



Secret Digits — Getting Started & Feature Guide

Every feature explained in plain English, step by step. Looking for quick answers? [Try the FAQ.](#)

[Download guide \(PDF\)](#)

Welcome — what Secret Digits does

Secret Digits is a digital safe for your passwords, API keys, notes, codes and documents. It works on a simple promise called zero-knowledge: only you hold the key. Everything is scrambled (encrypted) on your own device before it is saved, so we can never read your secrets — not even if we wanted to.

☰ HOW TO USE IT

1. Create a free account with your email address.
2. Choose a master password — this is the one key to your safe.
3. Unlock your safe and start adding your secrets.

💡 GOOD TO KNOW

- Zero-knowledge means we cannot see, read or recover your items.
- If you forget your master password, we cannot reset it — keep your recovery codes safe.

Creating your account

Your account is the front door to your safe. Signing up takes about a minute and needs only your email and a master password.

☰ HOW TO USE IT

1. Open the sign-in page and choose “Create a vault”.
2. Enter your email address.
3. Type your master password, then type it again in the “Confirm password” box. If the two do not match, the app tells you straight away.
4. Tap the eye symbol on either box to reveal what you typed, so you can check it is correct.
5. Press “Create account” and check your email for a verification link.

💡 GOOD TO KNOW

- Use a long master password you do not use anywhere else.
- The create button stays greyed out until both password boxes match.

Signing in & the master key

Signing in unlocks your safe with your master password. Because the safe is zero-knowledge, the master password can never be recovered or reset by anyone — including us. Recovery codes are your spare key.

HOW TO USE IT

1. Enter your email and master password on the sign-in page.
2. The app unscrambles your vault on your own device — nothing readable ever leaves it.
3. If you have set up a passkey or Face/Touch ID, you can use that instead.
4. If you lose your master password, use one of your recovery codes to get back in.

GOOD TO KNOW

- Store recovery codes somewhere offline, like a printed copy in a drawer.
- The safe locks itself after a period of inactivity — that is normal and keeps you safe.

Passkeys & Face/Touch ID

A passkey lets you unlock your safe with your fingerprint, face or device PIN instead of typing the master password each time. It uses the security already built into your phone or computer.

HOW TO USE IT

1. Sign in and open Settings.
2. Find the Passkeys section and choose “Add a passkey”.
3. Your device asks for your fingerprint, face or PIN — follow its prompt.
4. Give the passkey a name (for example “My iPhone”) so you recognise it later.
5. Next time you sign in, choose the passkey option instead of typing.

GOOD TO KNOW

- You can register more than one passkey — one per device is a good habit.
- Removing a passkey in Settings stops that device from unlocking your safe.

Vault

The vault is the heart of Secret Digits — the safe itself. It stores passwords, API keys, 2FA codes, secure notes, credit cards and documents, all encrypted before they leave your device.

HOW TO USE IT

1. Open Vault from the sidebar.
2. Press “Add item” and pick the type: password, API key, 2FA code, note, card or document.
3. Fill in the details and save — the item is encrypted instantly.
4. To change an item, open it and press Edit. Tap the star to mark favourites.
5. Copy buttons place values on your clipboard, which is wiped automatically after a short time.

GOOD TO KNOW

- The vault locks itself when you are away; unlock again with your master password or passkey.
- Favourites float to the top, handy for the logins you use daily.

Vault Explorer

Vault Explorer is a browsing view of everything in your safe — like a tidy filing cabinet you can filter and sort.

HOW TO USE IT

1. Open Vault Explorer from the sidebar.
2. Use the filters to narrow by type (passwords, notes, cards and so on).
3. Click any item to open it in the vault.

GOOD TO KNOW

- Explorer is great for a regular tidy-up: spot duplicates and old items you no longer need.

Search

One search bar for the whole app. Press Cmd+K (Mac) or Ctrl+K (Windows) anywhere to open it, or use the search button in the top bar.

HOW TO USE IT

1. Press Cmd/Ctrl+K, or click Search in the header.
2. Type a few letters of what you are looking for.
3. Pick a result to jump straight to it.
4. Use the filters to narrow results to vault items, pages or admin tools.

GOOD TO KNOW

- Privacy rule: you only ever see your own items. Nobody can find another person's vault items through search.
- Search matches item titles — never the secret contents.

Password Generator

The generator creates strong, random passwords for you, so you never have to invent (or reuse) one again. A strength meter shows how hard each password would be to crack.

☰ HOW TO USE IT

1. Open Password Generator from the sidebar.
2. Choose a length — longer is stronger; 16 or more is a good rule.
3. Pick the character types: capitals, numbers and symbols.
4. Press Generate, watch the strength meter, then Copy.
5. Paste it into the site you are signing up to, then save it in your vault.

🔔 GOOD TO KNOW

- Aim for the green end of the strength meter.
- Never reuse a password — generate a fresh one for every account.

Secrets Manager

A dedicated place for the technical secrets: API keys, server credentials and access tokens. Keeping them here means they are encrypted, searchable and never sitting in plain text files or emails.

☰ HOW TO USE IT

1. Open Secrets Manager from the sidebar.
2. Press “Add secret” and give it a clear label, like “Stripe live key”.
3. Paste the key or token and save — it is encrypted immediately.
4. Use the copy button when you need it; your clipboard is wiped shortly after.

🔔 GOOD TO KNOW

- Label secrets with where they are used, so rotation day is painless.
- Old keys you have replaced are best deleted, not kept “just in case”.

2FA codes (TOTP)

Two-factor codes are the six-digit numbers that change every 30 seconds when you sign in to important accounts. Secret Digits can generate them for you, so your codes live beside your passwords — safely encrypted.

☰ HOW TO USE IT

1. When a site offers two-factor authentication, choose “text code / authenticator app”.

2. Copy the secret key (or the otpauth link) the site shows you.
3. In your vault, add a 2FA item and paste the secret.
4. Open the item any time to see the live six-digit code and type it into the site.

GOOD TO KNOW

- Codes refresh every 30 seconds — if one is about to expire, wait for the next.
- Keep the site's own backup codes too, in case you ever switch apps.

Shared Secrets

The headline feature of Secret Digits. Share a login — say your booking.com account — with someone like a personal assistant so they can sign in and do the task for you, without seeing your password. In Secret Digits they cannot view, edit, delete or re-share the saved login, and you can revoke access any time.

HOW TO USE IT

1. Open your Vault and find the login you want to share — for example your booking.com entry.
2. Press the Delegate button on that item.
3. Enter the person's email and choose the “Use” permission — they can log in as you, but the password is never shown to them.
4. Set the limits: how long the access lasts and how many times a day it can be used.
5. Press Create delegation. You get two things to send privately: an invite link and a one-time passcode.
6. The other person opens the link (registering free if they have no account) and accepts — the passcode fills in by itself. Leave “Hide password from helper” ticked (the default) so they can only sign in through the Secret Digits browser extension on a computer, which fills the password in without ever showing or copying it.
7. Need them to stop? Open Delegations and press Revoke — access ends instantly.

GOOD TO KNOW

- Once they are signed in to the website, what they can do there is up to that website — Secret Digits can't limit it. Only share with people you trust, and change the password after revoking if you have any doubt.
- If the website has its own “add a user” or team feature (for example the Booking.com Extranet), use that instead where possible — your password is never shared at all.
- The extension hides the password from normal view. Like LastPass and Dashlane, it cannot stop a technically skilled person from digging it out with browser developer tools.
- Send the invite link and the passcode through separate channels (for example email and a text message) for best safety.
- Set an expiry so access switches itself off when the job is done, and revoke any time — it takes effect immediately.

- Every launch is recorded: open Delegations and press “show history” to see who launched it, when, and on which browser/device. How long they stay signed in happens on the website itself, so it can't be tracked.

Shared with me

This is where logins other people share with you appear. If someone sends you a shared-secret invite link and you do not have an account yet, the link lets you register free of charge and start using the secret straight away, to carry out the task you were given.

HOW TO USE IT

1. Open the invite link you were sent.
2. If you do not have an account, choose “Create a free account” — it takes about a minute and no card is required.
3. Verify your email and sign in; you are brought straight back to where you need to be.
4. Open “Shared with me” from the sidebar — the shared item is waiting there.
5. Press Accept. If you opened the invite link, the passcode is already filled in; otherwise paste the one the owner sent you. If your vault is locked, type your master password in the box that appears and press Unlock and accept.
6. Press Launch. If the owner hid the password, press “Sign in with the Secret Digits extension”: the site opens and the username and password are filled in for you. First time only, press Download extension and follow the 5 install steps shown (computer only — on a phone you'll be told to use a computer). If the owner allowed copying, you get Copy username and Copy password buttons instead; paste the password only into the site's password box (it clears from your clipboard after 15 seconds).

GOOD TO KNOW

- Accounts created this way are on the free plan: it exists to carry out the sharer's instructions, and paid-plan features are not included.
- You use the login without ever seeing the password itself.
- One honest limit: the extension fills the password in on the website rather than showing it to you — but, as LastPass and Dashlane also warn, a technically skilled person (or anyone with control of that computer) could still dig the password out with browser developer tools once it has been filled in.
- When the task is done, the owner can revoke access and the item simply disappears.

Delegations

Delegations let a trusted person log in on your behalf, safely and for a limited time — for example letting a colleague access a service while you are away. Every use is recorded.

HOW TO USE IT

1. Open Delegations and press “New delegation”.
2. Enter the person's email and describe what the access is for.
3. Set limits: how long it lasts and how many times a day it can be used.
4. The person accepts the delegation and can then log in on your behalf within those limits.
5. Check the usage history any time, or revoke the delegation early.

GOOD TO KNOW

- Every use is logged with the time — nothing happens silently.
- Keep delegations short; you can always create a fresh one.

Security Insights

An AI-powered report on the health of your passwords. It flags weak, reused and old passwords so you know exactly what to fix first. The checking happens without exposing your secrets.

HOW TO USE IT

1. Open Security Insights from the sidebar.
2. Press “Run report” and wait a few seconds.
3. Read the findings: weak, reused and ageing passwords, worst first.
4. Open each flagged item in the vault and replace it with a generated password.

GOOD TO KNOW

- Run a report after adding lots of new items, and every month or so.
- Reused passwords are the most urgent — fix those first.

Dark Web Monitoring

Checks whether your email addresses or passwords have appeared in known data breaches. The checking is done on your own device — your passwords are never sent away to be compared.

HOW TO USE IT

1. Open Dark Web Monitoring from the sidebar.
2. Add the email addresses you want watched.
3. Run a check to see any breaches they appear in.
4. If something appears, change that password everywhere you used it — the generator helps.

GOOD TO KNOW

- A breach finding is not a disaster — it is a to-do list. Change the password and move on.

- Check again after big breach news stories.

Audit Log

A tamper-proof record of everything that happens in your vault: items added, changed, shared, viewed and deleted, with dates and times. It cannot be edited — even by you — so it is always the truth.

HOW TO USE IT

1. Open Audit Log from the sidebar.
2. Scroll the list or search for an event.
3. Use it to answer “did that change happen?” with certainty.

GOOD TO KNOW

- If something looks unfamiliar, change your master password and review your shares and delegations.

Control Tower

A one-screen overview of your security position: how many items you have, what needs attention, and the state of your shares, delegations and alerts.

HOW TO USE IT

1. Open Control Tower from the sidebar.
2. Scan the cards — anything needing attention is highlighted.
3. Click a card to jump to the relevant feature and act on it.

GOOD TO KNOW

- Make Control Tower your Monday-morning check: thirty seconds keeps things healthy.

Plans & Billing

Secret Digits has plans from free to Enterprise. Upgrading unlocks more capacity and features. Payments are handled securely through the billing page.

HOW TO USE IT

1. Open Pricing from the sidebar (or Plans & Billing).
2. Compare the plans and press “Choose plan” on the one you want.
3. If you are not signed in, you will be asked to sign in first — you are brought straight back afterwards.

4. Enter payment details on the secure checkout.
5. Manage or cancel your subscription any time from the same page.

GOOD TO KNOW

- You can move between plans as your needs change.
- Receipts and subscription status live on the billing page.

Settings

Your account's control panel: profile details, security options, passkeys and active sessions.

HOW TO USE IT

1. Open Settings from the sidebar.
2. Update your display name and profile details.
3. Manage passkeys and security options in the security section.
4. Review active sessions and sign out of anything you do not recognise.

GOOD TO KNOW

- Visit after getting a new phone or laptop to register its passkey.

FOR ADMINS & THE OWNER

Administration

The admin dashboard: the full user list with search, and the tools to look after accounts — including deleting an account (which archives it safely) or deleting all accounts at once.

HOW TO USE IT

1. Open Administration from the sidebar (admins and the owner only).
2. Use the search box to find a person by email or name.
3. Press Delete on a row to archive that account — a reason is always required.
4. Delete all archives every ordinary account at once (you and the owner are always skipped) and asks you to type a confirmation first.

GOOD TO KNOW

- Deleted accounts are not gone — they move to Archives and can be reinstated.
- You can never delete your own account from here.

Team & Access

Where the owner appoints super admins, sends invites and manages the access roster — who is allowed into the admin area at all.

HOW TO USE IT

1. Open Team & Access from the sidebar.
2. Send an invite by email, choosing the role the person should have.
3. Promote a trusted user to super admin (up to two).
4. Use the access roster to review and change who has access.

GOOD TO KNOW

- Keep admin numbers small — every extra admin is another door to guard.

Archives

The resting place for deleted accounts. Archived accounts stay here for 24 months, fully restorable. After 24 months they are permanently deleted automatically. Super admins can purge earlier, and “red cards” ban an email from ever registering again.

HOW TO USE IT

1. Open Archives from the sidebar (owner and super admins).
2. Search or filter the list of archived accounts.
3. Press Reinstate to bring an account back exactly as it was.
4. Press Purge to delete permanently — this frees the email so it can register again.
5. Use Red card to ban an email permanently; bans can be lifted later if needed.

GOOD TO KNOW

- Every archive, reinstatement, purge and red card is written to a history log that cannot be edited.
- The owner can also remove archive entries earlier than 24 months.

Version & Deployments

Release management for the app itself: a history of every version and deployment, automatic release of new versions, and manual tools for recording deployments and building releases.

HOW TO USE IT

1. Open Version & Deployments from the sidebar.

2. See the live version, the deployment history and the full release history.
3. Turn automatic mode on or off — when on, an hourly check publishes the next version once it is due and tested.
4. Use “Run automatic release now” to trigger the check immediately.
5. “Record deployment” and “Release builder” handle things manually whenever you prefer.

🔔 GOOD TO KNOW

- When a new version goes live, everyone sees a refresh prompt so they get the latest app.
- The release history is unchangeable — a complete record of what shipped and when.

Secret Digits is a trading name of **New Age Bridge Ltd**. Company Number: 16701376. Registered Office: 18 Elizabeth Fry Place, SE18 4LA. Our registered domain is **secretdigits.com**.

Secret Digits is a company registered under UK law. v0.13.3 · development