

ENGAGE Mobile App User Manual

Applicable version: ENGAGE Mobile Wallet (Flutter / Android, HarmonyOS-compatible; includes PoE mobile mining and off-chain encrypted chat)

Last updated: 2026-09

This document is intended for end users. It explains how to use the ENGAGE mobile wallet for daily operations: asset management, mobile mining, block explorer, DApp & On-chain Youth, staking, governance, and off-chain encrypted chat.

Highlights of this update: ① The default node pool now keeps only the official node; ② The burn amount for submitting a proposal is **1000 ENGA** (voting is still 1 ENGA); ③ On-chain Youth message / nickname / confession fees are **paid to the contract party**, not burned, and messages are not paid to the author; ④ Posting is now **enforced to a minimum of 1 ENGA** by the contract; ⑤ Added a "Transaction Signature Confirmation (anti-blind-signing)" section; ⑥ The settings page adds **chat image cache** management.

1. Main Interface and the Five Tabs

The bottom of the App has **5 tabs**; there is no "Settings" tab (Settings is a separate page reached via the gear icon at the top-right of the Wallet page):

Icon	Tab	Content
Wallet	Wallet	Balance, receive, transfer, transaction history, account switching, security/settings entry (top-right icon)
Mining	Mining	PoE mobile mining switch, mining statistics, and integrated entries for Staking / On-chain Governance / Task Unlock
Explorer	Explorer	Network status (height / holder count / sync / supply), latest blocks, balance ranking, latest transactions, search
DApp	DApp	Integrates "On-chain Youth" by default (Youth Profile / Youth Ranking / Confession Wall)
Chat	Chat	Off-chain end-to-end encrypted chat (conversations, contacts, groups, backup)

Switching to the background does not lock the App immediately; the App auto-locks based on "idle duration" (see 4.3).

All on-chain operations (transfer, voting, contract calls, starting mining, etc.) pop up a confirmation dialog before signing — the App decodes the transaction content locally and shows it for your verification, then requires identity re-verification (see 4.4).

2. First Use (Create / Import Wallet)

2.1 Create Wallet

- 1 Go to "Create Wallet" and enter a **wallet name** (a local label only; default **My Wallet**; fill freely, unrelated to the chat nickname).

- 2 Choose the **mnemonic length**: 12 words or 24 words (different checksum; must match when recovering).
- 3 After clicking "Generate", **write down the mnemonic offline** (wrong order or missing words will make recovery impossible; keep it safe, do not screenshot or save it online).
- 4 Go to the **backup confirmation page**: tap the mnemonic words in order to complete verification before continuing.
- 5 If the app lock is not yet set, you will be **forced into the password setup page** (see 4.1); after setting it, wallet creation is complete.
- 6 (Optional) Fill in an **invite code**: deterministically derived from the device ID (`sha256(deviceId)` first 12 chars), **one code per device** — all wallets created on the same phone share the same invite code, which stays unchanged after reinstalling. Used later to exchange task unlocks for points (see 5.2).

Note: The creation flow **has no "agree to terms" checkbox**; generation is allowed without checking anything.

2.2 Import Wallet

- Two methods are supported: **mnemonic** or **private key**.
- A wallet imported via private key **does not show the mnemonic** (only the private key can be exported).
- You may fill in a wallet name when importing (default **Imported Wallet**).

3. Wallet Home Page

The top of the Wallet page contains: account switching (avatar), balance & address, a **security shield icon** (opens the Security page), and a **settings gear icon** (opens the Settings page). Below are quick entries for Receive / Transfer and the activity log (block rewards / incoming / outgoing).

3.1 Balance and Address

- Shows the **available balance** and the **locked balance** (mining-locked rewards, staking locks, etc.).
- The address is in **eg1...** format (mainnet). The Receive page can toggle between the **mainnet transparent address** and the **shielded address** (privacy address).

3.2 Receive

On the Receive page: shows the **QR code** and the **address**, with one-tap copy; supports toggling between transparent and shielded addresses. Send the address or QR code to the other party to receive funds.

3.3 Transfer

- 1 Fill in the **recipient address** (**eg1...**), **amount**, and **memo** (optional).
- 2 The page shows the **estimated network fee**: the PoE chain has no traditional Gas; a normal transfer costs about 0 (subject to the page display).

- 3 Click "Review & Send" → a **signature confirmation dialog** pops up: it lists the transaction type, payer, payee, and amount (content is **decoded locally** by the App, not taken from the node's returned description) → **identity verification** (biometrics or app-lock password) → after confirmation it signs and broadcasts (see 4.4).

3.4 Transaction History

- The Wallet page "Recent Activity" has four filter tabs: **All / Block Rewards / Incoming / Outgoing**, showing the latest 5 by default.
- **The time window changes with the filter** (easy to misunderstand):
 - "All" and "Block Rewards" → only the **last 3 days** (blocks are frequent, to avoid the list being flooded by rewards);
 - "Incoming" / "Outgoing" → **last 180 days**.
 - So if you switch to "Incoming" and cannot see a transaction from a few days ago, it is most likely because you were still under the 3-day window of "All".
- Recorded types are more than just transfers: registering a validator, slashing, active submission, contract deployment / call, Gas burn, dividend, unlock, etc. — **any action that changes the available balance** is grouped into "Incoming" or "Outgoing" (block rewards are a separate column).
- Click "View All" to enter the **transaction history page**; click a single entry to see **transaction details** (amount, counterparty address, block height, type, memo).

3.5 Multi-Account

Through the account-switching entry, open the **account list** (a separate page with bottom navigation):

- Create a new account (generate/import), switch the current account, rename, delete (deletion requires a second confirmation).
- Deleting an account removes the local key and cache; **make sure the mnemonic/private key is backed up first**.

3.6 Security Entry

The **shield icon** at the top-right of the Wallet page opens the Security page (see Section 4).

4. Security: App-Lock Password and Biometrics

The Security page is reached via the Wallet page shield icon and contains: app-lock password, biometrics toggle, auto-lock explanation, view mnemonic / export private key.

4.1 Set / Change Password

- Go to Security page "App-Lock Password" → enter the password settings page, where you can **create or change** the app lock (6 or more digits, numeric only or alphanumeric).
- Changing the password requires passing the existing biometric/password verification first.
- The same password page is used for first setup and later changes (create when none is set, change when one exists).

4.2 Biometrics

- Once enabled, system fingerprint/face (including HarmonyOS device capability) can replace the password for unlocking and authorizing transfers.
- Biometrics are only for unlocking convenience; **the password remains the ultimate recovery method**; disabling biometrics does not affect the password.

4.3 Auto-Lock

- Uses **LockManager**: **auto-locks after 10 minutes of no operation** (any click/swipe refreshes the timer).
- Switching to the background does **not** lock immediately; it only locks after cumulative idle time is reached.
- After locking, biometrics or password are required to unlock; asset operation capability is not exposed during this period.

4.4 Transaction Signature Confirmation (Anti-Blind-Signing)

For any on-chain operation that needs your signature (transfer, voting, submitting a proposal, staking / unstaking, On-chain Youth posting / liking / commenting / nickname, starting mining, etc.), the App does two things first:

- 1 **Local decoding**: The App parses the transaction bytes to be signed by itself and displays the "**transaction type, payer, payee, and amount**" for your verification. This content is **not taken from the node's returned summary** — any description given by the node is not trusted, to prevent a hijacked node from tricking you into signing with "A shown, B content".
- 2 **Identity verification**: Before the confirmation dialog pops up, you must again pass biometrics or the app-lock password (a second verification at the same level as exporting the mnemonic).

Therefore:

- If the App **cannot parse** the transaction content (illegal or truncated byte stream), or if the type is a **system transaction** (block rewards, dividend distribution, activity reporting, etc., which should not be signed by the wallet), it will **directly refuse to sign** and explain the reason — it will never let you sign something you cannot understand.
- If the content shown in the confirmation dialog does not match the operation you actually intend to do, **cancel immediately** and check whether you are connected to an untrusted node (see 11.2).

5. Mining (PoE Mobile Mining)

Mining is an **optional switch**, part of the PoE mainnet consensus.

5.1 Start Mining

- On the "Mining" tab, toggle "Start Mining": requires being connected to a mainnet node.
- **Starting mining requires signing a challenge once with the wallet's private key**: the App sends the signature along with the request to the node, which verifies that the signature is indeed derived from that address. This way, even if someone can access the public RPC, they cannot register your address as a miner or divert your mining share.

- Mechanism: all mobile miners connected to **any mainnet node evenly split each block's App mining share** (split by address, not by device).
- One phone usually corresponds to one mining wallet (controlled by the build-time flag `ENFORCE_ONE_WALLET_PER_DEVICE`; the release build defaults it off for testing; when on, only one wallet per phone may mine at a time).

5.2 Locked Rewards and Task Unlock (AP)

- Mining income is recorded to the address as **LOCK_MARKER (locked reward)** and must be unlocked before it can circulate.
- The "Task Unlock" entry (see 5.4) opens the **AP Active Points** page:
 - **Step task**: steps **can only come from the device motion sensor, manual entry is not supported** (the node side also rejects hand-filled data). You must first grant health / motion permission and click "Refresh to get steps". **Once per device per day**, and only the first address reported by this device; the node also **directly unlocks locked coins by steps** (≈ 1 ENGA per step, subject to locked balance and credential cap).
 - **AP exchange**: use AP to release locked rewards into liquid ENGA at the real-time rate.
 - **Invite**: the invite code is **device-level** (one code per device, shared by all wallets on this device). After others use your invite code, click "Report" to exchange for AP — **reporting itself requires no signature and sends no on-chain transaction**; it can be reported multiple times a day (each time a new person is invited). When reporting, the App also clears the on-chain cumulative counter (this step requires the invite-code registrant's signature).
 - **Daily cap**: all behaviors (steps, check-in, invite, posting, like, comment, etc.) **share the same daily quota, 50,000 AP per address per day**.

Note: it is **not** "keep the App active and locked rewards keep accumulating" — locked rewards come from mining block income and are unlocked via step tasks / AP exchange.

5.3 Background and Recovery

- After about **6 hours** with no heartbeat in the background, mining pauses and requires **manual recovery** (toggle to restart).
- Mining statistics show: balance, chain height, locked rewards, and other on-chain data.

5.4 Mining Page Quick Entries

The "Mining" page integrates three entries for direct access to deep functions:

- **Staking** (see Section 9)
- **On-chain Governance** (see Section 10)
- **Task Unlock / AP** (see 5.2)

6. Block Explorer

The "Block Explorer" tab shows network status and search:

- **Network card**: current height, holder count, sync progress, total supply (max / minted / burned), and the **currently active node and peer count**.

- **Three sub-pages:**
 - Latest blocks (height, time, block producer address, transaction count)
 - Balance ranking (address leaderboard sorted by balance)
 - Latest transactions (type, amount, address, time)
- **Search:** supports block height (number), address (eg1...), transaction hash (0x... or 64-hex) / block hash.
- Special addresses carry badges: treasury, team, burn, Gas burn, dividend, etc.

Note: the block explorer **has no "validator list"**; it only shows coin-holding addresses and node peer info.

7. DApp and On-chain Youth

The "DApp" tab integrates **On-chain Youth** by default, with three sub-pages: **Youth Profile / Youth Ranking / Confession Wall**.

7.1 Youth Profile

- **Growth value and level:** 21 levels (Sprout → ... → Chaos), upgrade cost increases with level ($25 \times L^2 + 75 \times L$); different levels correspond to different titles.
- **On-chain nickname:** first set **10 ENGA**, change **100 ENGA** (globally unique, duplicate rejected).
 - This nickname is the **same single on-chain record**: On-chain Youth and encrypted chat **share it**; it is not two independent nicknames; changing it in one place takes effect in the other.
 - The fee nature is **paid to the contract party (developer fee pool)**, not burned.
- **My Youth Manifesto:** published on-chain, text cap **500 characters**; the contract **enforces a minimum of 1 ENGA**, rejection if insufficient (fee paid to the contract party, not charged per character, plus network fee).
- You can "publish / republish" the manifesto; there is also a "Confession Wall" publishing entry.

7.2 Youth Ranking

- Browse others' manifestos, sort by **popularity / time / nickname**, searchable, can show "Mine" only.
- Click a single entry to open details: you can **like** and **comment**.
 - **Like:** free (the attached on-chain value is returned as-is, only network fee is consumed), the author does not get coins from it.
 - **You cannot like your own post:** clicking your own manifesto directly prompts "Cannot like your own post", no transaction is initiated, no fee is deducted.
 - **Comment:** consumes **0.5 ENGA + network fee**. This fee is **paid to the contract party (developer fee pool)**, **not** to the manifesto author; the author receives **growth value** compensation.

7.3 Confession Wall

- A separate sub-page, sorted by **popularity / latest**, can show "Mine" only.
- Publish: **anonymous by default**, can @ a target (nickname or address), consumes **2 ENGA (paid to the contract party)**, not burned).
- **Comment** on a confession: consumes **0.5 ENGA** (also paid to the contract party).

- **Likes are free**, but **you cannot like your own confession** (direct prompt, no transaction initiated).

8. Off-chain Encrypted Chat

The "Chat" tab is **end-to-end encrypted** chat (relayed for forwarding, the server cannot decrypt; nickname uniqueness is backed by on-chain fees).

8.1 Connection and Interface

- Entering chat auto-connects to the relay (default `ws://180.76.117.98:8770/ws`); images go through an image host (default `http://180.76.117.98:8780`).
- Both addresses are built-in App defaults; **the current version has no edit entry**.
- Top-right of the conversation list: backup, new group, contacts. The bottom-right "+" starts a **new conversation** (private chat by address `eg1...`, or group/channel by scope + channel name).

8.2 Nickname (Unrelated to Wallet Name)

The chat nickname is completely unrelated to the "name filled when creating the wallet". The wallet name is just a local label; the chat nickname must be explicitly set and an on-chain fee paid before it takes effect, default **empty**.

It is also **the same record as the On-chain Youth nickname** (see 7.1): they share the same on-chain record, and changing it in one place takes effect in the other.

- When empty for the first time, the button shows "Set"; after being set it shows "Modify".
- Set **10 ENGA**; modify **100 ENGA** (globally unique, duplicate rejected). The fee is **paid to the contract party (developer fee pool)**, not burned.
- Setting/modifying also publishes your **E2E encryption public key**, so friends can send you encrypted messages.

8.3 Add Friends and Chat

- In contacts click "Add": enter the **other party's address (eg1...) or nickname**; the nickname is resolved to an address by the relay (if no nickname, prompts "nickname does not exist"). Already-a-friend prompts accordingly.
- After starting a chat, messages are **end-to-end encrypted** via X25519 / NaCl box, only the two parties can decrypt.
- Sending an image: first upload to the image host to get a public link, then send it as an encrypted text message, which the other party loads automatically.

8.4 Groups and Contacts

- Contacts contain: friend requests (pending confirm / pending accept / sent / blocked), friends (note, block, remove), groups (invite / joined).
- You can create groups, accept/reject group invites; for friends you can set a **note, block, remove**.
- Conversations support **pin, mute, delete**.

8.5 Backup and Privacy

- Chat messages are not stored on-chain, only relayed; local records can be exported/restored on the **chat backup** page.
- Image-host attachments are stored on the server for long-term access; the nickname index is automatically rebuilt after restart by you re-publishing the nickname.

9. Staking

Entry: "Staking" on the Mining page, or via the Mining page quick entry.

- Staking locks ENGA to obtain **ve(ENGA) governance weight**. The lock duration determines the on-chain **ve time factor (strict tiers)**:
 - **< 6,000,000** blocks (≈ 1 year) $\rightarrow 1\times$
 - **6M–12M** blocks ($\approx 1\text{--}2$ years) $\rightarrow 2\times$
 - **12M–18M** blocks ($\approx 2\text{--}3$ years) $\rightarrow 3\times$
 - **$\geq 18M$** blocks (≈ 3 years+) $\rightarrow 4\times$ (cap)
- Governance weight = $\Sigma(\text{each lock amount} \times \text{that lock's own ve time factor})$; batch staking is weighted separately then summed.
- **Lock duration can be entered freely** (default **10000** blocks, the App prompts " ≈ 10000 blocks = 1 day" as the baseline; tiers are auto-determined by the number of locked blocks).
- You can see: lock amount, unlock height, progress, existing batches, withdrawable amount, etc.; settlement is on-chain by block height, batches past their lock period can be withdrawn.
- Staked ENGA also serves as governance voting weight (see Section 10) and is frozen during voting.

10. Governance

Entry: "On-chain Governance" on the Mining page.

- The community treasury is controlled by governance; you can submit **proposals** and **vote**.
- **Voting choices**: 0=Against / 1=For / 2=Abstain; weight = the ENGA you locked for this vote (frozen during voting, must be ≥ 1 ENGA).
- **Fee (burn)**:
 - **Submit proposal**: **burn 1000 ENGA** (threshold much higher than voting, to prevent spam proposals).
 - **Vote**: **burn 1 ENGA** + the locked voting weight.
 - Both require the wallet to reserve enough UTXOs to cover "burn amount + locked weight"; the App checks first and prompts if insufficient.
- **Proposal threshold**: from block height **210,000**, a proposal needs **balance > 10M ENGA** and **votes $\geq 5\%$ of circulation**; team-exclusive types (treasury / grant / team) are limited to founding team addresses.
- A **100-block** lock window before proposal execution prevents tampering near settlement.
- The locked weight auto-unfreezes about after voting ends + buffer (on the order of ~ 1 hour).

11. Settings (Language + Node Connection Pool + Chat Image Cache)

Settings is reached via the gear icon on the Wallet page and contains three items:

11.1 Language

- Supports Simplified Chinese / Traditional Chinese / English, single-select with instant switch.

11.2 Mainnet Node Connection Pool

- The default node pool has only one official node: <http://124.221.244.124:8545> (mainnet).
- You can **add a node** (format <http://host:port>, default port 8545), **set as default** (move to first), **test connection** (shows height / peers / sync %), **remove** (keep at least one), **reset** to default pool.
- The connection has **failover**: when the first choice is unreachable, it automatically tries other nodes in the pool.

Note: only add nodes you **trust** to the pool. Although the App decodes transactions locally before signing (see 4.4), connecting to a malicious node may still give you tampered balance and history queries.

11.3 Local Chat Image Cache

- Shows the space occupied by chat images on the device (e.g., **0.12 GB**), with one-tap **cleanup**.
- Cleanup only deletes the **local copy** and does not affect received image content — when needed, it is re-fetched from the image host; the other party's sent images remain on the server.

Note: the Settings page **does not contain** entries for staking, governance, security, or chat relay (they are on the Mining page, Security page, and within chat respectively).

12. Frequently Asked Questions (FAQ)

Q1: Why is the chat nickname empty at first and the button shows "Set"?

The chat nickname is completely unrelated to the "name filled when creating the wallet" — the wallet name is just a local label and will never automatically become the chat nickname. New users' nicknames default to empty and must be explicitly set in contacts (10 ENGA, paid to the contract party); only after being set does it show "Modify" (100 ENGA). The nickname is globally unique, duplicate rejected, and is the same record as the On-chain Youth nickname.

Q2: Are chat messages safe? Can the server see them?

Messages are end-to-end encrypted via X25519 / NaCl box; the relay can only forward, not decrypt. Nickname uniqueness is backed by on-chain fees; images are sent as encrypted text via the image host. Messages are not stored on-chain.

Q3: Is mining "keep the App active and it keeps accumulating"?

No. Mining is an optional switch; income comes from evenly splitting the block's App share (recorded as locked rewards), unlocked into liquid coins via "step tasks / AP exchange"; after ~6 hours in the background it requires manual recovery.

Q4: About how fast are blocks?

About 5–9 seconds per block; the App's "≈10000 blocks = 1 day" is for estimating the lock period.

Q5: How much do the various On-chain Youth operations cost?

Publishing a manifesto has a **minimum of 1 ENGA** (enforced by contract, rejected if insufficient, not charged per character); **like is free**; **comment 0.5 ENGA**; publishing a confession **2 ENGA**; commenting on a confession **0.5 ENGA**; on-chain nickname first set 10 ENGA, modify 100 ENGA. All the above fees are **paid to the contract party (developer fee pool)**, not burned, and are **not** paid to the content author (the author receives growth value); a small network fee also applies.

Q6: Which node is connected by default?

The default node pool only has one official node <http://124.221.244.124:8545> (RPC port 8545). You can add / set as default / test / remove / reset in Settings; only add nodes you trust.

Q7: Will switching to the background lose coins or disconnect?

No. Balance and mining status persist on the node; switching to the background does not lock the screen immediately, and auto-locks by the 10-minute idle timer.

Q8: Why do my published manifesto and like counts only change after a few seconds?

On-chain operations must wait for the transaction to enter a block (about 5 seconds per block). The App polls to confirm whether it is on-chain; if it does not take effect for a long time it prompts failure rather than pretending success.

Q9: Why does every operation pop a confirmation dialog and require identity re-verification?

This is anti-blind-signing protection. The App **decodes locally** the transaction to be signed, showing the type, payer, payee, and amount for your verification, and does not trust any description returned by the node; before confirming it also does one more biometric / password verification. If the transaction cannot be parsed or is a system transaction, the App directly refuses to sign, never letting you sign something you cannot understand (see 4.4).

Q10: Why does "Start Mining" also require my signature?

The node verifies whether the signature is derived from that wallet address. This way, even if someone can access the public RPC, they cannot register your address as a miner or divert the mining share that should belong to you.

Q11: Why does liking my own post prompt that I cannot like it?

The on-chain contract forbids liking your own manifesto / confession. The App intercepts locally first and prompts, initiates no transaction, and deducts no fee.

ENGAGE — Let every participation become on-chain assets.