DACS

CLIENT GUIDE · NOVEMBER 2026

Your step-by-step guide to a DACS verification report

For SMSF trustees and the accountants who help them. Every step is read-only: nothing in this guide moves your coins, and nothing asks for your recovery phrase.

Each chapter has a short video (1–2 minutes). The links open in your browser.

0 What you will need

Most trustees finish in one sitting once the documents are to hand. Set aside half an hour.

Equipment

- **A computer, not a phone.** Use Chrome, Edge or Brave. The wallet steps do not work in Safari or Firefox.
- **Your mobile phone.** We text you a one-time code when you connect a wallet.
- **Your hardware wallet and its USB cable** (Ledger), or the MetaMask extension installed — if you will sign the message in Step 4.

Documents and details

- **Identification** for one or two of the trustees or directors (two is better): driver licence or passport.
- **Proof of address** for at least one of them, ideally two: a utility bill issued in the last three months.
- **The fund's trust deed**, or another document that names all the members.
- **Corporate trustee:** the company's ASIC certificate of registration.
- **Exchange logins**, to create a read-only key for each exchange account.
- Your **accountant's and auditor's email addresses**.

Who should do this

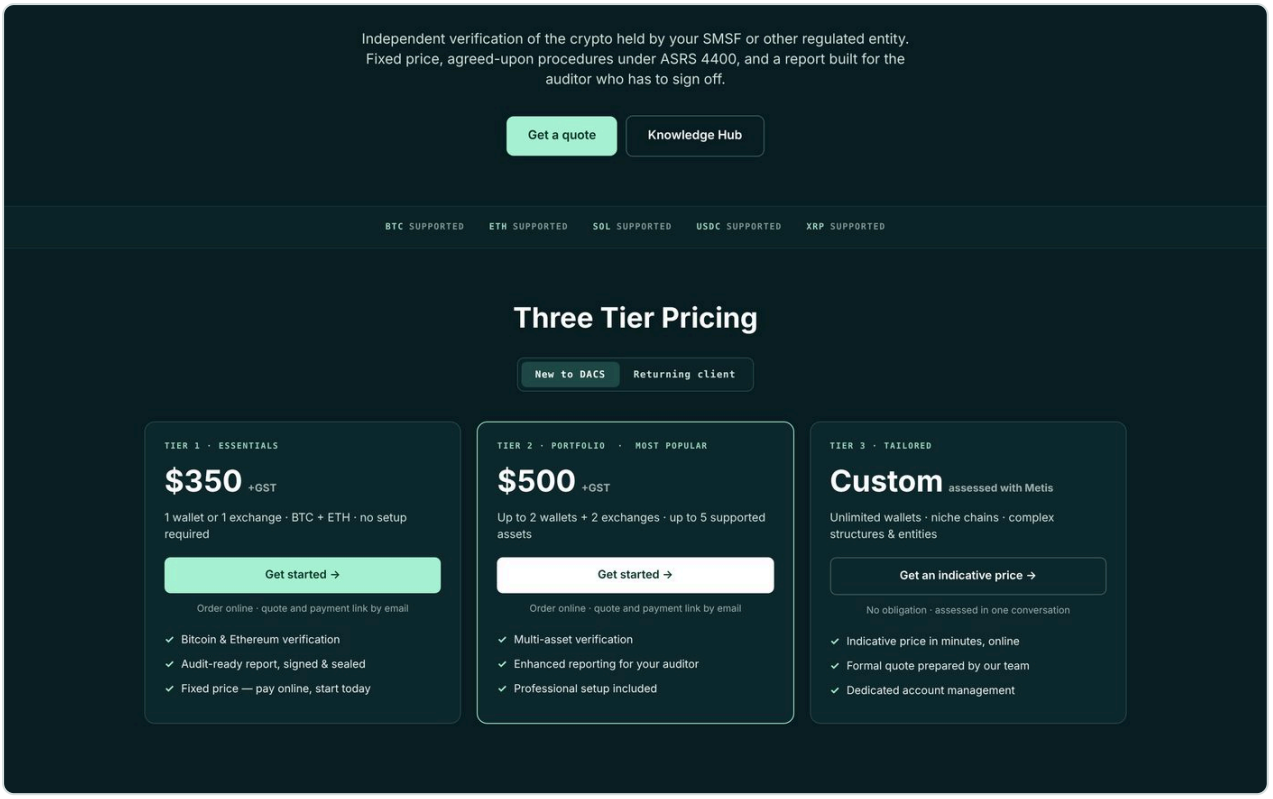
A trustee, or a director of the corporate trustee. Your accountant can register and upload documents on your behalf, but the signed message in Step 4 needs the person who holds the wallet. If someone other than a trustee will sign, the trustees nominate that person when we ask, after the quote.

> **NEVER**
> DACS never asks for your recovery phrase (seed words), your wallet PIN, a private key, an exchange password or a two-factor code. Anyone who does is not DACS. Every step below is read-only.

1 Get a quote — new or returning

▶ Watch chapter 1 — Quote and registration (1:12): https://media.dacs.io/getting-started/DACS-Getting-Started-1.mp4

Pricing is on the front page of dacs.io. Choose **New to DACS** or **Returning client**, then the tier that matches your holdings.



dacs.io — Three Tier Pricing. Current prices are shown on the site.

- **Tier 1 · Essentials** — one wallet or one exchange account, holding Bitcoin and/or Ethereum only. Order online; your quote and payment link arrive by email.
- **Tier 2 · Portfolio** — up to two wallets and two exchange accounts, up to five supported assets. Order online; your quote and payment link arrive by email.
- **Tier 3 · Tailored** — more wallets, niche chains, staking, trusts or companies, several funds. Chat with Metis for an indicative price; our team then prepares a formal quote.

> **NOTE**
> A third asset of any kind makes the engagement Tier 2, even on a single exchange. If you are not sure, ask Metis — it works out the tier from your holdings.

Accepting the quote

Accepting and paying the quote is the agreement between you and DACS. There is no separate engagement letter. The quote sets out what is in scope — the wallets, exchange accounts and assets we will verify — so check it before you pay. Quotes are valid for 14 days.

Returning clients

Most repeat verifications check what has changed rather than starting again. Choose **Returning client** and tell Metis what is different: new wallets, assets sold, a change of trustee, accountant or auditor. Your

entity details and identification carry forward unless they have changed. Two things are fresh every year:

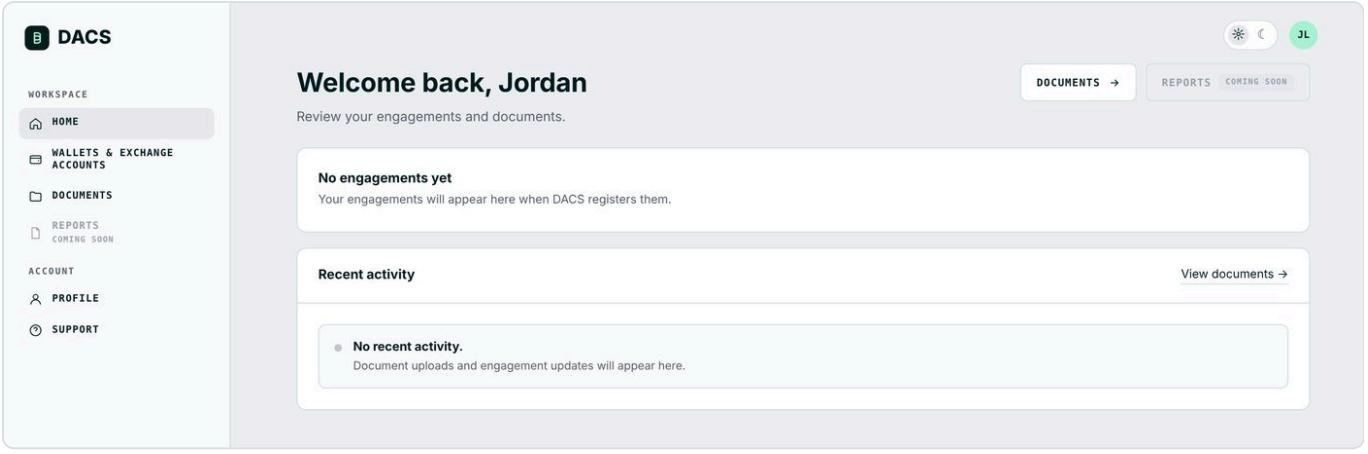
- **Exchange keys.** Read-only keys expire or get revoked. Expect to issue a new one for each exchange account.
- **The signed message.** A signature proves control on the day it is made, so we run it again each year — same wallet, same coins, new proof.

---

2 Create your portal account

The DACS portal at portal.dacs.io is where you upload documents, connect wallets and save exchange access. Everything you give us goes through the portal — not by email.

1. **Go to dacs.io and click Log-in/Register** (top right). It takes you to portal.dacs.io.
2. **Register with your name, email address and mobile number.** Use the same email address you used for the quote, so we can match your account to your order.
3. **Check your mobile number carefully.** The one-time code for connecting a wallet goes to this number.
4. **Complete the short profile set-up.** When it asks what kind of account you are opening, choose the option for **verifying a fund's or business's holdings** (on some screens it reads **Company / Organization**). That applies to an SMSF, trust or company, whether the trustee is an individual or a company — almost everyone using this guide. The other option is for auditors, accountants and advisers who review clients' reports. Then open your Home page.



Your Home page. "No engagements yet" is normal until DACS links your paid order to your account.

The left-hand menu is the whole portal: **Home**, **Wallets & exchange accounts**, **Documents**, **Reports** (coming soon), **Profile** and **Support**.

---

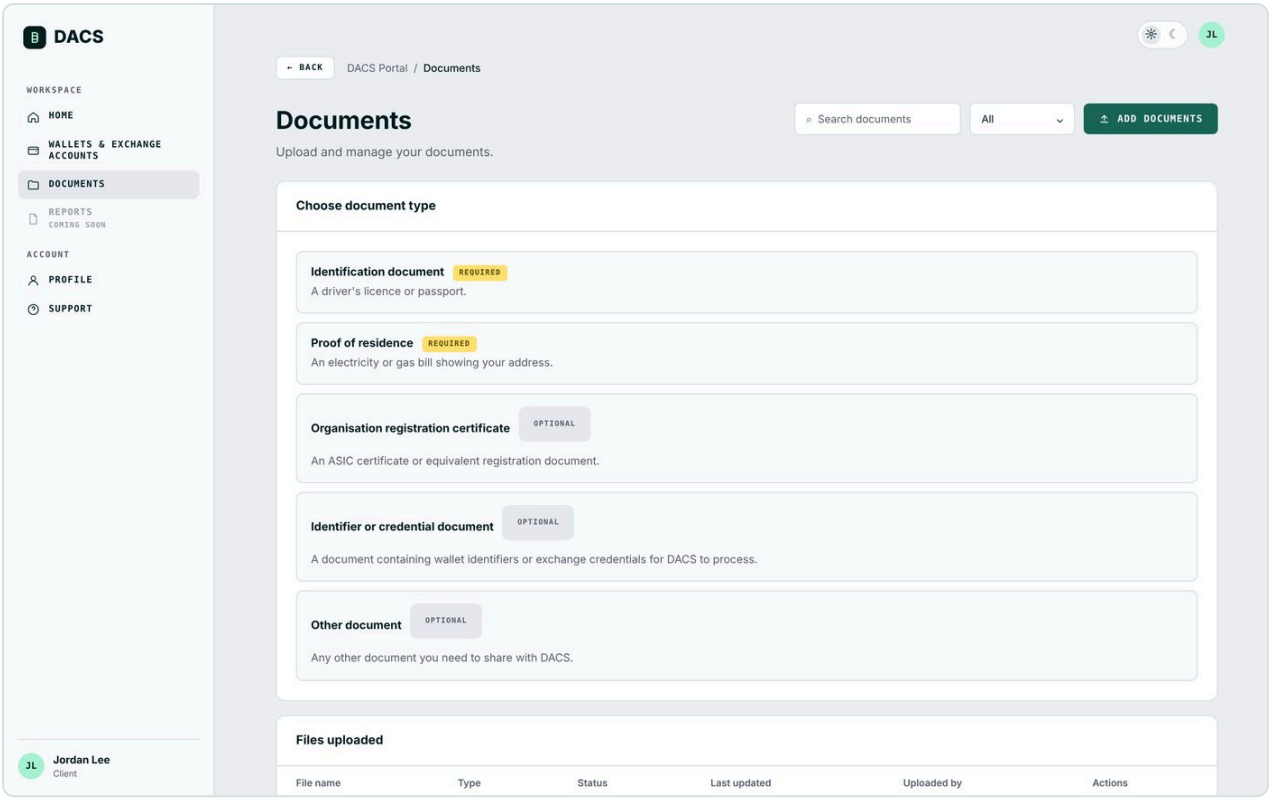
3 Identity documents

▶ **Watch chapter 2 — Identity documents** (1:37): https://media.dacs.io/getting-started/DACS-Getting-Started-2.mp4

Your report ties the holdings to the fund and its trustees. That link is what your auditor relies on, so we identify the trustees, the fund's members and, where the trustee is a company, the company itself. You do not need ID from every trustee or director: one or two is enough, and two is better.

What to upload

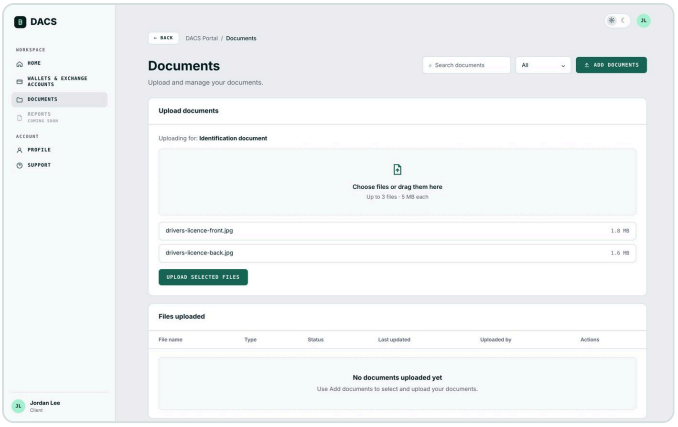
Go to **Documents → Add documents** and choose the document type first. Each type tells you what it needs.



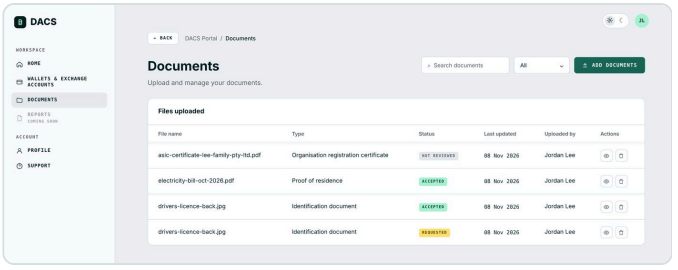
Documents → Add documents → Choose document type.

- **Identification document** (one or two trustees or directors) — driver licence (front and back) or the photo page of a passport. In date, all four corners visible, every line readable.
- **Proof of residence** (at least one trustee or director, ideally two) — a utility bill issued in the last three months, showing the name and the address on the ID. A council rates notice or bank statement also works.
- **Organisation registration certificate** (if the trustee is a company) — the ASIC certificate of registration, or a current company extract.
- **Other document** — the fund's trust deed, or another document that names all the members. Also statutory declarations, or anything else we ask for.
- **Identifier or credential document** (only when asked) — for example a signed-message text file (Step 4) or a CoinSpot transaction history (Step 5). Wallet identifiers and exchange keys otherwise go in the portal's Saved identifiers area, not here.

1. **Choose the document type**, then **Choose files or drag them here**. Up to three files per upload, 5 MB each.
2. **Name files by person** — for example `jane-citizen-licence-front.jpg` — so a fund with several trustees stays clear.
3. **Click Upload selected files.** The file appears in **Files uploaded** with the status **Not reviewed**.
4. **Repeat** for each document type and each person providing ID.



Two files selected for an Identification document.

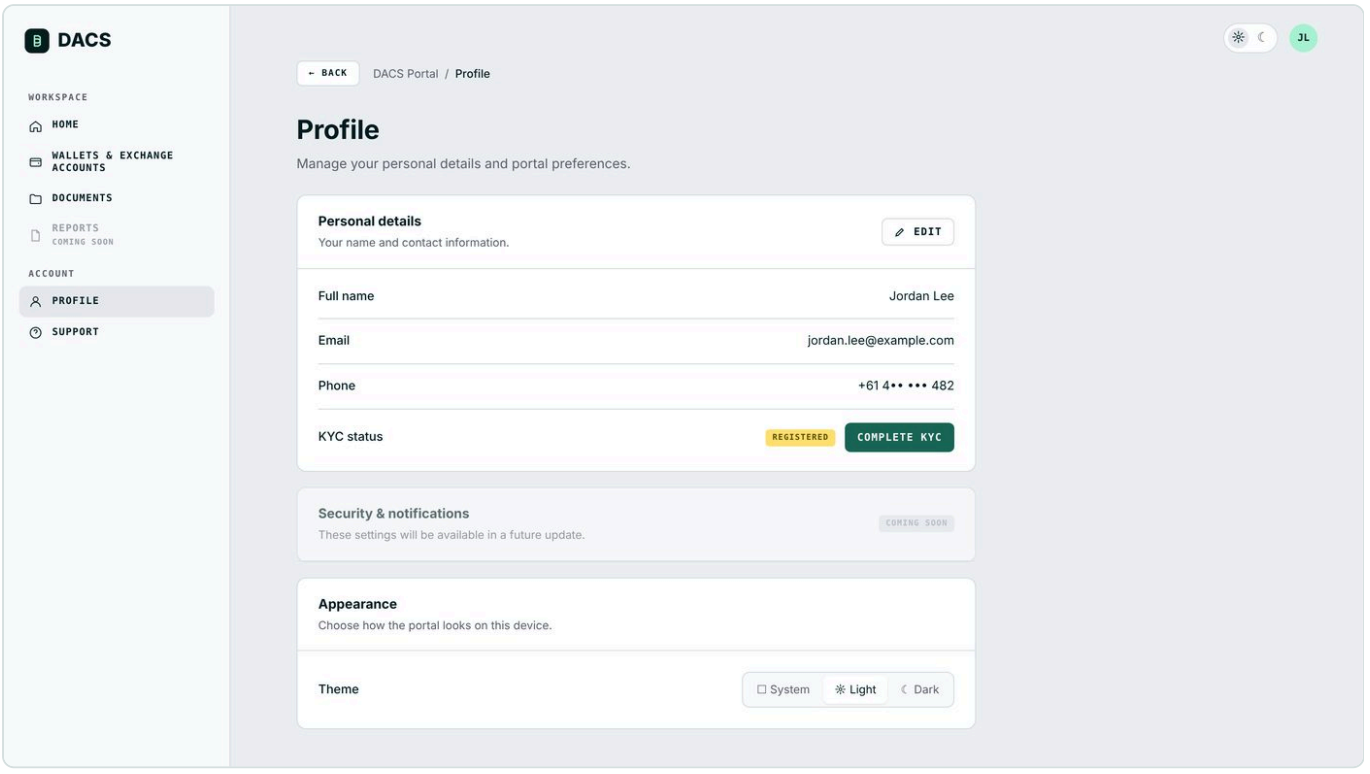


Statuses: Not reviewed, Accepted, Rejected, Requested.

What the statuses mean

- **Not reviewed** — received, waiting for a DACS officer.
- **Accepted** — done.
- **Rejected** — we could not use it (blurred, cropped, expired). We tell you why; upload a replacement.
- **Requested** — we need a document you have not yet uploaded.

Your **Profile** page shows your overall KYC status, and **Complete KYC** takes you to the same uploads.



Profile → KYC status.

If you have no proof of address

If you cannot produce a bill or statement in your name, ask us for the DACS statutory declaration form. Complete it, have it witnessed, and upload the signed declaration under **Other document**.

4 Prove control of your wallet — the signed message

▶ **Watch chapter 3 — The signed message** (2:02): https://media.dacs.io/getting-started/DACS-Getting-Started-3.mp4

A blockchain shows that an address holds a balance. It does not show who controls it. The signed message closes that gap: you sign a one-off message on your own device, and we verify the signature against the address.

> **WHAT A SIGNED MESSAGE IS — AND IS NOT**
>
> - It **is** a short piece of text signed with your wallet's key. We check the signature against the address it claims.
> - It is **not** a transaction. No coins move, there is no fee, and nothing is written to the blockchain.
> - Your recovery phrase, PIN and private keys **stay on your device**. The portal never sees them, and we never ask for them.
> - The message names your portal email address and the wallet address, so you can read exactly what you are signing. Your device shows the same text.

Supported today

Ledger (Bitcoin and Ethereum) and **MetaMask** (Ethereum). Trezor owners: see "Trezor and other wallets" below.

Before you start

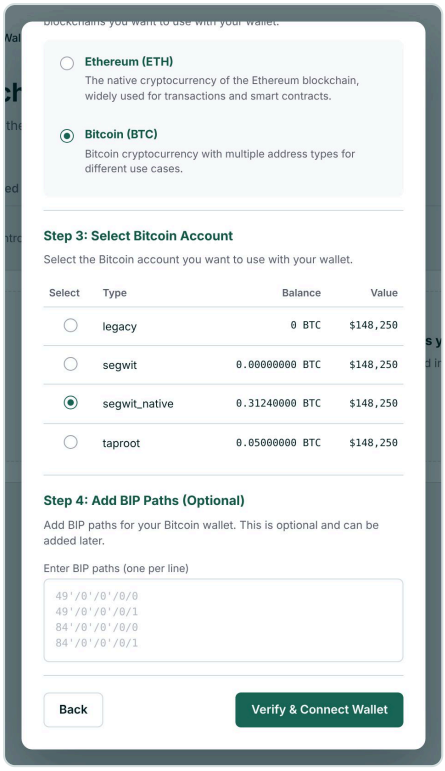
- A computer running Chrome, Edge or Brave. Hardware wallets connect over USB in the browser, which Safari and Firefox do not support. Phones and tablets cannot do this step.
- Your Ledger connected by USB, unlocked, with the **Bitcoin** or **Ethereum** app open on the device.
- The Ledger Wallet app (formerly Ledger Live) closed. If it is open it holds the USB connection and the browser cannot see the device.
- Your mobile phone within reach for the one-time code.

Connecting a Ledger

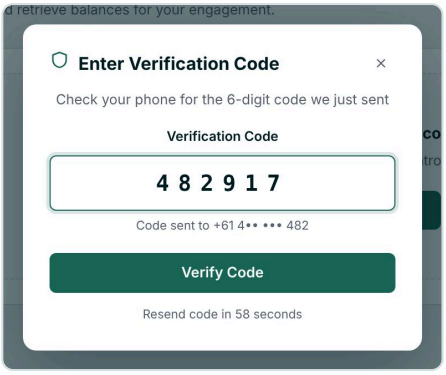
1. **Open Wallets & exchange accounts and click Connect wallet.**
2. **Step 1 — choose Ledger.** (Choose MetaMask if that is what you use; see below.)
3. **Step 2 — choose the blockchain:** Bitcoin or Ethereum. One at a time. If the fund holds both, repeat the whole process for the other.
4. **Allow the connection.** Your browser asks permission to connect to the device. Select your Ledger and click Connect.
5. **Step 3 (Bitcoin only) — select the account.** The portal lists the Bitcoin accounts on your device by type — legacy, segwit, native segwit (shown as `segwit_native`) and taproot — with their balances. Select the account that holds the fund's bitcoin. If in doubt, it is the one with the balance you expect to see.
6. **Step 4 — BIP paths are optional.** Leave this blank unless we have asked you to fill it in.
7. **Click Verify & Connect Wallet.**
8. **Enter the 6-digit code** we text to the mobile number on your profile.
9. **Review the message.** The portal shows the message — your portal email and the wallet address — and asks you to review it on your Ledger. The same text appears on the device screen. Check they

match, then approve on the device.

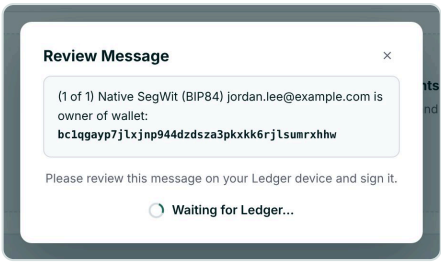
10. **Done.** The wallet appears under **Connected wallets** with the addresses that hold a balance and today's value. (Your report uses the value at your fund's balance date, not today's.)



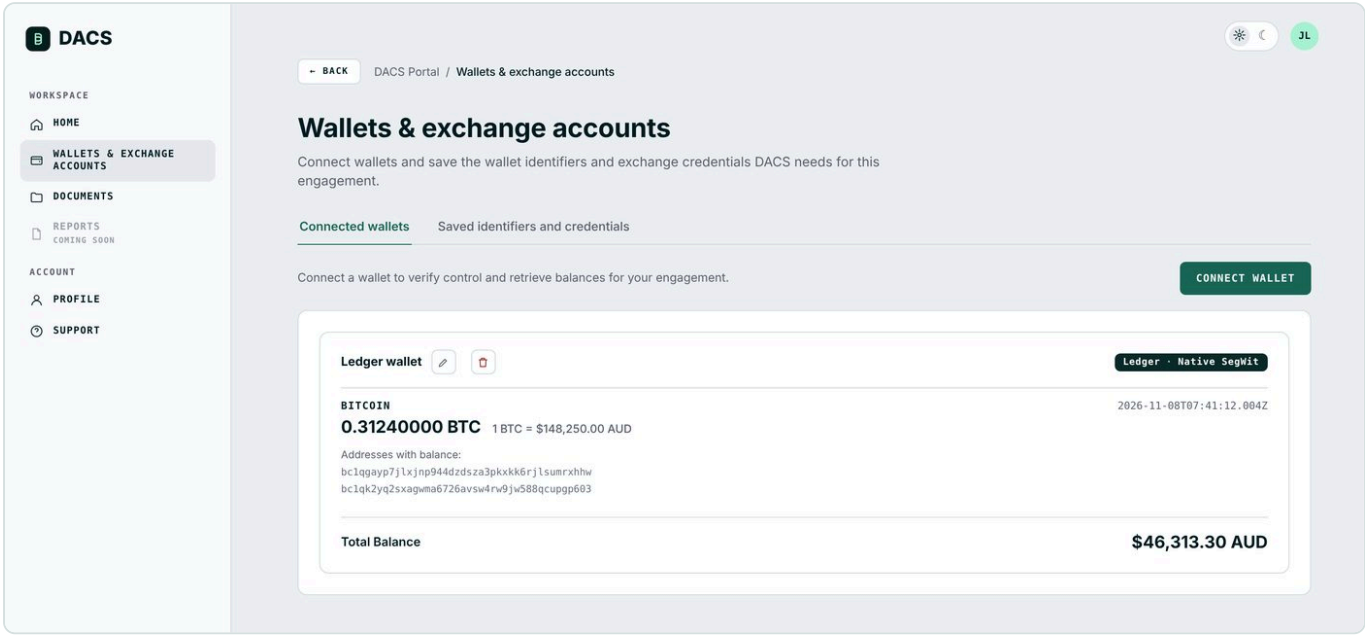
Steps 2–4: choose Bitcoin, select the account, leave BIP paths blank.



The one-time code goes to your mobile.



Compare this text with your Ledger screen, then approve on the device.



Connected: the addresses holding a balance, and the value at today's price.

Connecting MetaMask

Unlock the MetaMask extension first. Choose **MetaMask** at Step 1 and **Ethereum** at Step 2, then **Verify & Connect Wallet**. After the one-time code, MetaMask opens a signature request. Read the message, then click **Sign**. There is no gas fee, because nothing is sent to the network.

If something goes wrong

- **The browser cannot find the device.** Close the Ledger Wallet app, unplug and re-plug the Ledger, unlock it, open the Bitcoin or Ethereum app, and try again. Check you are in Chrome, Edge or Brave.
- **The message on the device does not match the screen.** Reject it on the device and contact us through Support.
- **No code arrives.** Check the mobile number on your Profile page.
- **You selected the wrong account.** Tell us through Support; we can remove it and you can connect again.

If you prefer not to sign

The signed message is not compulsory, but it is the stronger evidence. If you do not connect your wallet, give us your wallet identifiers instead (Step 5) and we verify the balances from those. Your report will then record that the balances were taken from identifiers you supplied and that control of the wallet was not tested. Your auditor may not accept that — ask before you decide.

Trezor and other wallets we cannot connect yet

The portal does not yet connect to a Trezor. You can still prove control yourself. We send you a message to sign — the fund name, the financial year and a one-time code — and you sign it in Trezor Suite:

1. **Open Trezor Suite**, select the account, click the three dots and choose **Sign & Verify**.
2. **Type the message exactly as we sent it** into the Message box.
3. **Paste an address from that account** into the Address box — one that held the fund's coins at 30 June.
4. **Click Sign**, check the message on your Trezor screen, then confirm.
5. **Copy the message, the address and the signature** into a plain text file and upload it under **Documents → Identifier or credential document**. Then save the account's xpub in Step 5.

Trezor Suite cannot sign from a Taproot account. If that is where the coins are, give us the xpub and we report on that basis.

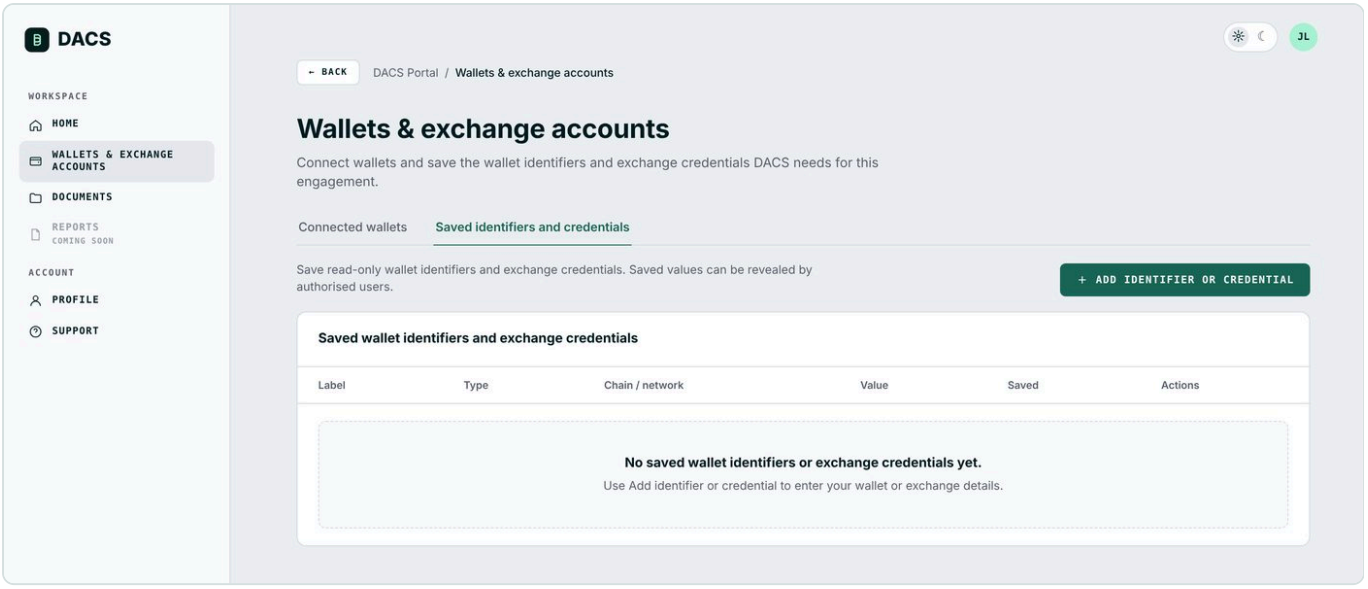
---

5 Save your identifiers and exchange access

▶ Watch chapter 4 — Identifiers and API keys (2:17): https://media.dacs.io/getting-started/DACS-Getting-Started-4.mp4

Everything we read is read-only. For a wallet that is an extended public key or an address; for an exchange it is a read-only API key. Save them in the portal under **Wallets & exchange accounts → Saved identifiers and credentials**.

> **ALREADY CONNECTED A WALLET IN STEP 4?**
> If you connected it and signed the message, you do not need to save it again here. Use this step for wallets you could not connect or chose not to sign with, and for every exchange account.



Saved identifiers and credentials → Add identifier or credential.

> **IMPORTANT**
> **Type or paste identifiers and keys as text.** Never send a screenshot or photo of them — we cannot use an image and will have to ask again. Never send them by email.

Extended public key or address: the rule

This is the question that trips up most trustees, so here is the rule.

- **Bitcoin** (also Litecoin, Bitcoin Cash, Dogecoin) — give us the account's **extended public key** (`xpub…`, `ypub…` or `zpub…`). A Bitcoin wallet is not one address: every payment can land on a new address, and change goes to another. The extended public key lets us see every address in the account, balances only.
- **Ethereum** and ERC-20 tokens — the account **address** (`0x…`). Ethereum uses one address per account; the address is the account.
- **Solana, XRP, Cardano, Polkadot, Stellar** and other account-based chains — the account **address**. Same as Ethereum: one address per account.
- **Staked or wrapped positions, DeFi, NFTs** — tell us through Support before you add anything. These need scoping, and may change your tier.

> **TIP**
> An extended public key can see balances and addresses. It cannot move coins. Give it to DACS through the portal and nobody else: anyone holding it can see your whole account history.

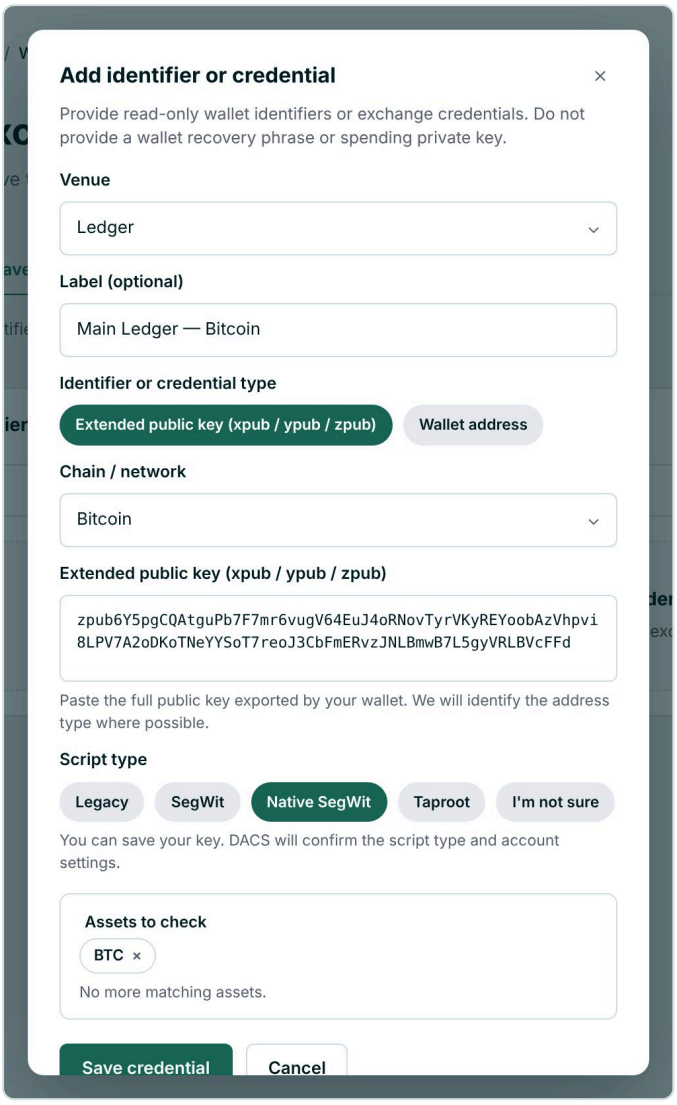
Where to find your Bitcoin extended public key

- **Ledger Wallet (formerly Ledger Live):** Accounts → select the account → the settings cog → Advanced → the **xpub** field. Copy it exactly.
- **Trezor Suite:** select the account → the three dots → **Show public key (XPUB)**.
- **Sparrow:** Settings → the keystore shows the **xpub**. **Electrum:** Wallet → Information.

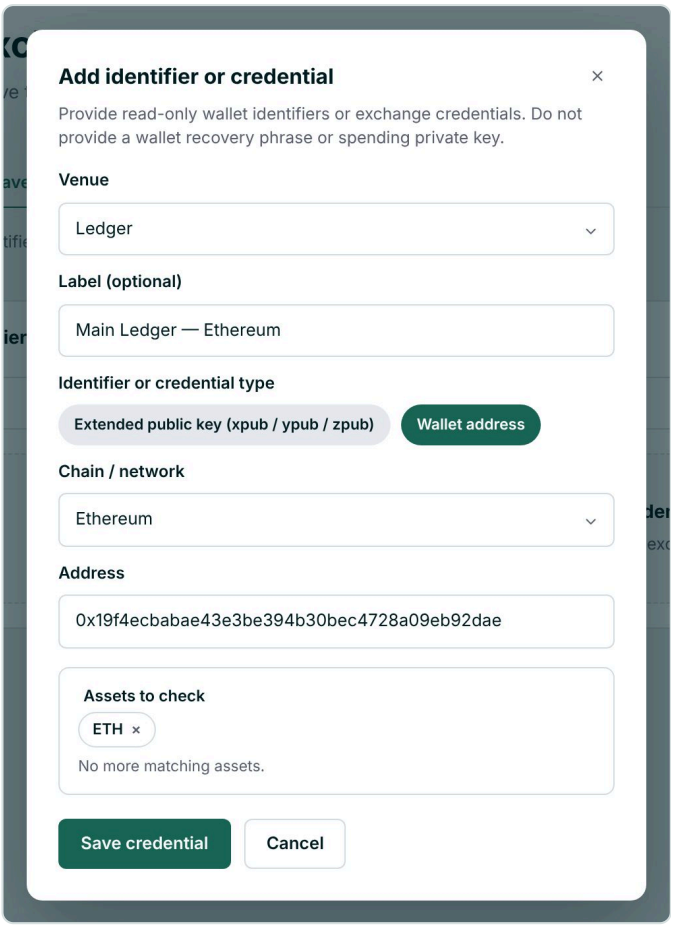
Give us the key exactly as your wallet shows it. The prefix tells us the account type: `xpub` legacy or taproot, `ypub` segwit, `zpub` native segwit. If you are not sure, choose **I'm not sure** for the script type and we work it out.

Adding a wallet identifier

1. **Venue:** Ledger, Trezor, or "Other" with a name.
2. **Label (optional):** something you will recognise — "Main Ledger — Bitcoin".
3. **Type:** Extended public key, or Wallet address.
4. **Chain / network:** Bitcoin, Ethereum, XRP Ledger, Solana and so on.
5. **Paste the key or address.** For Bitcoin choose the script type if you know it.
6. **Assets to check:** the assets held in that wallet. Then **Save credential**.



Bitcoin: extended public key, script type, assets to check.

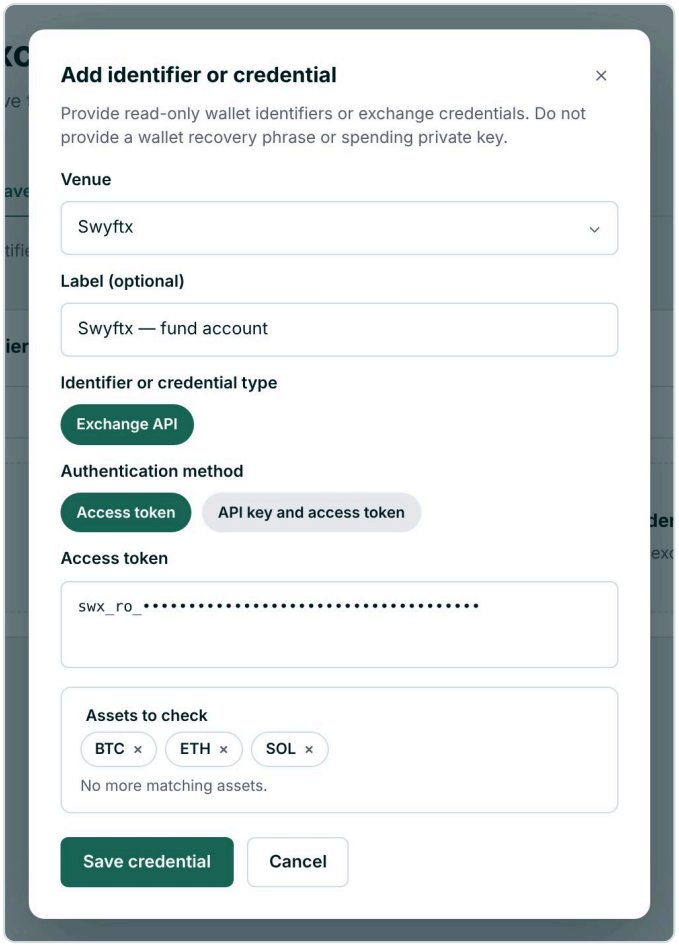


Ethereum: the account address.

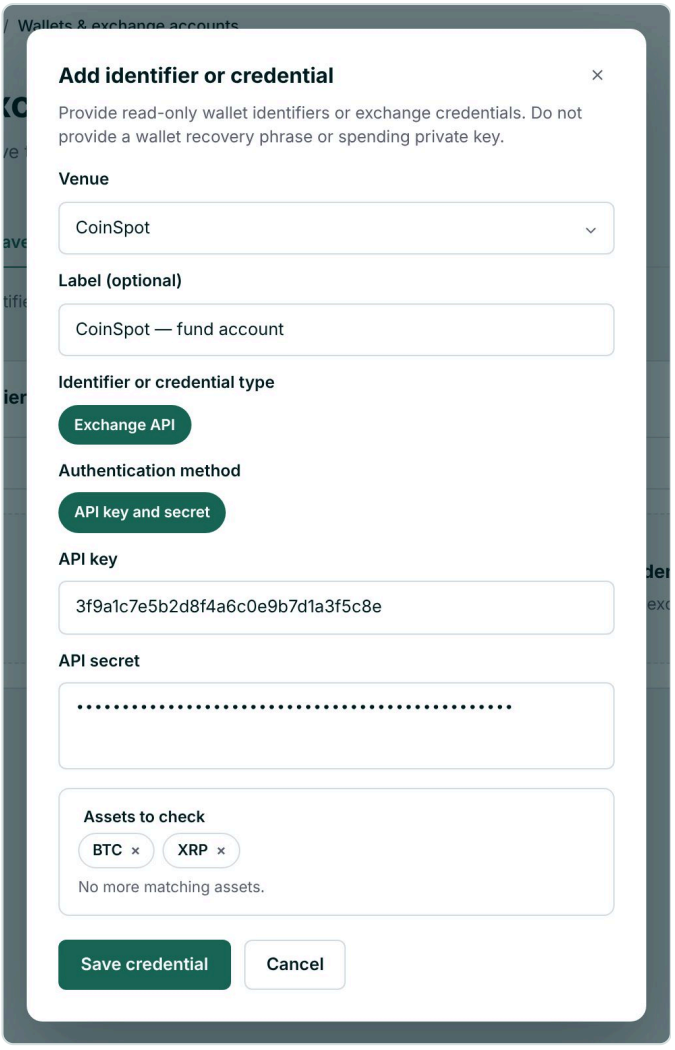
An exchange account: read-only API access

Coins on an exchange sit in the exchange's custody, so there is no wallet to sign with. Instead you give us read-only access to the account and we pull the balances and transaction history ourselves. Read-only means balances only — no trading, no withdrawals.

1. **In your exchange account, create a new API key.** Choose **Read only** (sometimes called "view" or "query") and nothing else. Set the expiry to at least seven days so it stays valid while we work.
2. **In the portal, choose the exchange as the Venue** — CoinSpot, Coinbase, Swyftx, Kraken, Binance, BTC Markets, Hyperliquid, or Other.
3. **Paste the key.** Swyftx: the read-only access token on its own is enough. CoinSpot and the others: the API key and the API secret. Paste as text, straight from the exchange.
4. **Add the assets held** on that exchange, then **Save credential**.



Swyftx: access token.

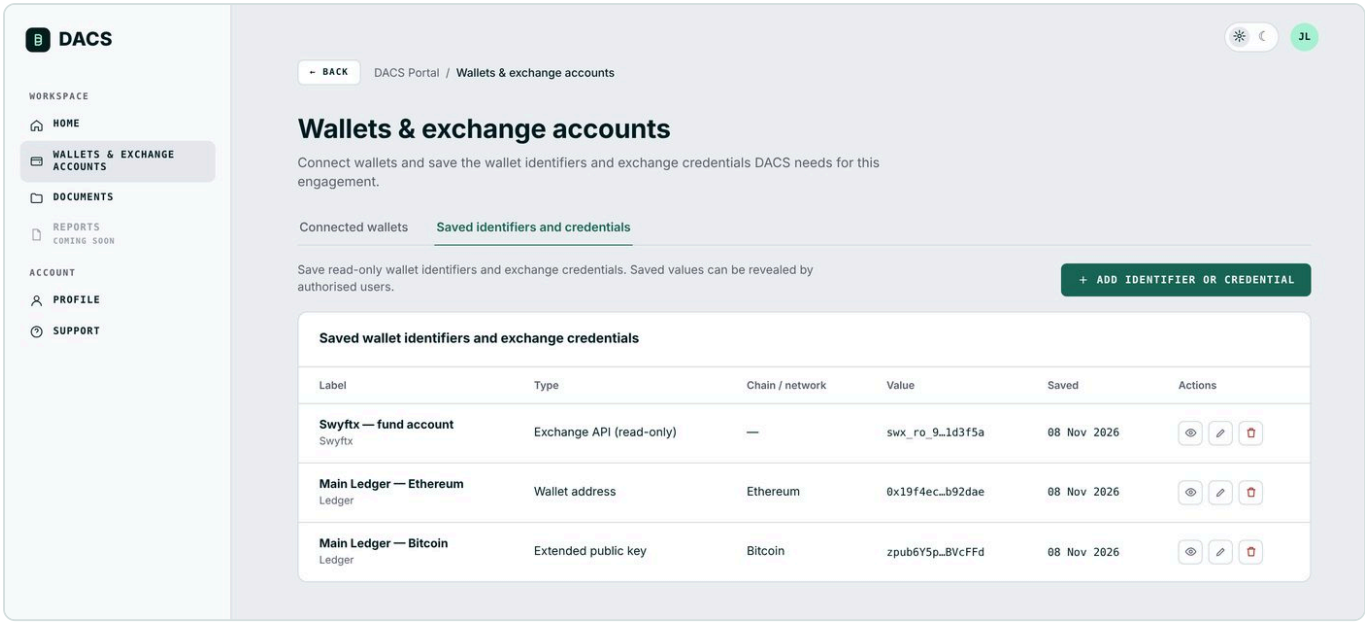


CoinSpot: API key and secret.

If your exchange is not listed, or you cannot see how to make a read-only key, tell us which exchange it is through Support and we send you the steps.

> **COINSPOT CLIENTS**
> CoinSpot does not provide a balance as at 30 June, so we also need a transaction history report downloaded from CoinSpot. Upload it under **Documents → Identifier or credential document**.

We treat your exchange credentials as confidential, use them only to read the account for this engagement, and destroy them once verification is complete. You can also delete the key in your exchange account once your report has issued.



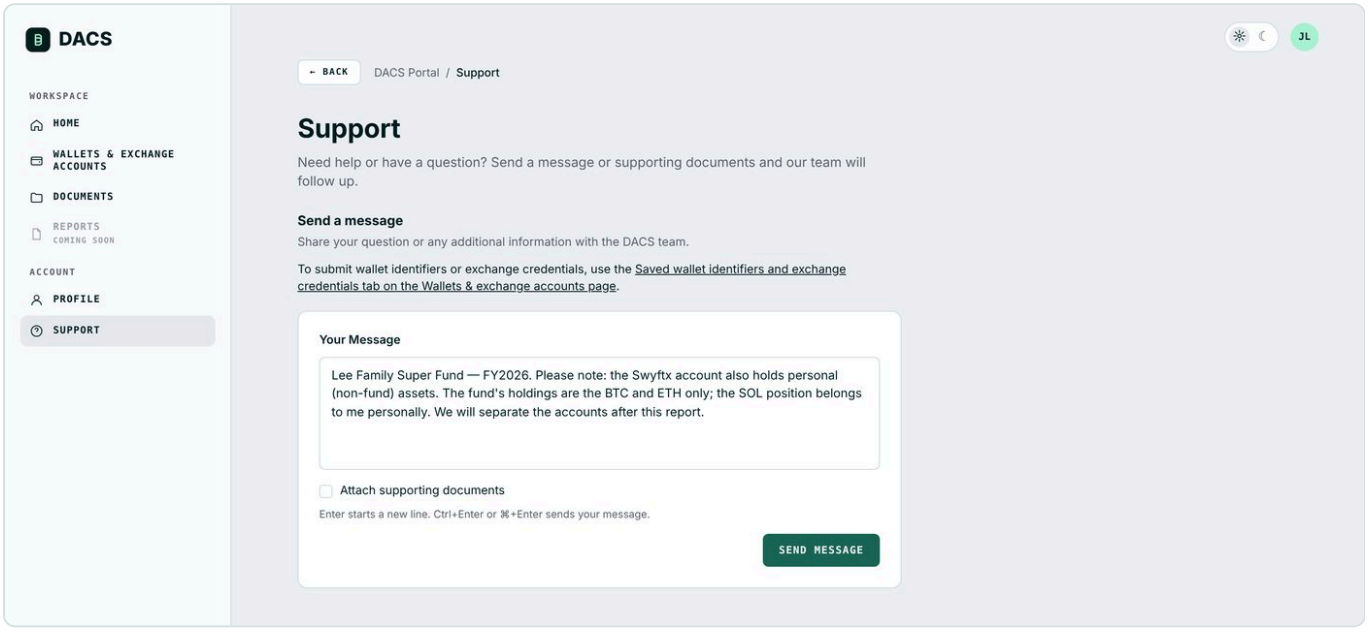
Saved. Values are masked; authorised DACS officers can reveal them to run the verification.

6 Tell us what we need to know

Use **Support → Send a message** in the portal. Attach documents there if you need to. Four things matter.

Fund and personal assets in the same place

Fund assets should sit in their own wallet or exchange account, separate from anything you hold personally. If they are mixed, tell us before we start: which holdings belong to the fund and which do not. We report the position as it stands at the balance date, with that explanation. You can separate the holdings afterwards — that will not hold up this report.



Support → Send a message. An example of telling us about mixed holdings.

Everything the fund holds

List every wallet and exchange account holding fund assets at the balance date. Our evidence can show what exists in the places you point us to; it cannot show that nothing exists elsewhere. If a wallet or

account is left out and comes to light after the report has issued, we adjust the report — by reissuing it or adding an addendum — and there is a cost either way.

Coins that have moved

If coins have moved since 30 June — sold, transferred, moved to a new wallet — say so. We evidence the balance at the balance date from statements and the transaction history, and the signed message evidences control today.

Who holds the device and who will sign

Tell us who holds the hardware wallet, and whether anyone other than the trustees has had access to it or to its recovery words during the year. If someone other than a trustee will sign the message, the trustees nominate that person when we ask, after the quote.

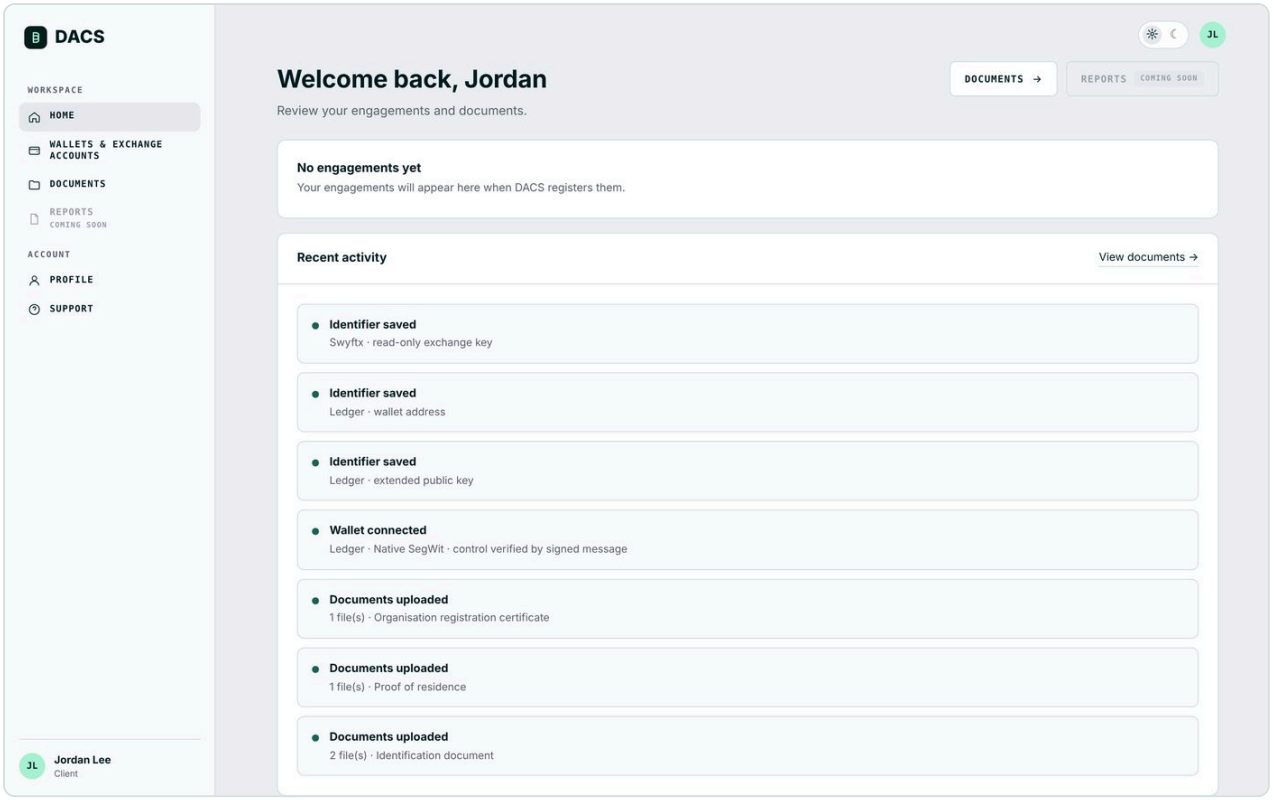
> **NOTE**
> Also confirm your accountant's and auditor's email addresses. The sealed report goes to you, with both copied.

---

7 What happens next

Once your documents, wallets and identifiers are in, the work moves to us.

1. **We check your documents.** Watch the statuses on the Documents page. If something is missing, it shows as **Requested**.
2. **We verify.** Read-only, from the source: signatures checked against addresses, balances read on-chain and from exchange accounts, each holding priced at your balance date.
3. **We draft, and a person checks.** The report is drafted from the evidence and checked by an authorised DACS officer. This takes time after verification is complete — the report does not issue the moment your wallet connects.
4. **We seal and send.** The finalised PDF is hashed so it cannot be quietly changed, and emailed to you with your accountant and auditor copied.



Home → Recent activity records each upload, connection and saved identifier.

Next year

Your identity documents and entity details carry forward unless something has changed. Each year you will issue fresh read-only exchange keys and sign a fresh message, because both are evidence of a point in time.

---

8 Help and common questions

Questions about your engagement: **Support** in the portal, or support@dacs.io. Questions about price or tier before you order: **Metis**, on dacs.io.

Is signing a message safe?

A message signature cannot move coins and does not reveal your private key. It is the same mechanism wallets use to prove ownership, and the reason the portal shows you the exact text before your device signs it.

Why can't I do this on my phone?

Hardware wallets connect to the portal over USB through a desktop browser. Documents and identifiers can be added from any device; the signed message needs a computer.

Why do you need my mobile number?

The one-time code confirms that the person at the keyboard also holds the phone registered to the account. It is one more link between the person, the account and the wallet.

What is a BIP path?

A technical setting that tells the portal where in your wallet to look. The defaults cover almost every wallet. Leave it blank unless we ask.

My trustee is a company with several directors. Who provides ID?

One or two directors — two is better — plus the company's ASIC certificate of registration and the fund's trust deed (or another document that names all the members). Upload them all under the one portal account, named by person.

Can my accountant do this for me?

Your accountant can register as the contact and upload documents and identifiers. The signed message needs whoever holds the wallet, because the device has to be in their hands.

Do I have to do all this every year?

Identity documents only if they have changed. Exchange keys and the signed message, yes — each year's report needs fresh evidence.

Digital Asset Compliance Solutions Pty Ltd · ABN 80 625 017 110 · dacs.io · portal.dacs.io · support@dacs.io

DACS performs agreed-upon procedures engagements under ASRS 4400. An agreed-upon procedures engagement is not an audit, review or other assurance engagement, and DACS expresses no opinion and no assurance conclusion. Screens in this guide are shown with dummy data.