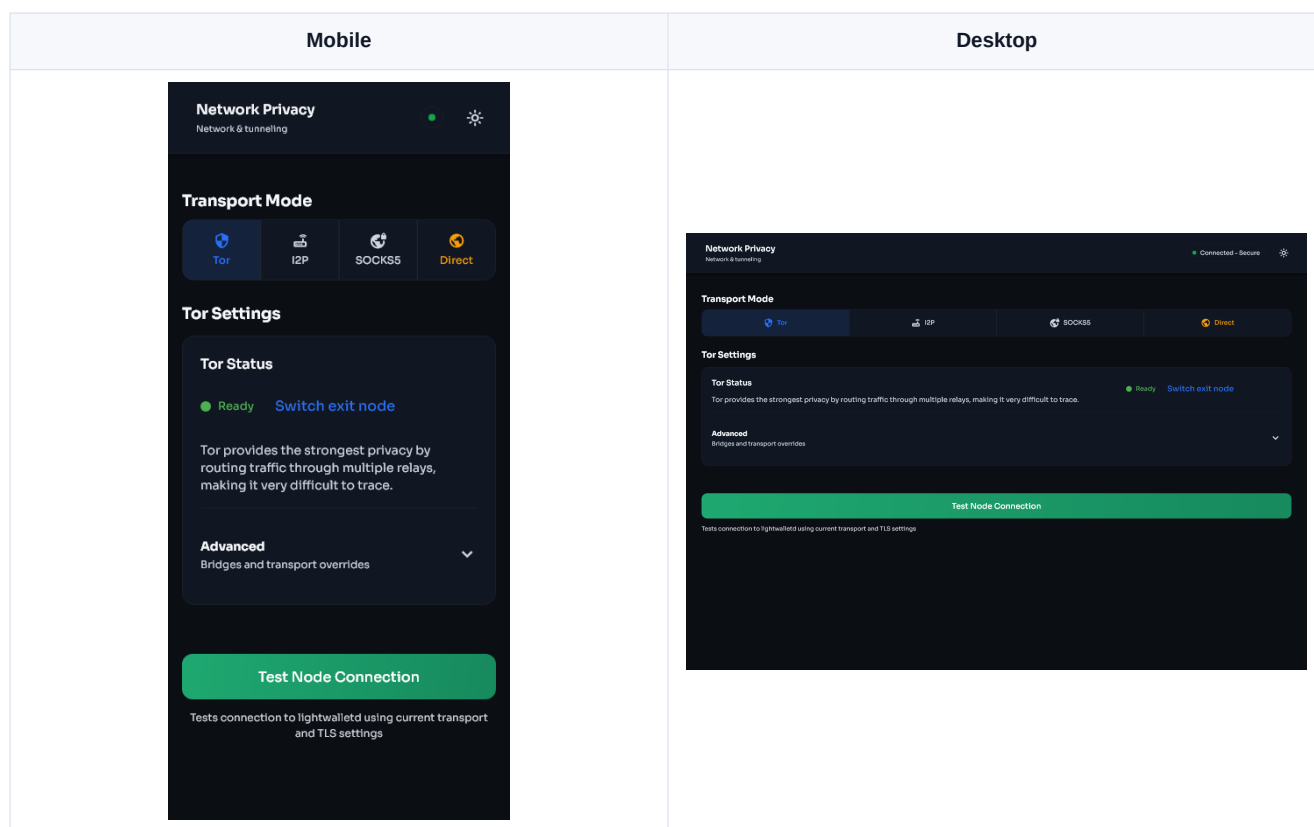
Keep the previous wallet until all of the following statements are true:

- The expected confirmed balance is present.
- Important incoming and outgoing transactions are visible.
- You have identified every imported key that still holds funds.
- You have tested a small receive and send, if practical.
- You have verified the Stashi Wallet seed phrase backup offline.

Network privacy and synchronisation

[Previous: Moving from another wallet](#) | [Guide contents](#) | [Next: Security and backups](#)

Open **Settings > Privacy and Network > Transport** to select how Stashi Wallet reaches its light server.



Transport choices

Direct

Direct mode connects without an anonymity network. It is usually the simplest and fastest option, but the network path can reveal to your internet provider that the device is connecting to wallet infrastructure. Direct mode uses the device's configured DNS resolver.

Tor

Tor routes the light-server connection through the Tor network. It improves network-level privacy but can be slower and may require time to establish a circuit. Stashi Wallet prefers the listed Tor endpoints and can also reach compatible clearnet endpoints through Tor when required.

Changing a Tor exit path does not change wallet keys or addresses.

SOCKS5

SOCKS5 sends the connection through a proxy that you provide. Enter a host and port that you control or trust. A proxy can observe connection metadata and is not automatically private because it uses SOCKS5.

I2P

I2P uses an available I2P route and a compatible endpoint. It requires working I2P connectivity on the device or through a supported configuration. An initial connection can take longer than Direct mode. I2P may not be available on every platform or release.

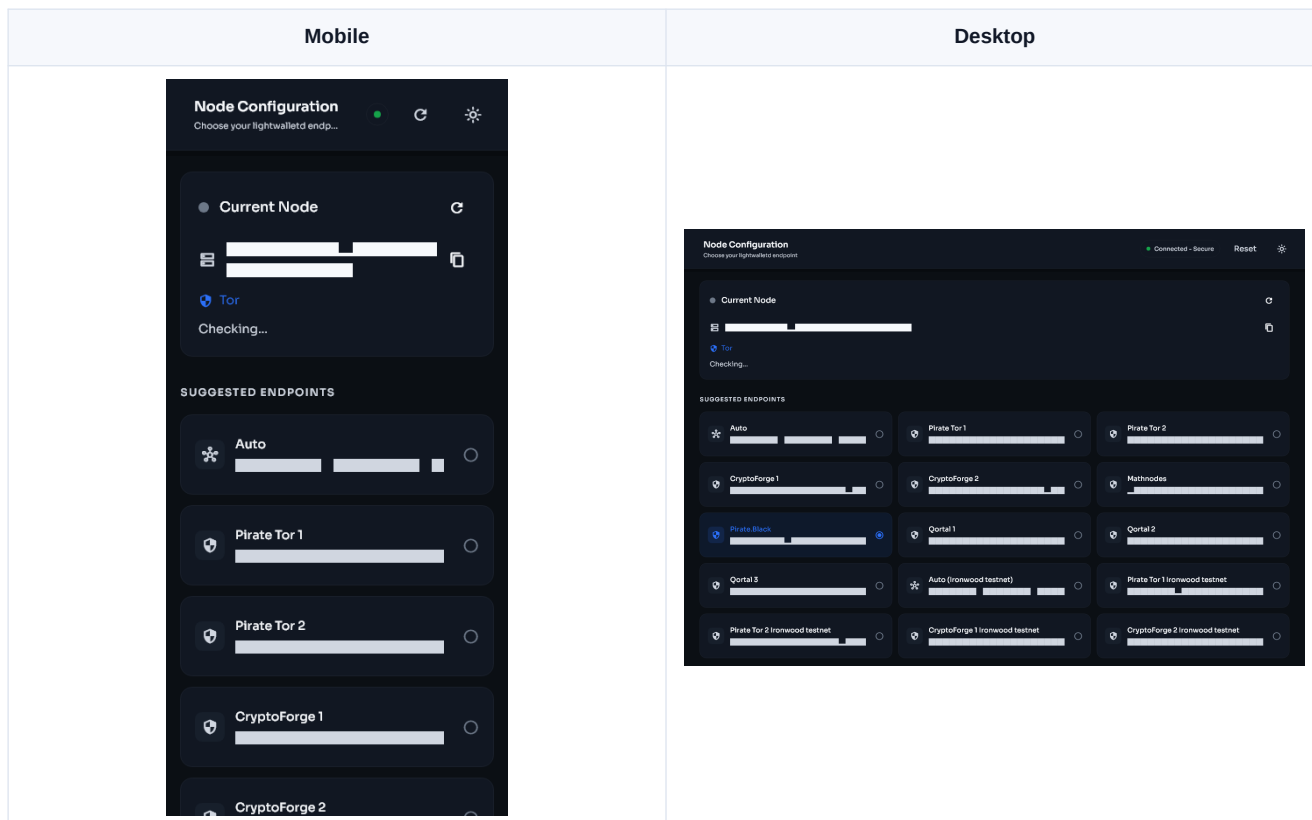
Node selection

Open **Settings > Privacy and Network > Node**.

- **Auto** uses the endpoint pool and automatic failover checks.
- **Manual** remains connected to the selected server until you change it or return to Auto.

Auto mode checks more than whether a network connection opens. A usable endpoint must also report and serve suitable blockchain data. If a server is reachable but stalled or behind, Stashi Wallet can move to another endpoint.

Use Manual mode for testing or when you operate a trusted server. Return to Auto if the selected server stops advancing.



Synchronisation stages

- **Preparing sync** means that Stashi Wallet is opening the wallet database, checking its state, selecting an endpoint, and preparing cached or remote block data.
- **Downloading** means that Stashi Wallet is obtaining compact blockchain data that is not already cached.
- **Scanning** means that Stashi Wallet is testing compact outputs against the wallet's Sapling and Ironwood keys and updating wallet information.
- **Finalising** means that Stashi Wallet is saving the latest results and refreshing balances and Activity.
- **Synced** means that Stashi Wallet has processed the chain height reported by the light server.

The blockchain height should continue to move when the chain advances. A connected status without block progress does not confirm that a server is healthy.

Cached blocks and rescans

Stashi Wallet keeps validated compact blocks locally so that a rescan does not need to download the same range again. Stashi Wallet checks cached data before reuse. Adding a seed account or imported key starts the historical replay required to test the new key against the relevant blocks.

If Preparing sync does not finish

- 1 Leave Stashi Wallet open for several minutes after an update, local data upgrade, key import, or seed-account addition.
- 2 Confirm that the device has working internet access.
- 3 In Auto node mode, allow time for endpoint health checks and failover.
- 4 Try another transport. Direct mode can help determine whether Tor, I2P, or a proxy is preventing the connection.
- 5 Select another light server manually, then return to Auto after testing.
- 6 Restart the application.
- 7 Check the available storage and system time.
- 8 Enable debug logging and reproduce the delay.

Do not start another rescan while a scan is active.

Rescan the wallet

Use a rescan when Stashi Wallet has the correct keys but its local transaction information is incomplete.

- 1 Open **Settings > Advanced > Rescan blockchain**.
- 2 Select a height before the earliest missing transaction.
- 3 Confirm the rescan.
- 4 Keep the application open and allow the rescan to finish.
- 5 Check Activity and the confirmed balance.

An earlier start height requires more time but does not exclude a later transaction. A rescan cannot find funds that belong to a different seed phrase, a missing seed account, or a private key that was not imported.

Backups and wallet security

[Previous: Network and synchronisation](#) | [Guide contents](#) | [Next: Settings and release verification](#)

What protects the funds

Cryptographic keys control ARRR. The seed phrase can recreate seed-derived keys. A spending key that was imported separately must have a separate backup.

The local passphrase protects access to the wallet database on the device. It does not replace the seed phrase and cannot recover a lost seed phrase.

Back up the seed phrase

- 1 Confirm that no other person can see or record the seed phrase.
- 2 Open **Settings > Backups > Backup seed phrase**.
- 3 Authenticate with the requested biometric method or local passphrase.
- 4 Write the words in order on an offline medium, such as paper with permanent ink or a metal seed phrase backup.
- 5 Check every word and its position.
- 6 Store the backup separately from the unlocked device.
- 7 Leave the seed phrase screen and confirm that no photograph, clipboard entry, or print job remains.

Never enter a seed phrase into a support form, website, Telegram bot, Discord bot, browser extension, or remote support session.

Back up imported keys

The seed phrase does not include keys that were imported separately.

- 1 Open **Settings > Keys & addresses**.
- 2 Open each imported spending key.
- 3 Select **Export keys** and authenticate.
- 4 Record the key offline and label the backup without exposing the key itself.
- 5 Record a birthday height or approximate first-use date.
- 6 Test the backup in a separate offline profile if your security process allows it.

A viewing key can also be backed up for monitoring. It cannot spend funds, but it reveals wallet activity within its scope.

Local passphrase

Use **Settings > Security > Change passphrase** to change the local unlock passphrase. Select a long, unique passphrase that meets the requirements shown by Stashi Wallet.

A password manager can store the local passphrase. Store the seed phrase offline unless your security plan explicitly accounts for the risks of an online vault.

Changing the local passphrase does not change blockchain keys or addresses.

Biometrics

Biometric unlock uses the device security system. Its security depends on the device, operating system, enrolled fingerprints or faces, and platform secure storage.

- Keep the local passphrase available as a fallback.
- Remove biometric access before giving the unlocked device to another person.
- If secure storage fails, use the local passphrase and review the device's Keychain, Keystore, or credential settings.

Duress passphrase

The optional duress passphrase opens a separate empty decoy wallet when it is entered during unlock. It does not erase the primary wallet or move funds.

Before enabling a duress passphrase:

- 1 Understand the difference between the real and decoy passphrases.
- 2 Test both the real and decoy passphrases while the real seed phrase is safely backed up.
- 3 Do not reuse either passphrase elsewhere.
- 4 Remember that a decoy does not guarantee protection against every physical or forensic threat.

Before deleting or resetting anything

Confirm the following points before deleting or resetting Stashi Wallet:

- You have the correct seed phrase.
- You have every separately imported spending key.
- You know the seed phrase language if it is not English.
- You have a birthday date or height early enough for recovery.
- You have a record of any higher seed account indices that were used.

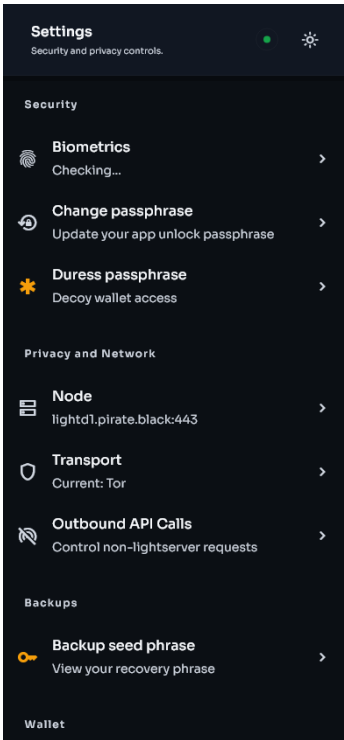
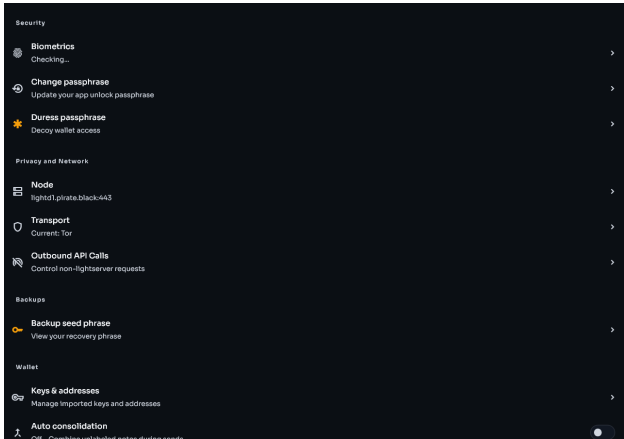
A wallet database backup can preserve labels and local history, but it must not be the only recovery method.

Settings and release verification

[Previous: Security and backups](#) | [Guide contents](#) | [Next: Troubleshooting](#)

Settings map

Section	What it controls
Security	Biometrics, local passphrase, and duress passphrase
Privacy and Network	Light-server node, Direct, Tor, SOCKS5, I2P, and non-lightserver API access
Backups	Seed phrase display and confirmation
Wallet	Keys, seed accounts, addresses, and auto consolidation
Trading	Swap interface preference when swaps are enabled
Appearance	Theme, fiat currency, application language, and seed phrase language
Advanced	Birthday height, blockchain rescan, debug logging, and diagnostics
About	Version, Verify build, terms, privacy information, and open source licences

Mobile	Desktop
 The mobile app settings screen is shown in a dark theme. At the top, it says 'Settings' with a subtitle 'Security and privacy controls.' Below this are several sections: 'Security' with options for 'Biometrics' (Checking...), 'Change passphrase' (Update your app unlock passphrase), and 'Duress passphrase' (Decoy wallet access). 'Privacy and Network' includes 'Node' (lightd1.pirate.black:443), 'Transport' (Current: Tor), and 'Outbound API Calls' (Control non-lightserver requests). 'Backups' has 'Backup seed phrase' (View your recovery phrase). 'Wallet' is partially visible at the bottom.	 The desktop app settings window is shown in a dark theme. It has a similar layout to the mobile version. The 'Security' section includes 'Biometrics' (Checking...), 'Change passphrase' (Update your app unlock passphrase), and 'Duress passphrase' (Decoy wallet access). The 'Privacy and Network' section includes 'Node' (lightd1.pirate.black:443), 'Transport' (Current: Tor), and 'Outbound API Calls' (Control non-lightserver requests). The 'Backups' section includes 'Backup seed phrase' (View your recovery phrase). The 'Wallet' section includes 'Keys & addresses' (Manage imported keys and addresses) and 'Auto consolidation' (Off - Consolidate unspent entries during sync).

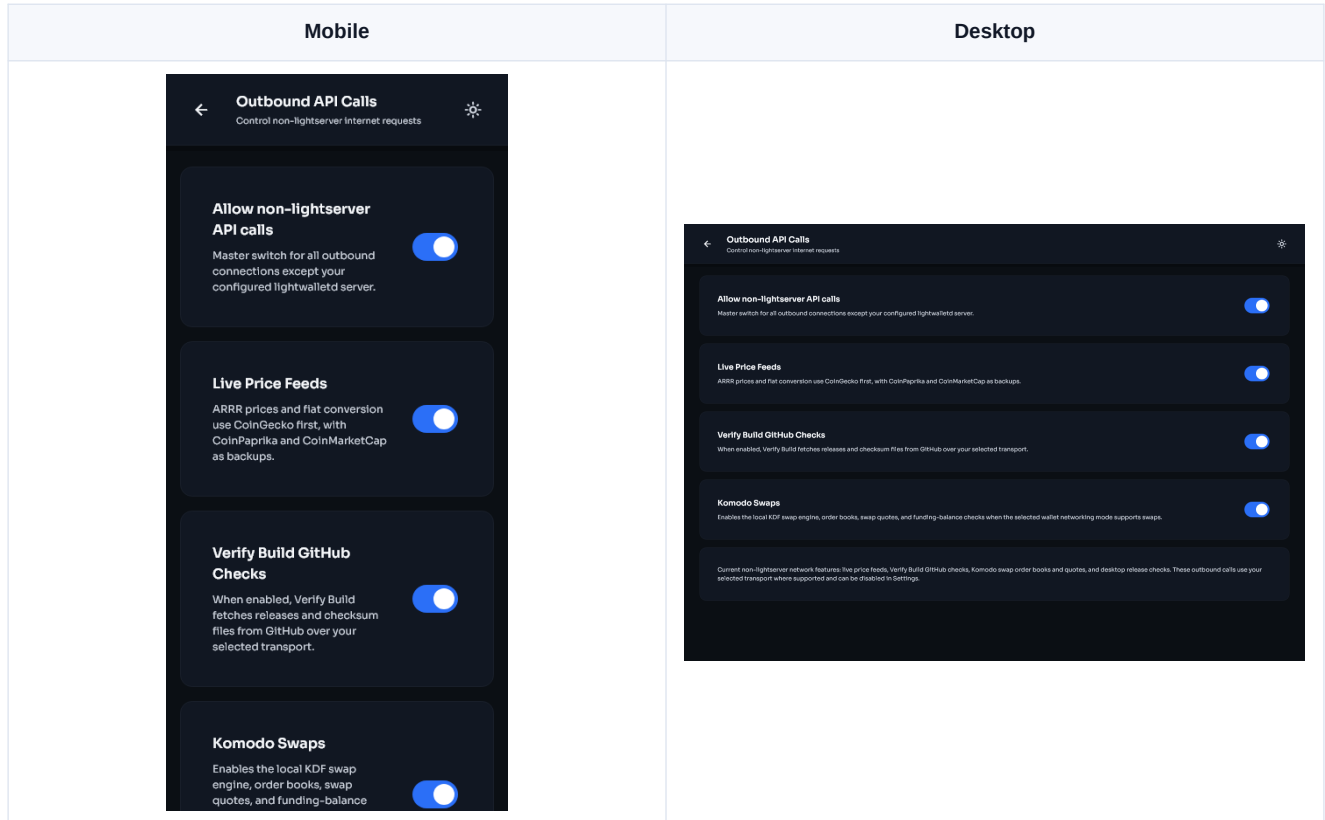
Outbound API Calls

The light-server connection is required for wallet synchronisation. Other internet features can be controlled separately under **Settings > Privacy and Network > Outbound API Calls**.

- **Live Price Feeds** controls ARRR price and fiat conversion requests. Stashi Wallet uses CoinGecko first, with CoinPaprika and CoinMarketCap as alternatives.

- **Verify Build GitHub Checks** allows Stashi Wallet to download signed release metadata from GitHub.
- **Komodo Swaps** allows order book, quote, and funding balance requests when swaps are supported.
- **Desktop Update Checks** allows desktop versions to check GitHub for new releases.

Turning off **Allow non-lightserver API calls** disables all of these non-lightserver requests. Turning off **Live Price Feeds** can leave the fiat estimate blank without affecting ARRR funds.



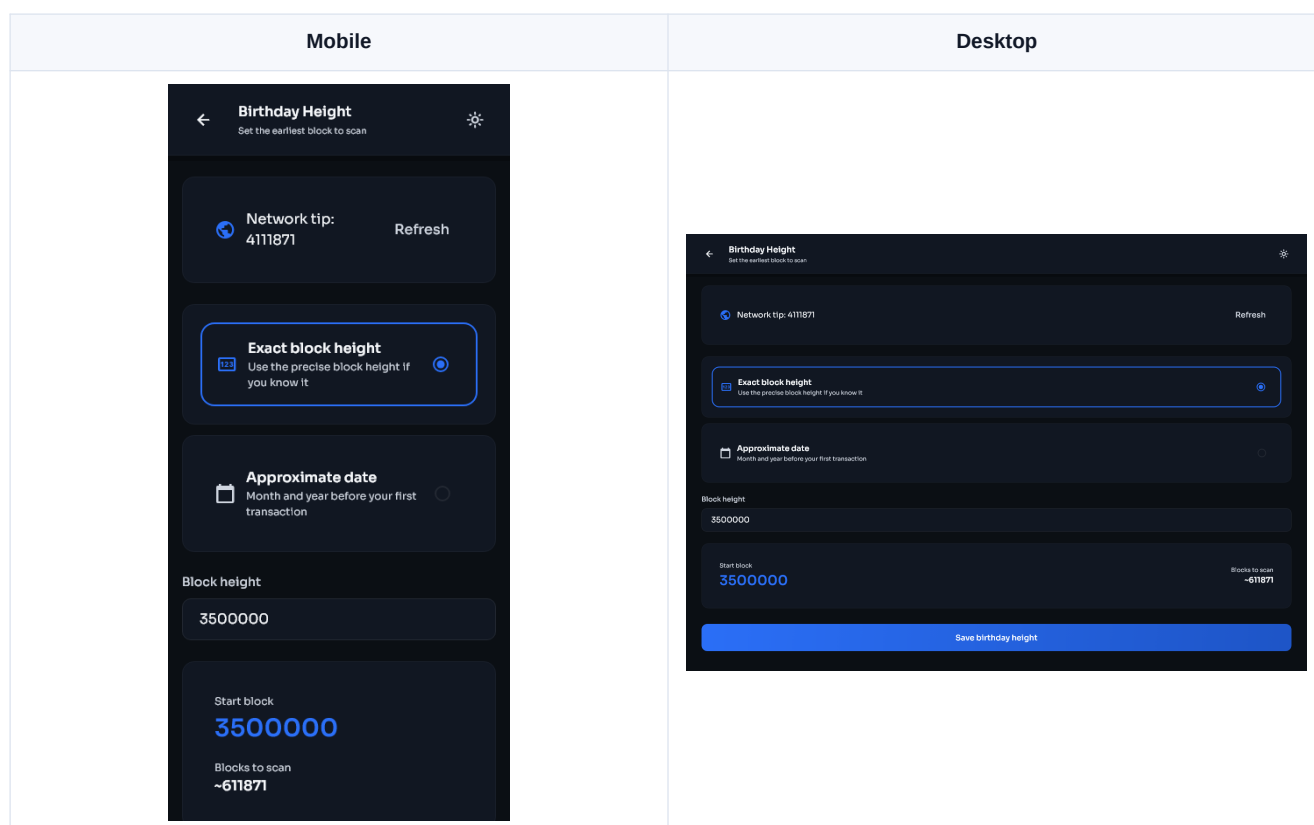
Currency, language, and theme

- The currency setting changes only the estimated fiat display. It does not convert or move ARRR.
- The application language setting changes menus and messages.
- The seed phrase language setting tells Stashi Wallet how to interpret seed words. Do not change it casually for an existing backup.
- The theme setting changes only the appearance.

Birthday height

The birthday height is the earliest block that Stashi Wallet needs to inspect. Set it before the first expected transaction.

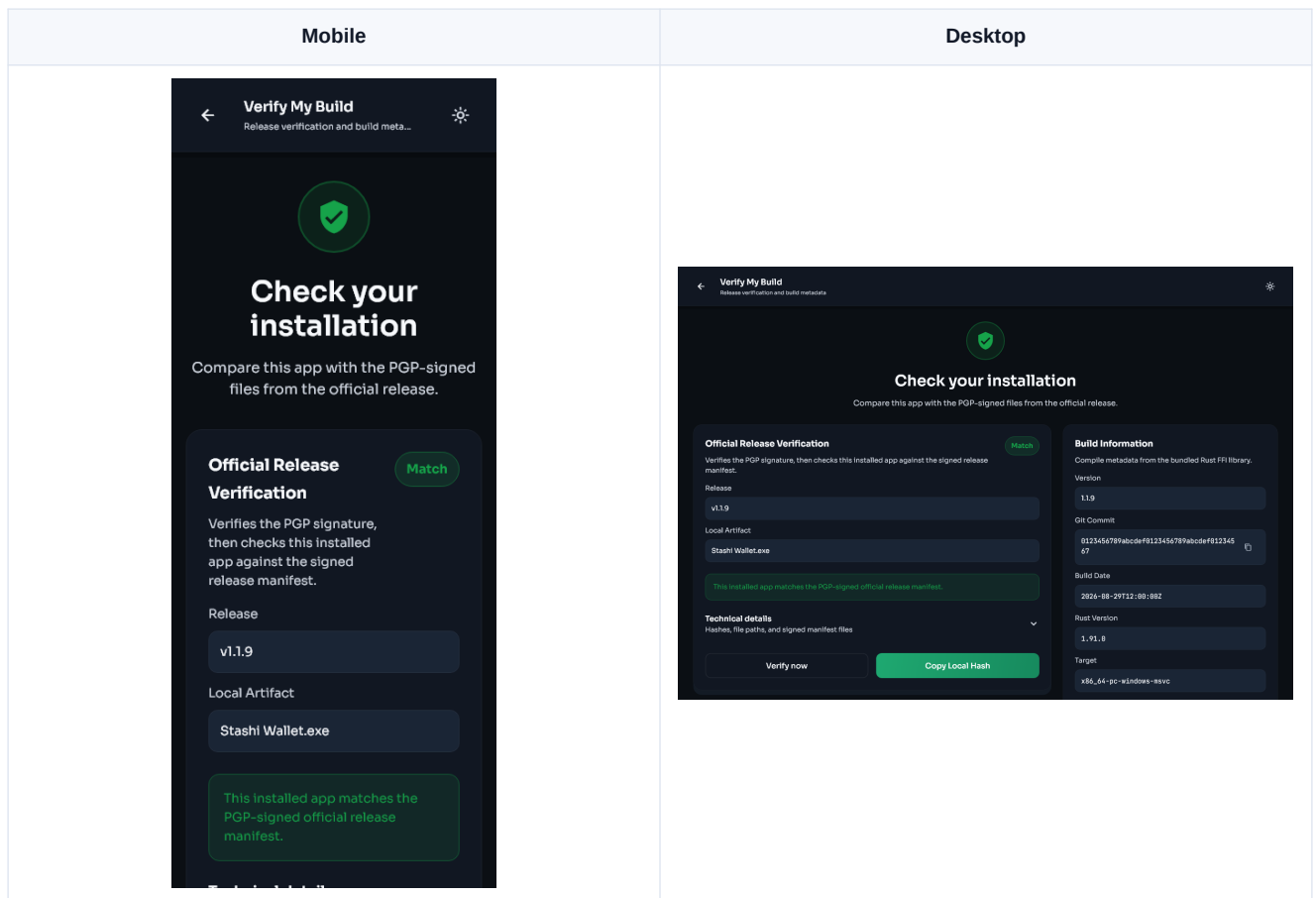
- 1 Open **Settings > Advanced > Birthday height**.
- 2 Select an approximate date or enter an exact height.
- 3 Save the value.
- 4 Start the offered rescan if you are trying to recover earlier history.



Moving the birthday height earlier increases scanning work. Moving it later can exclude previous transactions from a future rescan.

Verify the Stashi Wallet installation

Open **Settings > About > Verify build**, then select **Verify now**. Stashi Wallet downloads the signed release manifest for its exact version, verifies the PGP signature against the pinned Stashi Wallet release key, hashes the installed application file, and compares the result with the signed checksum.



Result meanings

- **Match** means that the PGP-signed official manifest was valid and the local file hash matched its entry.
- **Check unavailable** means that Stashi Wallet could not complete the online check. This is not a failed integrity result. Check the selected transport and outbound GitHub permission, then try again.
- **Mismatch** means that the local file did not match the signed manifest. Stop using that installation for sensitive work and download a fresh copy from the official release page.
- **Unsupported package** means that the current platform or package format does not expose a local file that the verifier can hash. Use manual release verification.

An unavailable network check is shown differently from a cryptographic mismatch.

Release verification is unavailable because the signed files cannot be reached

The screenshots use sample release data to show the possible states. The version, filename, hash, target, and release date will differ on your device.

Verify the downloaded release files

Each official release provides a signature bundle for its tag. The bundle contains the Stashi Wallet public key, a checksum manifest, a signature for that manifest, and detached signatures for release files.

The authoritative primary key fingerprint is:

```
E4FB 2399 AECC F9B9 447D ED47 2CE6 5343 4015 53A6
```

The existing user ID on that key is:

```
Pirate Unified Wallet <dev@piratechainfoundation.com>
```

The previous user ID text remains attached to the same established Stashi Wallet release key. Confirm the complete fingerprint through an independent official Pirate Network channel. Do not trust a key only because it was downloaded beside the file that it signs.

Typical GnuPG steps are:

```
gpg --import public_key.asc
gpg --fingerprint E4FB2399AECCF9B9447DED472CE65343401553A6
gpg --verify sha256sum-vX.Y.Z.txt.sig sha256sum-vX.Y.Z.txt
gpg --verify Stashi-Wallet-linux-x86_64.AppImage.sig Stashi-Wallet-linux-x86_64.AppImage
```

Use the filenames from the release that you downloaded. PGP verification does not decrypt the application. It proves that the matching private key signed those exact files.

For the full command reference, see [Verify Builds](#).

Debug logging

Debug logging is off by default.

- 1 Open **Settings > Advanced > Debug logging**.
- 2 Read the warning and enable debug logging.
- 3 Reproduce the problem.
- 4 Return to Debug logging and use the share or save action.
- 5 Turn off debug logging when you have finished. Disabling it clears the active debug log when the screen states that it will do so.

The active debug .log file is stored at the following location:

- Windows: %LOCALAPPDATA%\Pirate\PirateWallet\data\logs\debug.log
- macOS: ~/Library/Application Support/com.Pirate.PirateWallet/logs/debug.log
- Linux: \${XDG_DATA_HOME:-~/.local/share}/piratewallet/logs/debug.log

Troubleshooting

[Previous: Settings and release verification](#) | [Guide contents](#) | [Next: Advanced use](#)

Start with these three checks:

- 1 Confirm the selected wallet at the top of Home.
- 2 Confirm that synchronisation has reached the current chain height.
- 3 Confirm that the receiving address belongs to a key loaded by the selected wallet.

Missing balance or transaction

Complete the following checks in order:

- 1 Open Activity and remove any filters.
- 2 Wait for Stashi Wallet to show **Synced**.
- 3 Compare the destination address and transaction ID with the sending wallet or a block explorer.
- 4 Confirm that the transaction is confirmed and was not sent to a change address controlled only by the sender.
- 5 Confirm that the imported seed phrase is correct.
- 6 If you are moving from another wallet, add higher seed accounts under **Settings > Keys & addresses**.
- 7 Import any separate spending or viewing key again.
- 8 Confirm that the wallet birthday height is before the transaction block.
- 9 In Auto node mode, allow Stashi Wallet to replace an endpoint that is connected but not serving current blocks.
- 10 Rescan from a height before the missing transaction.

Stuck on Preparing sync

- 1 Wait several minutes after an update, local data upgrade, key import, or seed-account addition.
- 2 Confirm that the device clock is correct and that storage is available.
- 3 Try another transport.
- 4 Try another light server manually.
- 5 Return to Auto and allow failover.
- 6 Restart the application.
- 7 Enable debug logging and reproduce the delay.

If a server is reachable but its block height is stale, Auto endpoint selection should treat it as degraded and move to another endpoint.

Fiat value is blank

The fiat value is for information only. ARRR funds and transaction construction do not depend on it.

- 1 Confirm that **Allow non-lightserver API calls** is enabled under **Settings > Privacy and Network > Outbound API Calls**.
- 2 Confirm that **Live Price Feeds** is enabled.
- 3 Check the internet connection and selected transport.

- 4 Leave the Home screen open while the price refreshes.
- 5 Change the selected fiat currency and change it back if the preference appears out of date.

Stashi Wallet tries CoinGecko first and uses CoinPaprika and CoinMarketCap as alternatives. All providers can be temporarily unavailable or rate-limited.

Insufficient funds when the total balance is larger

- 1 Include the network fee in the required total.
- 2 Wait for incoming funds to confirm.
- 3 Select **Auto (all keys)** in the source selector.
- 4 If you select a specific key, compare its spendable balance with the amount.
- 5 Wait for any transaction using the same notes to finish or fail.
- 6 If the wallet has many small notes, enable auto consolidation or send a smaller amount first.

The wallet-wide balance can include notes from several keys. A selected key cannot spend notes owned by another key.

Verify build cannot download files

- 1 Open **Settings > Privacy and Network > Outbound API Calls**.
- 2 Enable **Allow non-lightserver API calls** and **Verify Build GitHub Checks**.
- 3 Check the selected transport. GitHub must be reachable through it.
- 4 Try Tor, SOCKS5, or Direct if I2P or the selected transport cannot reach GitHub.
- 5 Select **Verify now** again.

A download error is not a mismatch. If online verification remains unavailable, use the signed files from the release page and follow [Verify the downloaded release files](#).

AppImage does not open

- 1 Confirm that you downloaded the AppImage for x86_64 Linux.
- 2 Make it executable in the file manager, or run the following command:

```
chmod +x Stashi-Wallet-linux-x86_64.AppImage
```

- 1 Start it from a terminal to view any error:

```
./Stashi-Wallet-linux-x86_64.AppImage
```

- 1 If the distribution blocks FUSE, use the AppImage extract-and-run support:

```
./Stashi-Wallet-linux-x86_64.AppImage --appimage-extract-and-run
```

- 1 Use the DEB or Flatpak package if either format is more suitable for the distribution.

Verify the checksum and signature before changing permissions or running the file.

Interface looks too large on a laptop

Stashi Wallet follows the operating system display and text scaling. It also changes to a more compact desktop layout when the available window height is limited.

- 1 Install the latest Stashi Wallet version.

- 2 Maximise the window or make it taller if the desktop allows it.
- 3 Check the operating system display scale and accessibility text size. Retain a larger setting if you need it for readability.
- 4 Scroll the page if controls do not fit vertically. The compact layout does not remove wallet functions.

Do not reduce an accessibility text setting only to make Stashi Wallet match a screenshot. The layout is designed to keep scaled text readable.

Send failed

- 1 Check the recipient address and amount.
- 2 Check the confirmed spendable funds and fee.
- 3 Confirm that Stashi Wallet shows **Synced**.
- 4 Confirm that the light server is healthy.
- 5 If the error occurred before broadcast, correct the problem and try again.
- 6 If the broadcast status is uncertain, check Activity and the transaction ID before sending again.

Do not create a duplicate payment until you know whether the first transaction was broadcast.

Information for a support report

Include the following information:

- Stashi Wallet version
- Operating system and version
- Package type, such as DMG, AppImage, DEB, Flatpak, installer, or APK
- Selected network transport and whether node selection is Auto or Manual
- Current wallet height and target height
- Exact error text
- Time of the problem, including the time zone
- Transaction ID, when relevant
- Debug log captured immediately after reproducing the problem

Do not include seed words, spending keys, local passphrases, or unredacted personal information.

Advanced use

[Previous: Troubleshooting](#) | [Guide contents](#)

Manage several wallets

Use the wallet selector at the top of Home to change the active wallet. The active selection controls balances, receiving addresses, key imports, rescans, and sends.

Double-check the wallet name before a sensitive action. A key imported into a wallet is not automatically added to another wallet.

Exact birthdays and controlled rescans

An expert recovery normally uses a known block height before the first relevant transaction. This minimises scanning work without excluding transaction history.

- Use an exact height when a transaction record or previous wallet provides it.
- Use an earlier estimate when the first-use height is uncertain.
- Treat a birthday update and a rescan as separate decisions. Save the value, then accept the rescan prompt when the wallet information must be rebuilt immediately.
- Use the birthday stored with an imported key for its historical scan.

Manual light-server configuration

Manual node settings are intended for users who operate or explicitly trust a `lightwalletd` endpoint.

- 1 Open **Settings > Privacy and Network > Node**.
- 2 Turn off automatic endpoint selection.
- 3 Enter the endpoint as a host and port.
- 4 Select TLS when the endpoint supports it.
- 5 If you use an SPKI pin, obtain and independently confirm the expected pin.
- 6 Save the endpoint and monitor its health and blockchain height.

Return to Auto if the endpoint stops advancing. A valid TLS connection does not confirm that a server is current or complete.

SOCKS5 and I2P details

For SOCKS5, the proxy must be reachable from the Stashi Wallet process. Localhost means the same device, not another computer on the network.

For I2P, use an endpoint and route that are compatible with the current I2P configuration. I2P destinations cannot be reached through ordinary Direct networking.

Address management

Open a key under **Keys & addresses** to complete the following tasks:

- Generate a new address for a supported shielded pool.
- Copy an existing address.

- Label addresses and apply colour tags.
- Archive addresses that you no longer want in the main list.
- Consolidate or sweep spendable balances.
- Export key material after authentication.

Archiving an address does not invalidate it. A payment sent to an archived address can still belong to the wallet.

Seed accounts and sparse account layouts

Stashi Wallet adds seed accounts consecutively. This avoids a manual field in which a mistyped number could create a confusing sparse account layout.

If another wallet used a distant account index, add five accounts at a time and allow each scan to finish until you reach the expected account. Account additions are saved and derive both supported shielded key types from the parent seed phrase.

Automatic recovery checks the standard account and the bounded Sapling lookahead used by previous wallets. It does not scan every possible ZIP-32 account because the account space is large and shielded ownership requires each key to test the relevant outputs.

Payment disclosure

Payment disclosure tools can prove selected facts about a transaction to a person that you choose. Disclosure data can reveal information that is otherwise shielded.

- 1 Open the payment disclosure tool from Wallets.
- 2 Read the information that the proof or disclosure will reveal.
- 3 Verify the transaction and recipient.
- 4 Share the disclosure only with the intended recipient.

Do not confuse a payment disclosure with a seed phrase or viewing key. Do not provide broader authority when a transaction proof is sufficient.

Swaps

When swaps are available in your Stashi Wallet version, the swap interface uses the local KDF engine and external order book and quote services.

- Enable the **Komodo Swaps** outbound permission.
- Check the selected wallet and funding balance.
- Review both assets, the rate, minimums, fees, and timeout conditions.
- Keep the application running while an active swap requires it.
- Do not assume that a displayed quote is guaranteed until the order is accepted.

Swaps have risks beyond a normal ARRR transfer.

Local privacy data

Wallet labels, colour tags, address book notes, preferences, cached blocks, and debug logs can contain sensitive information even when they cannot spend funds.

- Encrypt device backups.

- Remove debug logs after support work.
- Treat viewing keys as private financial information.
- Review application data before transferring a computer to another person.

Independent release verification

Use unsigned release files for close byte comparison because platform signing, notarisation, and store packaging can change the final package bytes. Check the signed checksum manifest first, then compare a locally reproduced unsigned file with the matching published unsigned file.

See [Verify Builds](#) for package names, compilation scripts, checksum commands, provenance information, and Software Bill of Materials (SBOM) details.