Credential Vault

for Confluence

User Guide

Published by CowboyMSP

https://cowboymsp.com
support@cowboymsp.com

Version 1.0 - May 2026

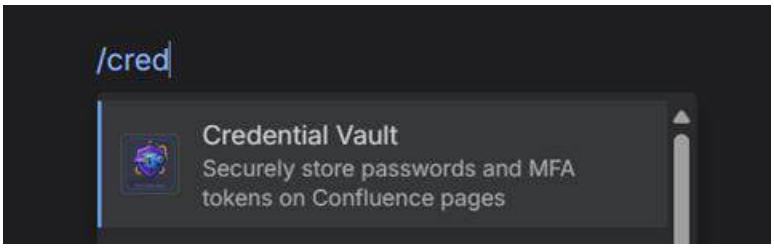
Table of contents

1 Getting started

1.1 Adding the vault to a Confluence page

1. Open any Confluence page and click Edit.
2. Type /Credential Vault in the editor body.
3. Select Credential Vault from the macro menu.
4. Click Save or Publish the page.

The vault macro can be added to any page. Each page has its own independent vault, with its own PIN, entries, templates, and settings.



1.2 Protecting the vault page

Anyone with edit access to the Confluence page can delete the page (and the vault macro along with it). Use one of the following Confluence-native protections:

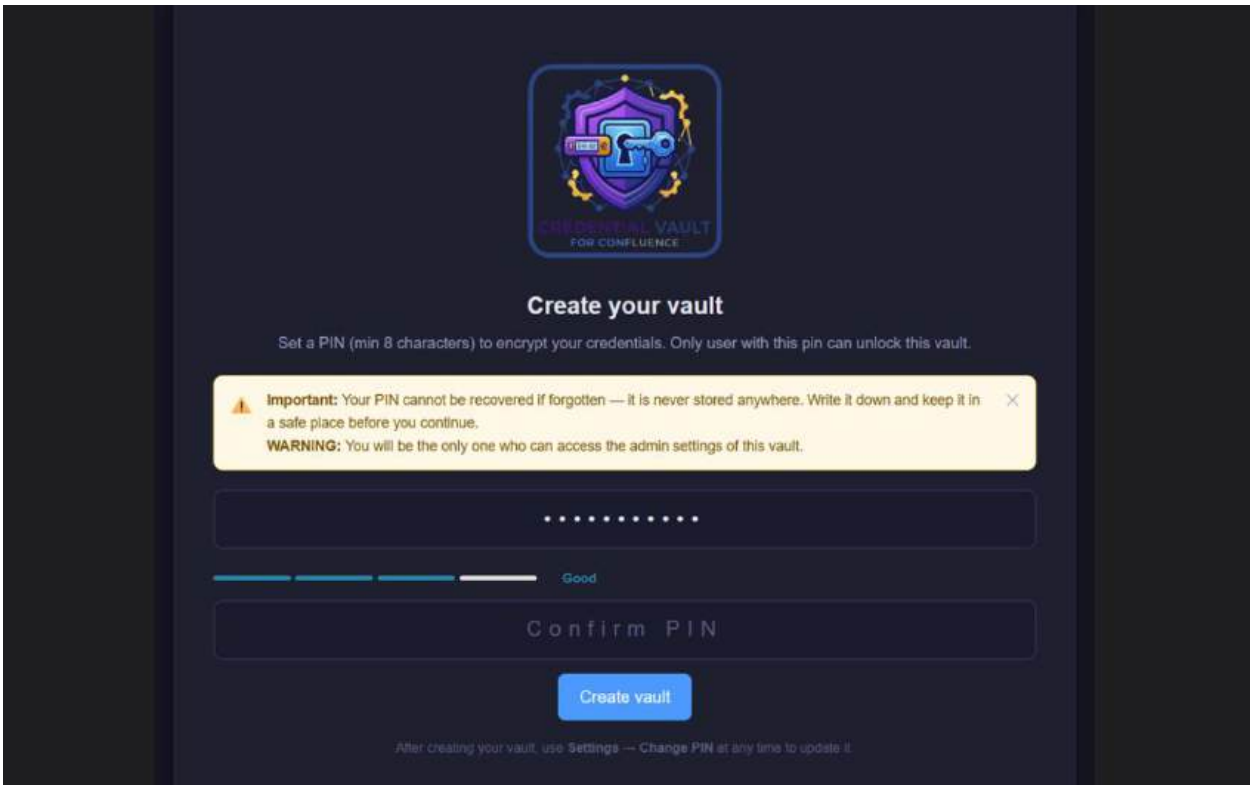
- Page Restrictions (simplest): on the page, click the lock icon (or the more-actions menu, then Restrictions). Set view and edit so only specific users or groups can change the page. Admins keep full access.
- Space Permissions: in Space Settings, then Permissions, remove the "Delete Pages" permission from all users except admins and space admins. This protects every page in the space.

1.3 Creating your PIN

The first time the vault macro is opened on a new page, you are prompted to create a PIN.

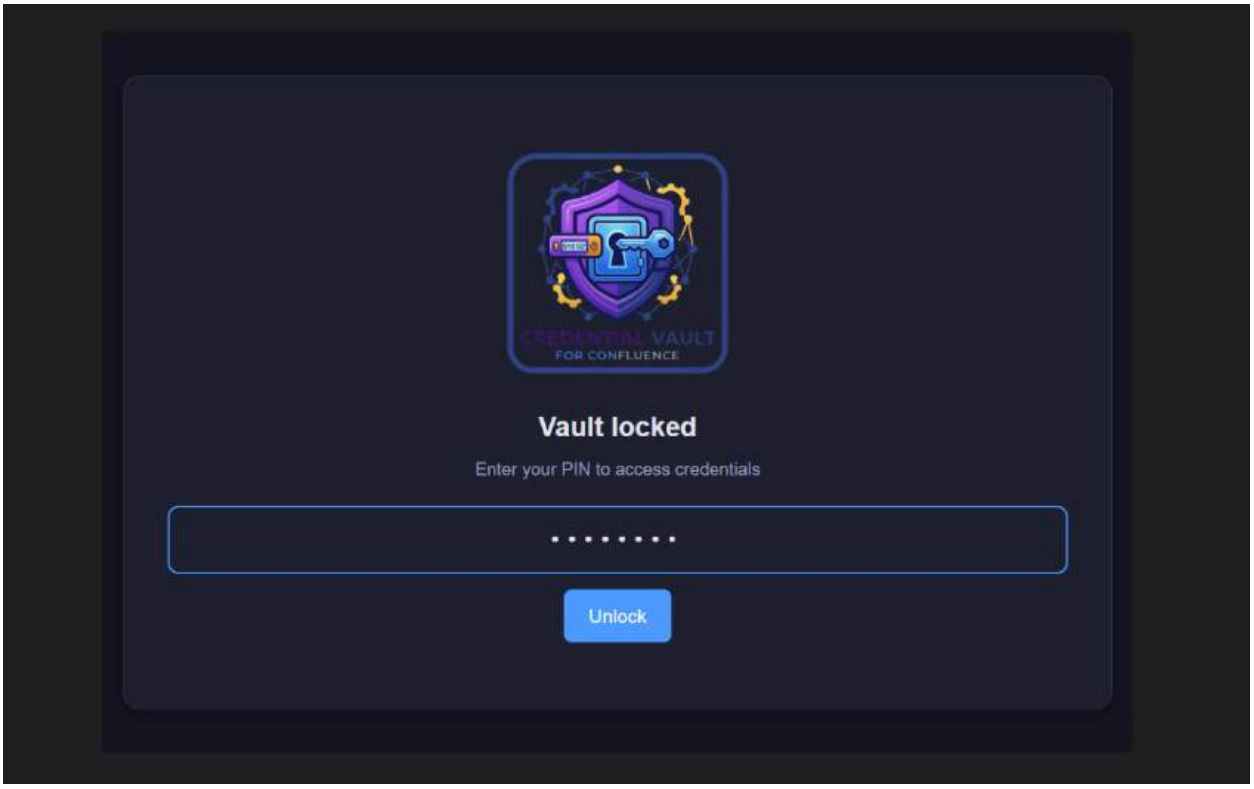
- Minimum 8 characters for new vaults (longer is stronger).
- Pins can Have Upper & Lower Case Letters, Numbers and Symbols
- A live strength meter (Weak / Fair / Good / Strong) is shown as you type.
- Your PIN is used to derive your encryption key. It is never stored anywhere - only a salted SHA-256 hash is kept for verification.
- Write your PIN down before you continue. If you forget it, your credentials cannot be recovered. See Section 19 - Recovery.

Enter your PIN, confirm it, and click Create vault. The user who creates the vault becomes the vault owner (see Section 3 - Vault ownership and roles).



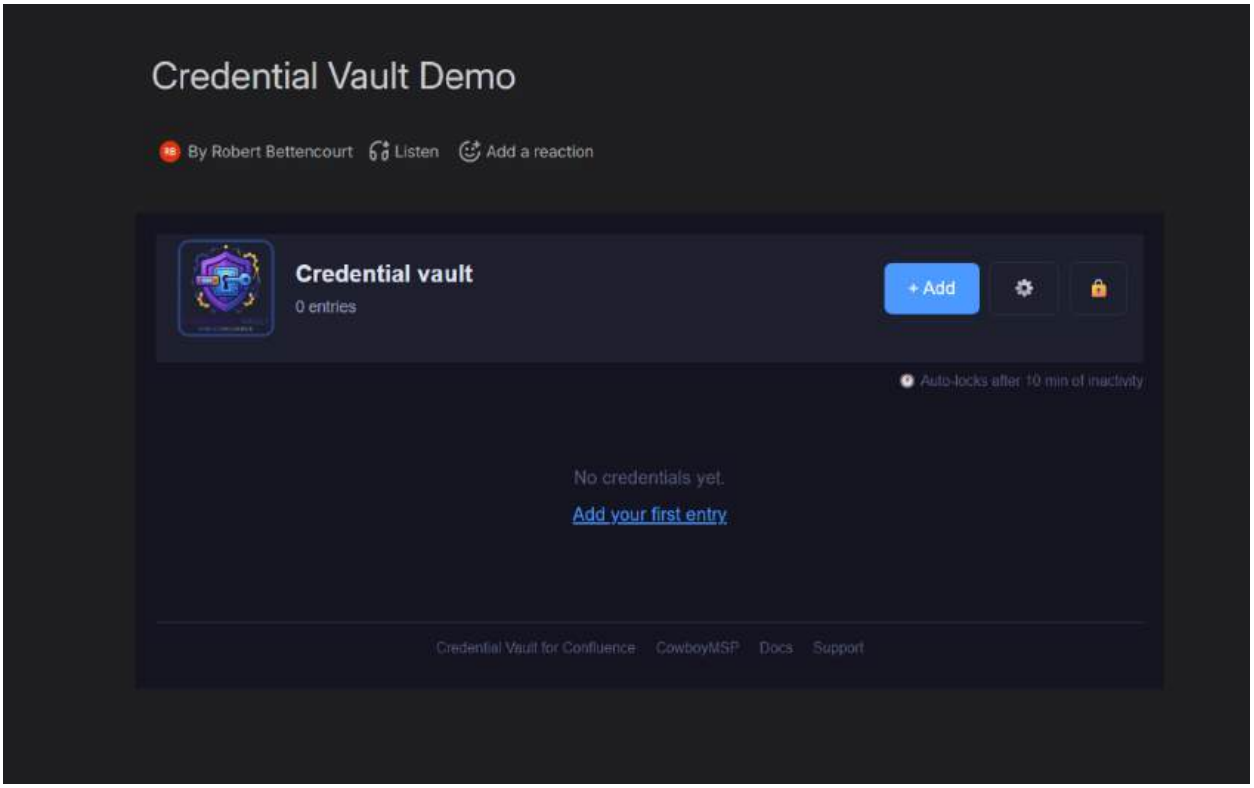
1.4 Unlocking Vault your PIN

Enter Pin to Unlock Vault



2 The vault interface

After unlocking, you see the main vault screen. The header always contains four controls; below the header are the search bar, sort dropdown, category filter pills, and the list of credential entries.



2.1 Header controls

Button	Action
+ Add	Open the templates picker, then the new credential form. Disabled at the free-tier limit.
Archive (count)	Open the Archive screen. Only shown when at least one entry is archived.
Settings (gear)	Open the Settings panel - Change PIN, Activity log, Auto-lock, Archive retention, Theme, Password Generator, Categories, Templates, Import / Export, Transfer ownership.
Lock	Lock the vault immediately. All decrypted data is cleared from memory.

2.2 Auto-lock notice strip

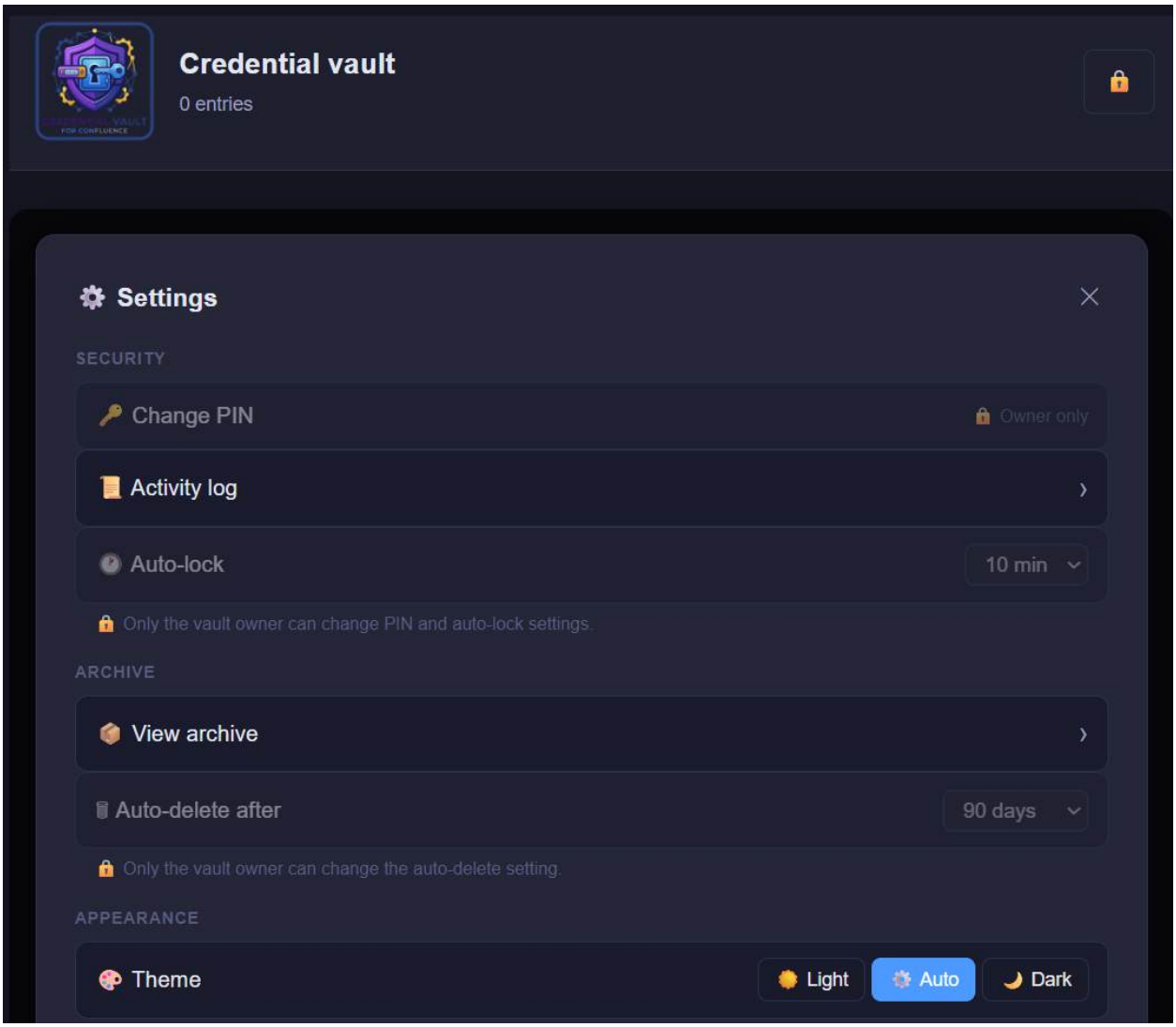
Beneath the header is a small notice showing how long until the vault auto-locks after no user activity. The auto-lock window is configurable in Settings (owner only).

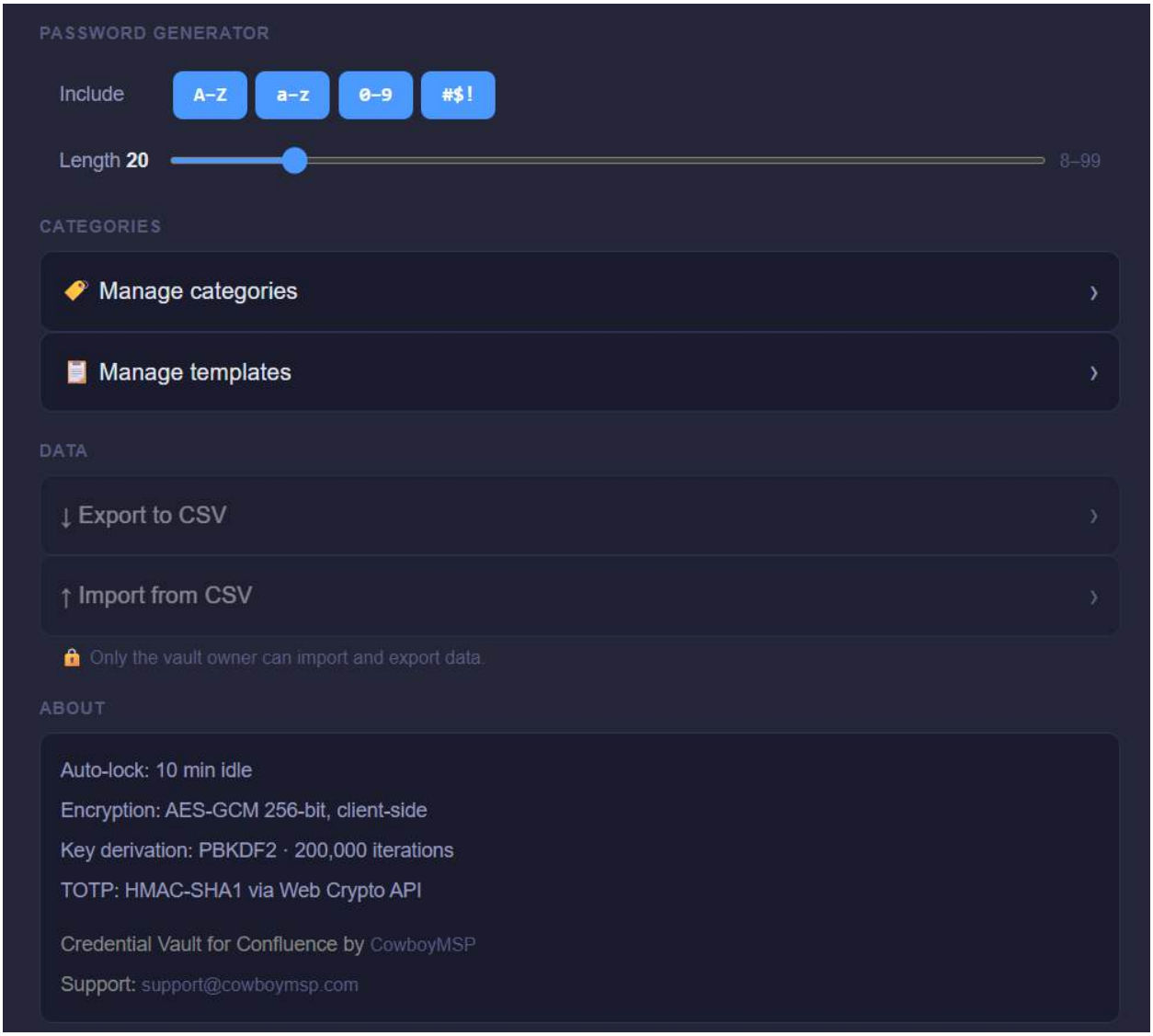
3 Vault ownership and roles

Each vault has one owner, set automatically to the Atlassian account of the user who first creates the vault. Everyone else with page access is a regular user.

Action	Owner	Regular user
Unlock with PIN	Yes	Yes
View, copy, reveal entries	Yes	Yes
Add, edit, archive entries	Yes	Yes
Restore archived entries	Yes	Yes
Permanently delete entries	Yes	No (must archive)
Change PIN	Yes	No
Change auto-lock timeout	Yes	No
Change archive auto-delete window	Yes	No
Import from CSV	Yes	No
Export to CSV	Yes	No
Manage shared templates	Yes	No
Transfer vault ownership	Yes	No
Manage personal "My view" templates	Yes	Yes
Manage personal theme and generator preferences	Yes	Yes

Owner-only actions still appear in Settings for regular users but are disabled (greyed out) with a small "Owner only" badge next to them.


Credential vault
0 entries
Settings
SECURITY
Change PIN
Owner only
Activity log
Auto-lock
10 min
Only the vault owner can change PIN and auto-lock settings.
ARCHIVE
View archive
Auto-delete after
90 days
Only the vault owner can change the auto-delete setting.
APPEARANCE
Theme
Light
Auto
Dark



4 Adding credentials

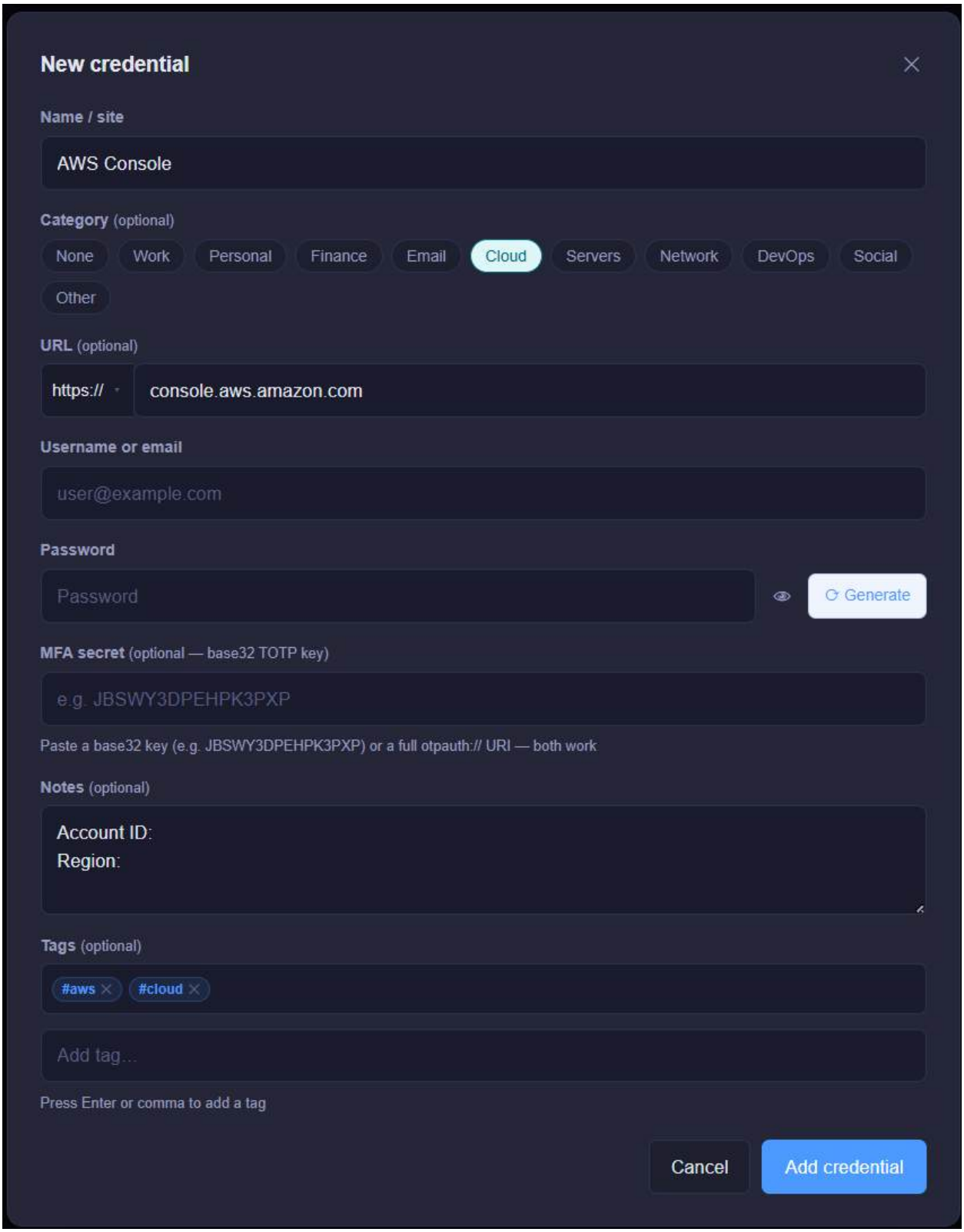
Click + Add in the header. You are first shown the templates picker - choose a template to pre-fill common fields, or click Blank to start empty. See Section 5 for details on templates.

4.1 Credential fields

Field	Description
Name / site	Required. Label for this entry (for example "GitHub" or "AWS Console - Prod").
Category	Optional. Tag the entry as Work, Personal, Finance, Email, Cloud, Servers, Network, DevOps, Social, Other, or any custom category the owner has added.

Field	Description
URL	Optional. The protocol picker on the left offers https, http, rdp, ssh, vnc, sftp, ftp, ftps, smb, ldap, ldaps, mysql, mssql, postgresql, mongodb, redis, telnet, smtp, smtps, imap, imaps. Dangerous schemes (javascript, data, vbscript, file) are blocked.
Username or email	Required. The login username or email.
Password	Required. Use Generate for a strong random value, or type your own.
MFA secret	Optional. The base32 TOTP key, or a full otpauth:// URI. See Section 4.4.
Tags	Optional. Type a tag and press Enter or comma. Tags are lower-cased and spaces become hyphens. Searchable and filterable.
Notes	Optional. Multi-line. Use for recovery codes, account numbers, hints.

Click Save to encrypt and store the entry. A small "Saving" indicator appears briefly while the encrypted blob is written to Forge KV storage.



4.2 Password generator

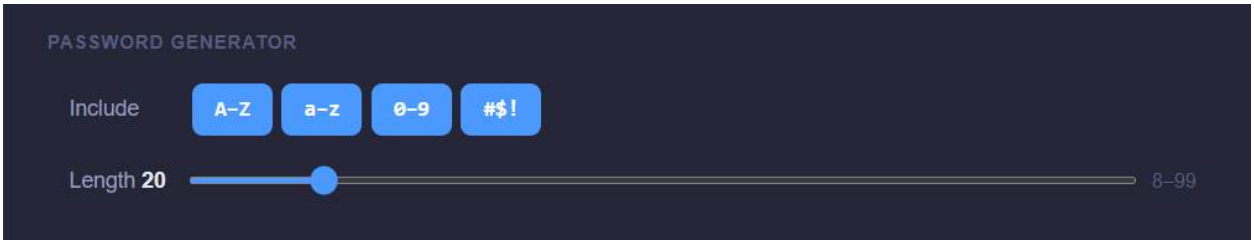
Click Generate next to the password field to create a strong random password. The generator uses the browser's cryptographic random number generator.

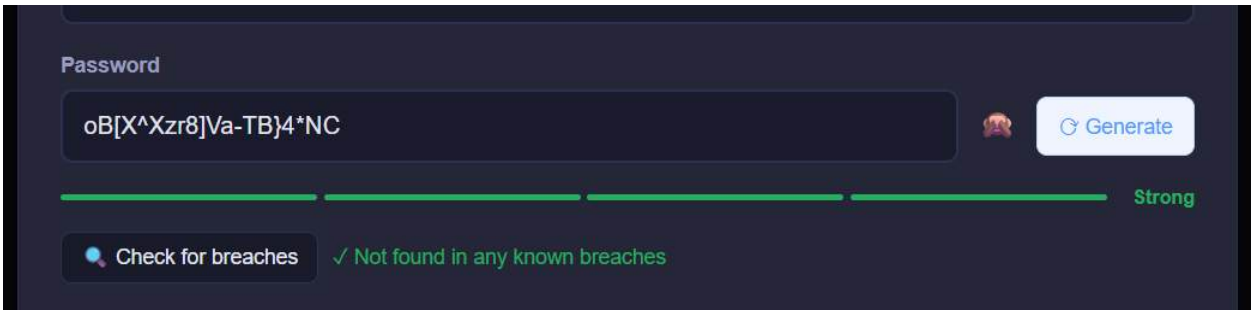
Generator preferences are configurable under Settings > Password Generator:

- Include toggles for uppercase (A-Z), lowercase (a-z), digits (0-9), and symbols (#$!).
- Length slider from 8 to 99 characters (default 20).
- At least one character class must remain enabled.

The generated password is automatically revealed in the field so you can see and copy it before saving.

Settings per User





4.3 Strength meter and breach check

As you type or generate a password, four coloured segments and a label appear: Weak (red), Fair (amber), Good (blue), or Strong (green).

Click Check for breaches below the password field to verify whether the password appears in a known data breach. The check uses k-anonymity: only the first 5 characters of a SHA-1 hash of your password are sent to the Have I Been Pwned API. Your actual password and the full hash never leave your browser. The check is optional and does not block saving.

4.4 Setting up MFA codes

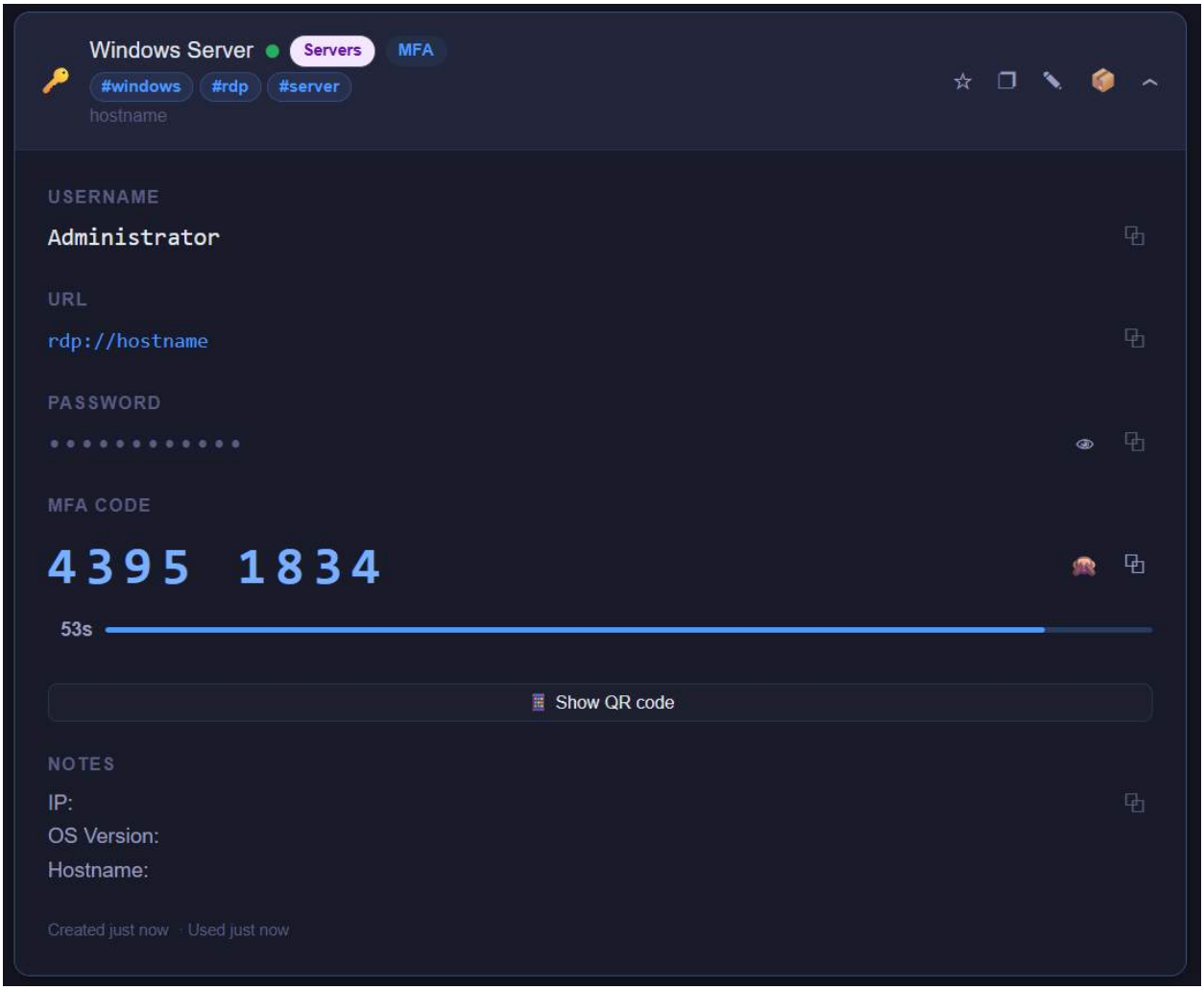
If the account uses two-factor authentication (2FA), you can store the TOTP secret so the vault generates live codes automatically - no separate authenticator app needed.

When enabling 2FA on any website, you are normally shown a QR code to scan. Look for a link near the QR code that says one of:

- "Can't scan the QR code?"

- "Enter setup key manually"
- "Show secret key"

That text string (example: JBSWY3DPEHPK3PXP) is your base32 TOTP secret. Paste it into the MFA secret field. You can also paste a full otpauth:// URI - the vault parses digits, period, and algorithm from it automatically.



4.5 Duplicate and password-reuse warnings

When saving a new entry, the vault checks for two things and shows a non-blocking warning if they match:

- Duplicate name - another entry uses the same Name.
- Duplicate URL - another entry uses the same URL.

You can tick "Don't warn me again on this device" on the duplicate warning to suppress it in future.

Separately, if the password is already used by another entry in the same vault, a "Password reused" notice is shown naming the conflicting entry. You can save anyway - it is informational.

5 Templates

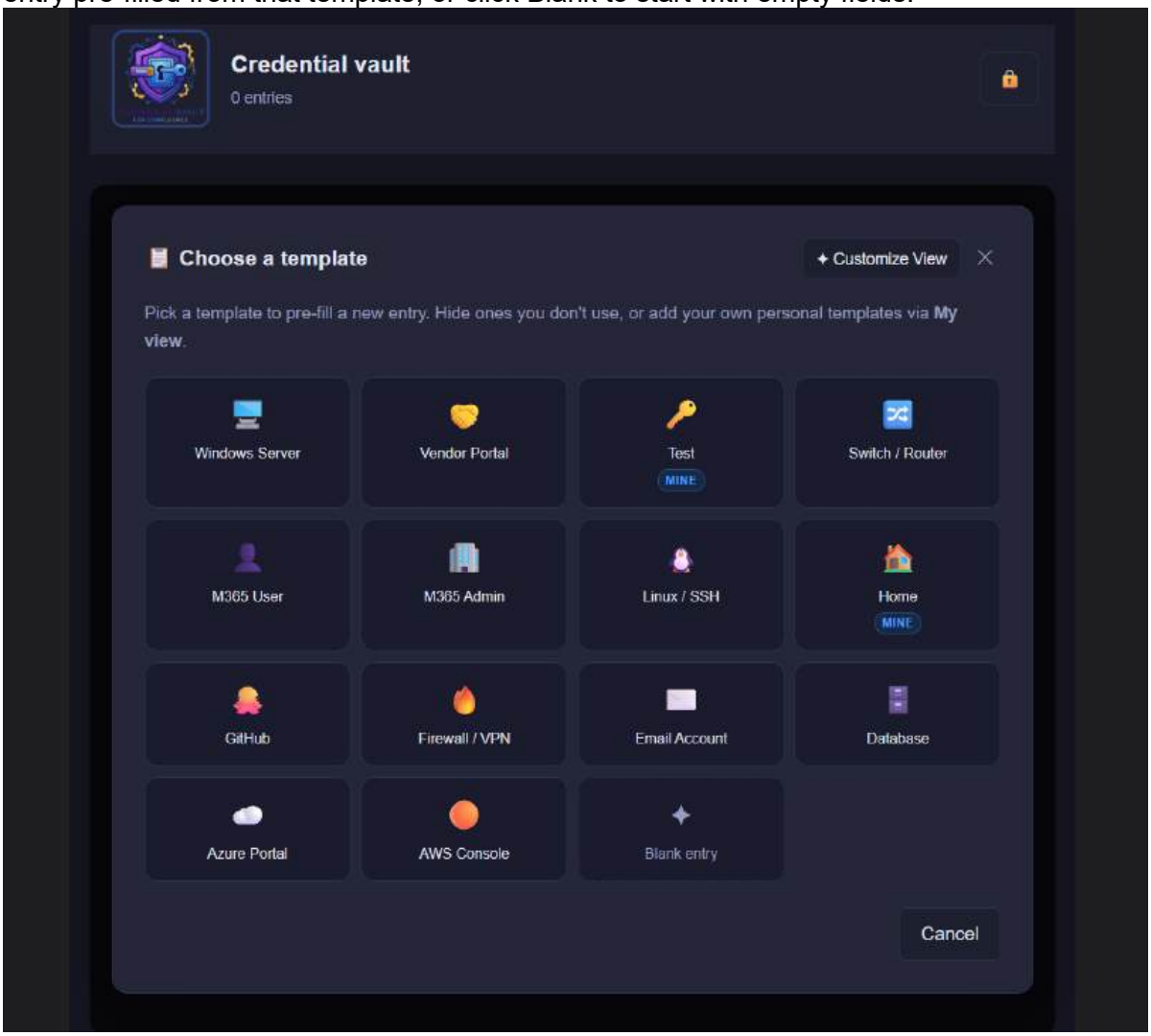
Templates let you pre-fill the new-entry form with sensible defaults for common credential types - MSP-focused presets such as M365 Admin, AWS Console, Windows Server (RDP), Linux / SSH, Firewall / VPN, Switch / Router, Database, GitHub, and more.

5.1 Three kinds of template

Type	Scope	Who can manage
Built-in	Same in every vault	Cannot be edited; each user can hide them from their own grid.
Admin (shared)	Stored server-side per vault, shared with everyone on the page	Vault owner only.
Personal (My view)	Stored in this browser's local storage, visible only to you	Anyone.

5.2 Choosing a template

Clicking + Add in the header opens the Choose a template modal. Click any tile to start a new entry pre-filled from that template, or click Blank to start with empty fields.



5.3 Managing shared templates (owner only)

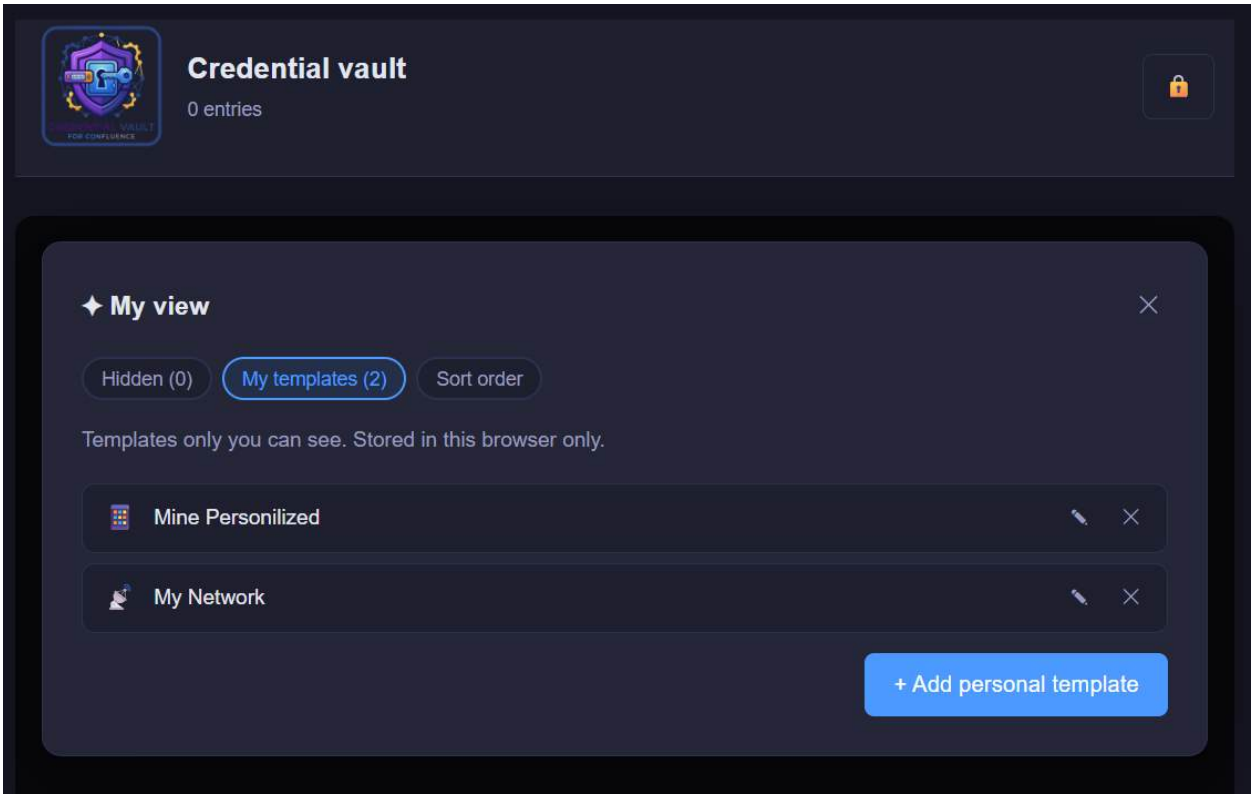
Open Settings > Manage templates to add, edit, rename, or remove templates that everyone using the vault will see. You can choose an icon for each template from the built-in icon picker (30+ options). Built-in templates can be reset back to defaults from this screen.

5.4 My view - personal templates and hidden tiles

From the Choose a template modal, click My view (top-right) to open your personal customisation screen. Three tabs:

- Hidden - tick built-in templates you want hidden from your personal grid.
- My templates - create, edit, or delete templates only you see.
- Sort order - choose how templates are ordered: A to Z, Z to A, Team first, or Mine first.

Hidden templates and personal templates are stored in your browser's local storage - they follow your browser, not your Atlassian account.



6 Viewing and using credentials

Click any entry row to expand it. Opening an entry records a "last used" timestamp shown at the bottom of the expanded card.

6.1 Copying fields

Every field has a small copy button on the right. Clicking it copies the value to your clipboard silently - no reveal required. A toast confirms what was copied.

Field	Behaviour
Username	Always visible; copy button on right.
URL	Shown as a clickable link; copy button on right.
Password	Hidden by default. Click the eye to reveal, or copy without revealing.
MFA code	Hidden by default (rendered as bullets). Click the eye to reveal, or copy without revealing the digits.
Notes	Shown; copy button on right.
Tags	Shown as chips inside the expanded card.

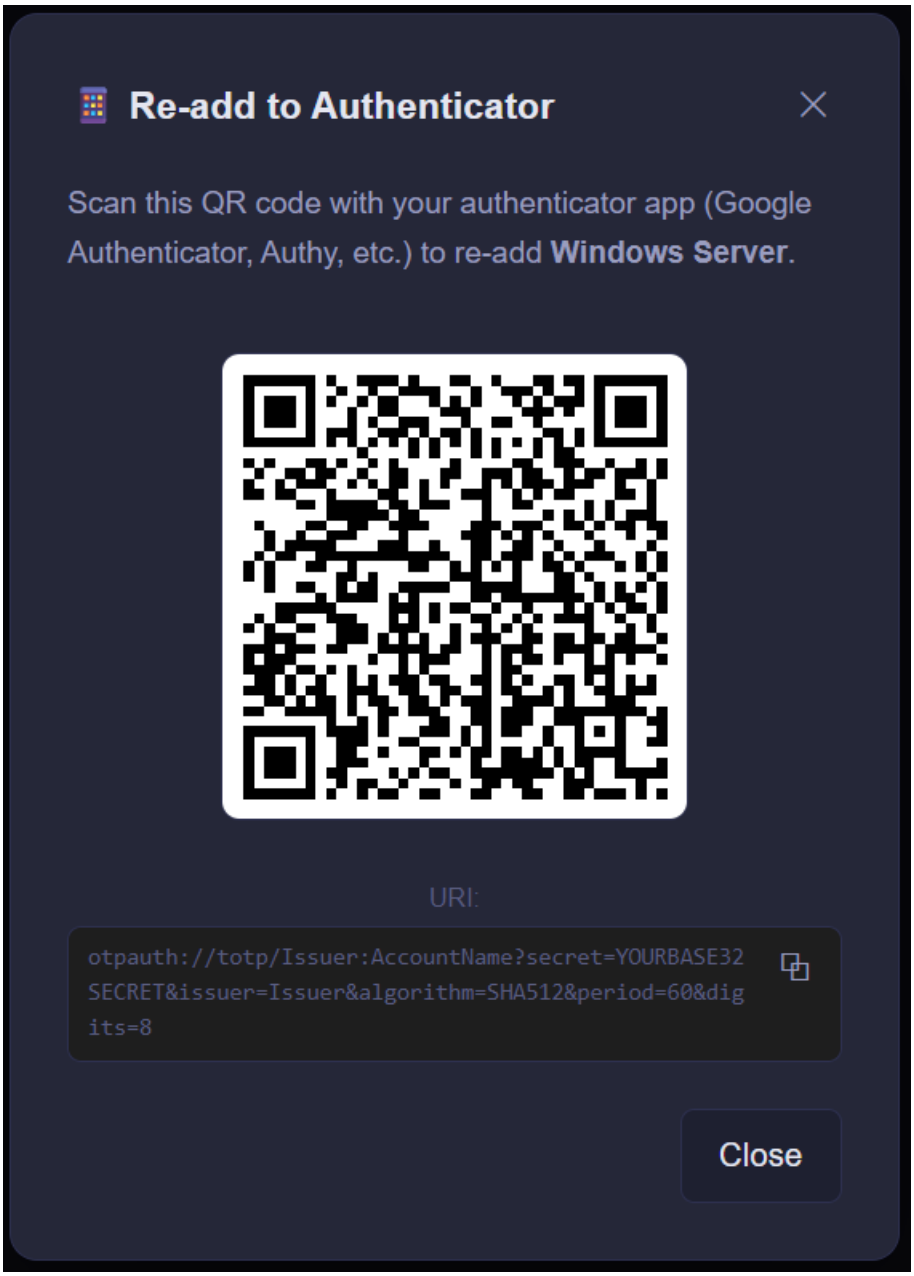
The recommended workflow is to always use the copy button - you rarely need to reveal the password or MFA code at all.

6.2 MFA countdown timer

When an MFA secret is stored, a live 6-digit code is displayed with a countdown showing seconds remaining in the current 30-second window, a progress bar that turns amber at 10 seconds and red at 5 seconds, and automatic refresh every 30 seconds.

6.3 Re-add to authenticator (QR code)

Click the QR-code button inside an expanded entry to open a printable QR code suitable for scanning into any standard authenticator app (Google Authenticator, Authy, Microsoft Authenticator, 1Password, Bitwarden, etc.). The raw secret or otpauth:// URI is also shown below the QR code for manual entry.



7 Tags

Tags are freeform labels you attach to any entry to make it easier to find. Unlike Categories, which come from a fixed list managed by the owner, tags are typed by the user.

Adding tags: in the entry form, type a tag in the Tags input and press Enter or comma. Tags are automatically lower-cased and spaces become hyphens (so "Prod Server" becomes "prod-server"). Each tag is shown as a chip you can remove with the small x.

Searching tags: tags are searchable. Typing in the main search bar matches against entry name, username, URL, category, notes, and any tag.

8 Categories

Entries can be tagged with a category to help organise your vault as it grows.

Default categories: Work, Personal, Finance, Email, Cloud, Servers, Network, DevOps, Social, Other.

8.1 Assigning a category

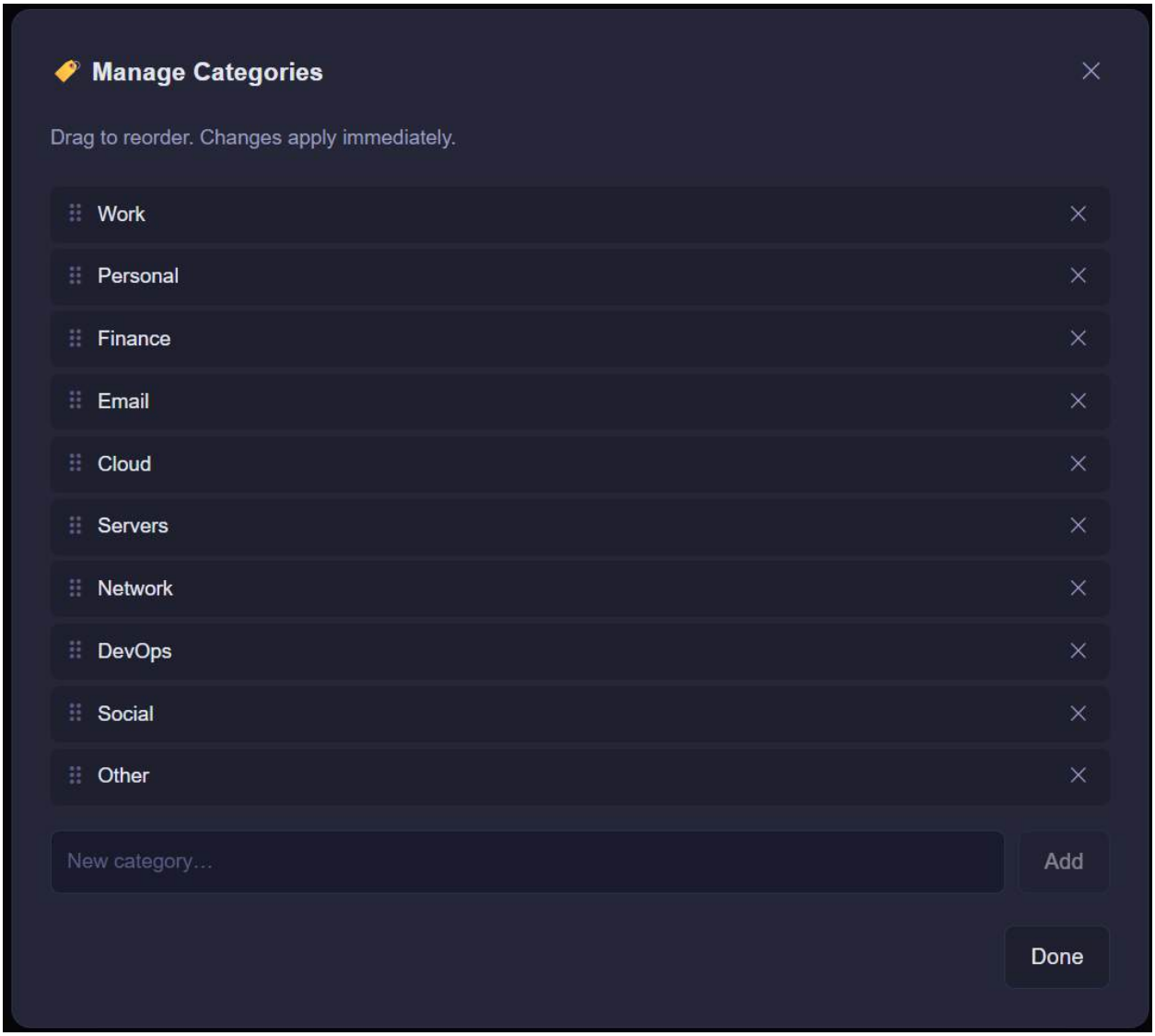
When adding or editing an entry, choose a category from the dropdown, or pick "None" to leave the entry uncategorised.

8.2 Filtering by category

When the vault has entries with categories assigned, a row of category pills appears below the search bar. Click a category to show only matching entries. Click All to return to the full list. The active filter is highlighted with the category's colour.

8.3 Managing categories (owner only)

Open Settings > Manage categories to add or remove categories, and drag-and-drop to reorder them. Changes apply immediately.



9 Search, sort, and filter

9.1 Multi-tag search

- Type any text and press Enter to convert it into a search chip. This allows multiple search terms (AND logic). The list narrows further with each chip.
- Backspace in an empty search input removes the last chip.
- Click the x on a chip to remove it; click the main x to clear everything.

Searches match against entry name, username, URL, category, notes, and tags.

9.2 Sort options

Option	Description
A to Z	Alphabetical by name (default).

Option	Description
Z to A	Reverse alphabetical.
Category	Grouped by category in the category-list order.
Newest first	Most recently created entries at top.
Oldest first	Original creation order.
Recently used	Entries you opened most recently appear first.

Pinned entries always appear at the top of the list within their sort order.

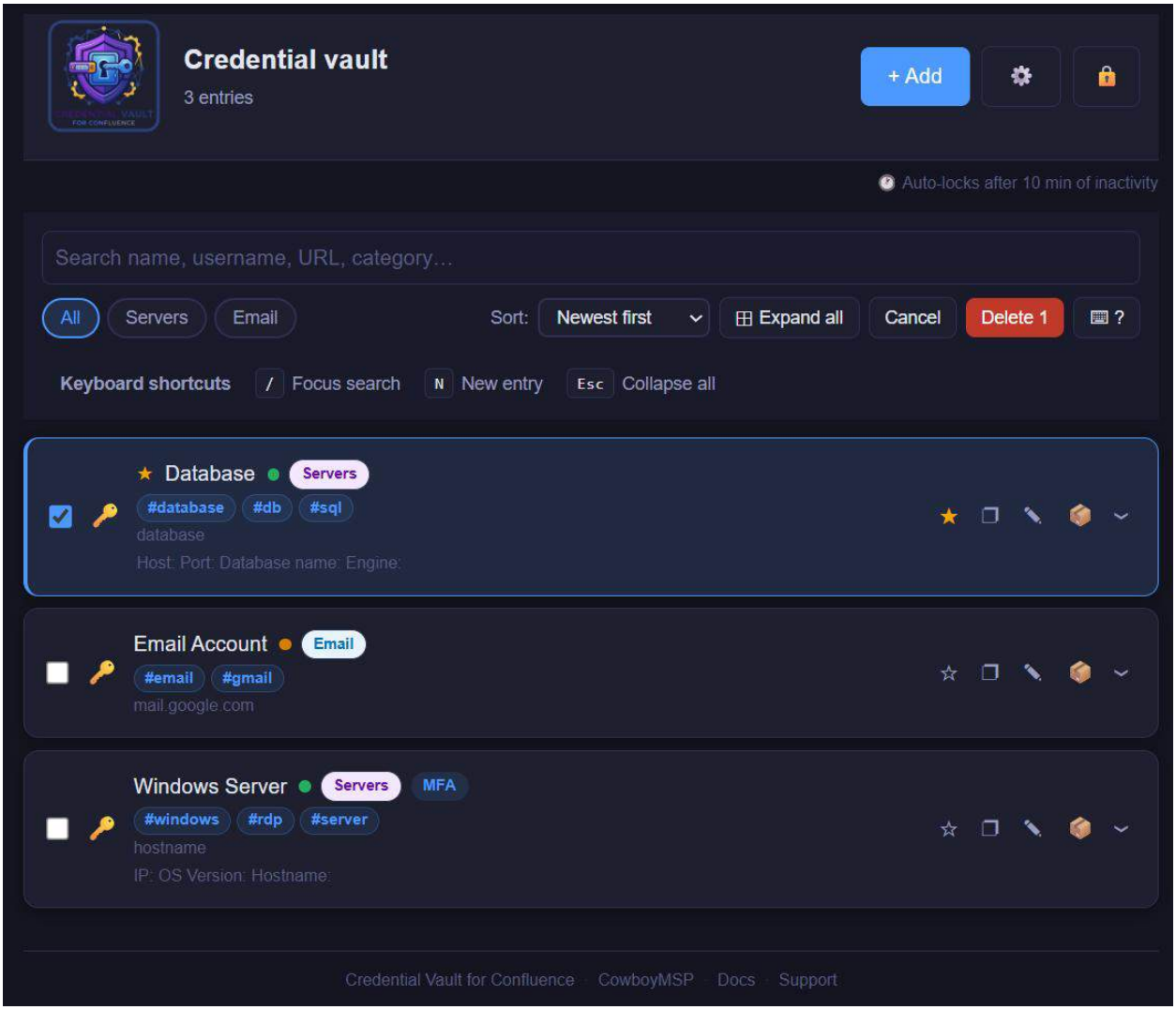
9.3 Combining filters

Search chips, category filter, and sort all work together - only entries matching all active filters are shown, then sorted.

10 Pinning, duplicating, editing, and archiving

Each entry header (collapsed or expanded) shows these icon buttons on the right:

Button	Action
Star	Pin to top. Pinned entries always appear at the top regardless of sort. Click again to unpin.
Duplicate	Open a pre-filled copy of the entry. The name is prefixed with "(copy)".
Pencil (Edit)	Open the edit form. All fields can be changed. The Modified timestamp updates on save.
Archive	Soft-delete the entry to the Archive. See Section 12.
Expand / Collapse	Toggle this entry's expanded view.



10.1 Timestamps

Each entry tracks four timestamps shown at the bottom of the expanded card:

Timestamp	When it updates
Created	When the entry was first saved.
Modified	When the entry was last edited and saved.
Password changed	When the password value was last changed (separate from edits to other fields).
Last used	When the entry was last expanded (opened) in the vault.

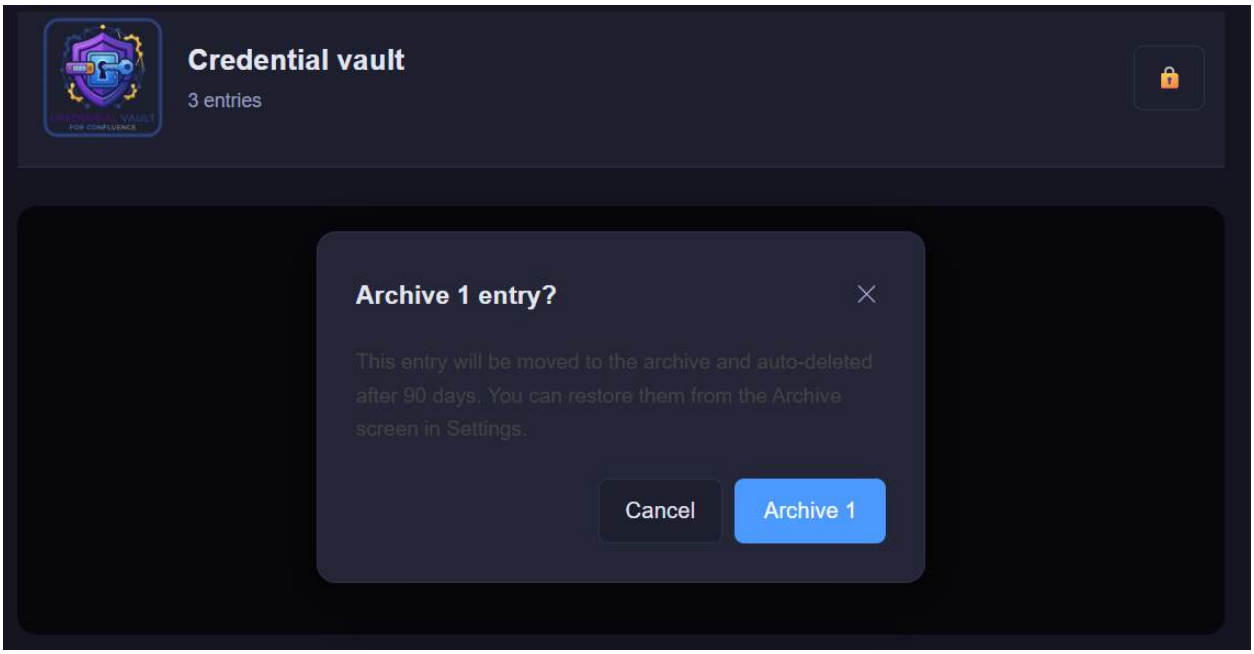
Hover any timestamp for the full date and time. Timestamps are included in CSV exports.

11 Bulk actions

Click Select in the toolbar to enter selection mode. A checkbox appears on every entry; tick the ones you want to act on.

- The toolbar shows Delete N (which archives the selected entries in bulk).
- Click Cancel to leave selection mode without changes.

Bulk delete moves the entries to the Archive, where they can be restored before being auto-purged. Only the vault owner can permanently delete from the Archive.

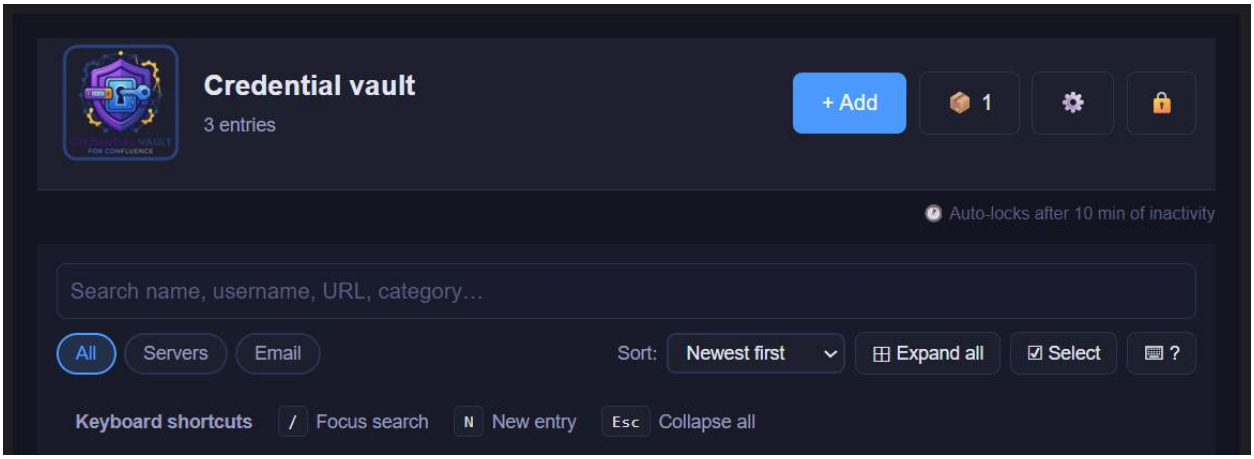


12 Archive (soft delete)

Clicking the archive icon on an entry soft-deletes it - the entry is hidden from the main list but still encrypted and stored. You can restore it before it is auto-purged.

12.1 Opening the archive

When at least one entry is archived, an Archive button appears in the header showing the count. You can also reach it from Settings > View archive.



12.2 Restoring an archived entry

Click Restore on any archived entry. The entry returns to the main list with its Modified timestamp updated. If the name already exists on another live entry, "(restored)" is appended automatically.

12.3 Permanent deletion (owner only)

Inside the Archive, the owner sees a small red x next to each entry. Clicking it permanently deletes the entry after a confirmation prompt. Regular users cannot hard-delete; the button is hidden for them.

12.4 Auto-delete after N days (owner only)

In Settings > Auto-delete after, the owner picks a retention window: Never, 7, 14, 30, 60, 90 (default), 180, or 365 days. When an entry's archivedAt timestamp is older than this window, it is permanently and silently deleted the next time the vault is unlocked.

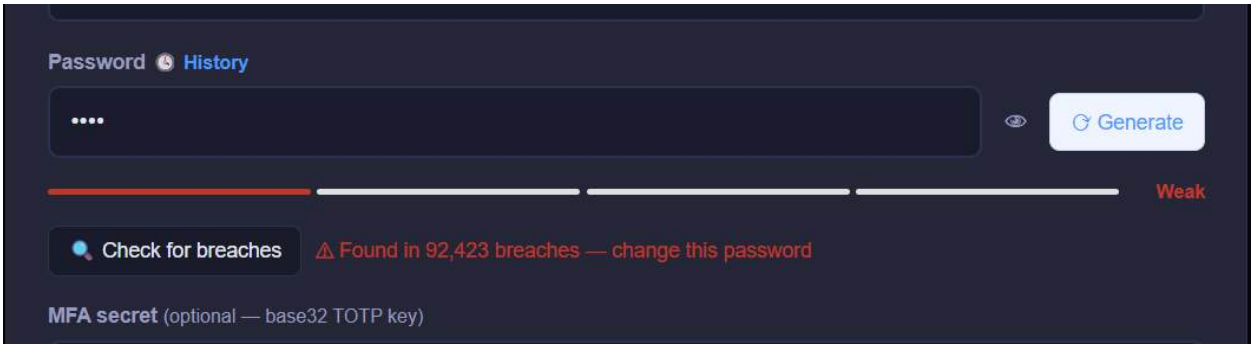
When you archive an entry while auto-delete is enabled, a one-time notice reminds you of the retention window. Tick "Don't warn me again on this device" to suppress that notice in future.

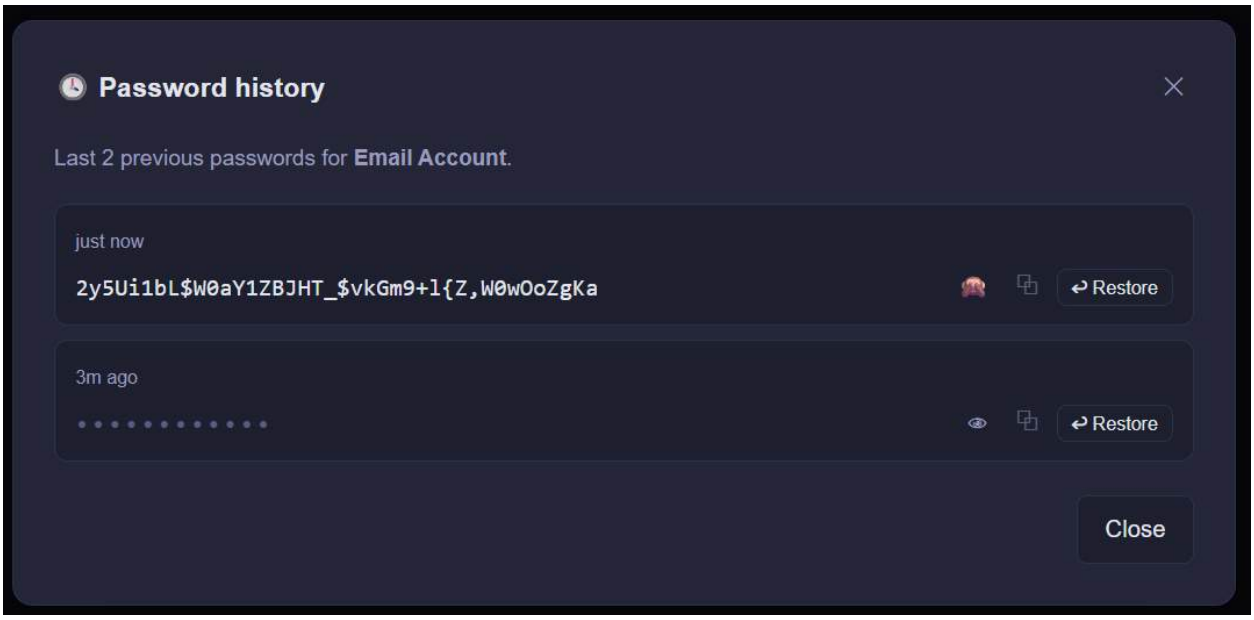
13 Password history

Whenever you change an entry's password, the previous password is added to that entry's password history. Up to the last 5 previous passwords are kept per entry, along with the date each was changed.

13.1 Viewing history

Inside an expanded entry, click the clock icon next to the password field to open the Password history modal. Each row shows when the password was changed, the masked password with a reveal toggle and copy button, and a Restore button.





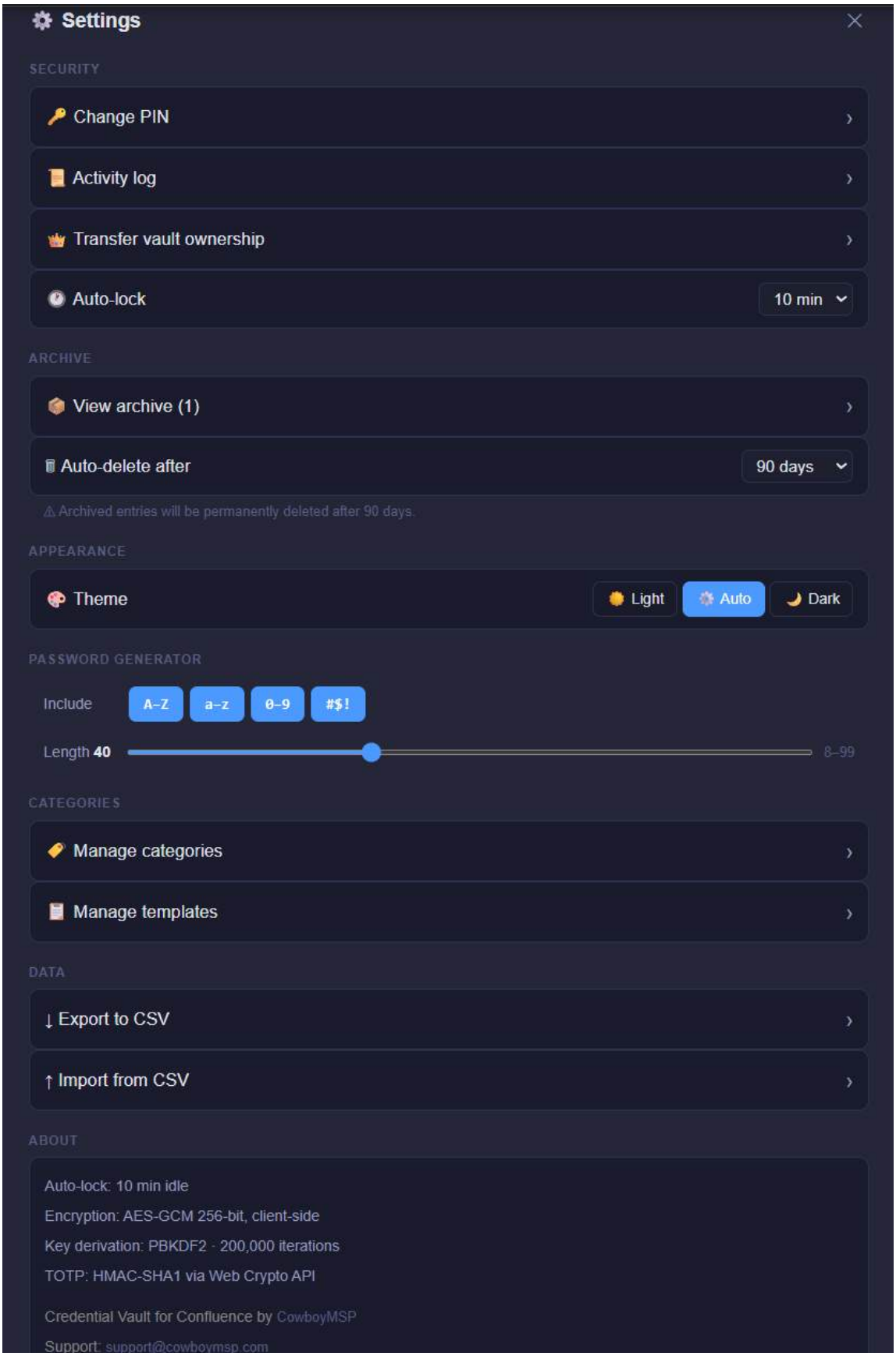
13.2 Restoring a previous password

Clicking Restore on a history row sets that old value back as the live password. The current password is pushed into history (so you can undo the restore). If the restored password was already in history, it is removed from the list (since it is now active again).

14 Settings

Click the gear icon in the header to open the Settings panel. Sections in order:

Section	Contents
Security	Change PIN (owner), Activity log, Transfer vault ownership (owner), Auto-lock timeout (owner).
Archive	View archive (with count), Auto-delete after N days (owner).
Appearance	Theme - Light, Auto, Dark.
Password Generator	Toggle character sets (A-Z, a-z, 0-9, #$!), Length 8 to 99.
Categories	Manage categories (owner), Manage templates (owner).
Data	Export to CSV (owner), Import from CSV (owner).
About	Current auto-lock, encryption details, support links.

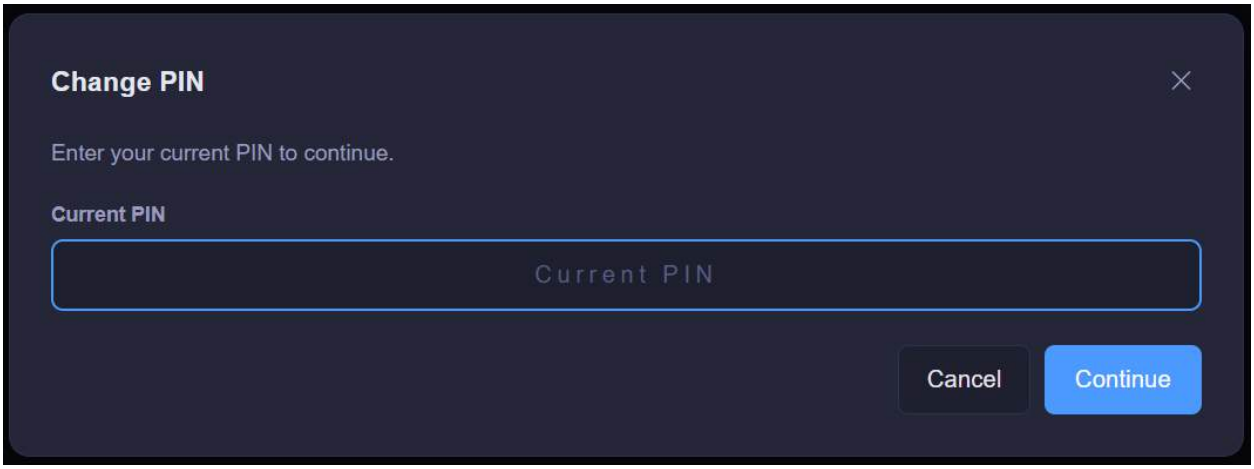

Settings
SECURITY
Change PIN
Activity log
Transfer vault ownership
Auto-lock
10 min
ARCHIVE
View archive (1)
Auto-delete after
90 days
⚠ Archived entries will be permanently deleted after 90 days.
APPEARANCE
Theme
Light
Auto
Dark
PASSWORD GENERATOR
Include
A–Z
a–z
0–9
#$!
Length 40
8–99
CATEGORIES
Manage categories
Manage templates
DATA
↓ Export to CSV
↑ Import from CSV
ABOUT
Auto-lock: 10 min idle
Encryption: AES-GCM 256-bit, client-side
Key derivation: PBKDF2 · 200,000 iterations
TOTP: HMAC-SHA1 via Web Crypto API
Credential Vault for Confluence by CowboyMSP
Support: support@cowboymsp.com

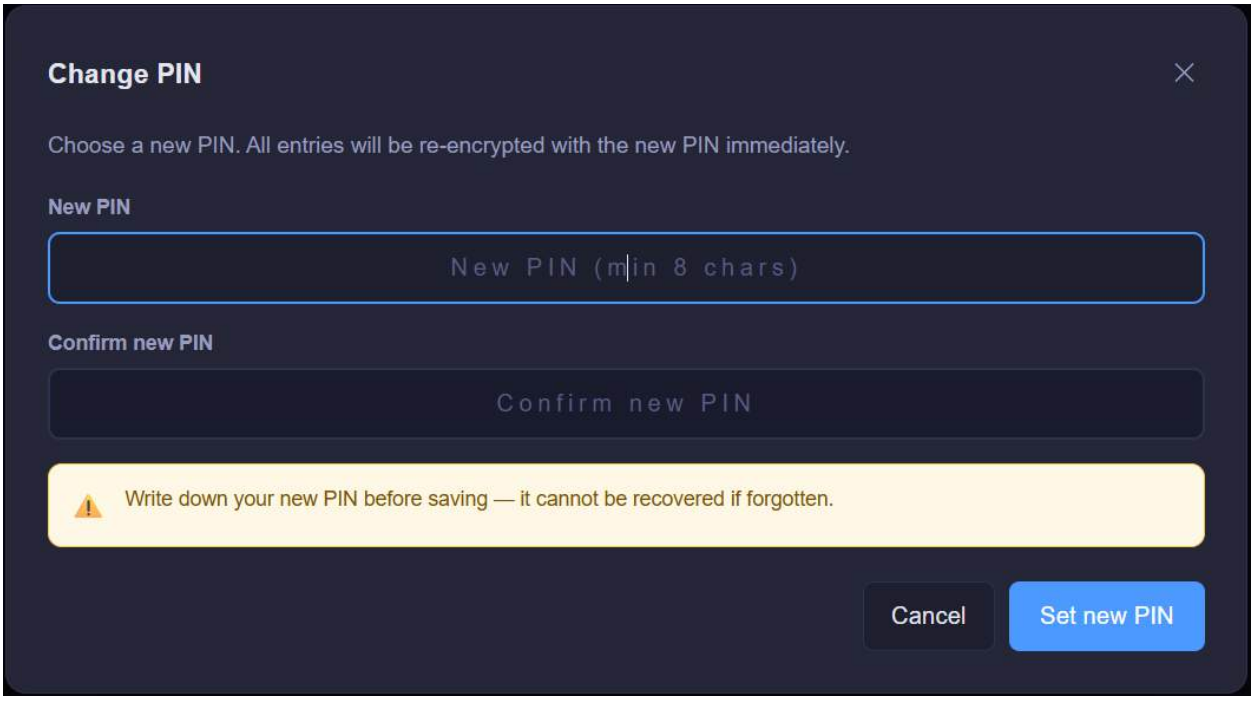
14.1 Change PIN (owner only)

5. Open Settings > Change PIN.
6. Enter your current PIN to verify.
7. Enter and confirm your new PIN (minimum 8 characters; strength meter is shown).
8. Click Set new PIN.

All entries are immediately re-encrypted with the new PIN and a fresh per-vault salt. The old PIN no longer works. You receive a "PIN changed successfully" toast when complete.

Important: write down your new PIN before saving. Like the original, it cannot be recovered if forgotten.





14.2 Auto-lock timeout (owner only)

Choose how many minutes of inactivity before the vault locks. Options: 1, 3, 5, 10 (default), 15, 30, 60 minutes. The vault shows a 60-second countdown banner before locking (20 seconds for the 1-minute setting), so you can stay unlocked with one click on Stay unlocked.

14.3 Theme

Choose Light, Auto (follows your OS preference), or Dark. The setting is stored per browser, per user.

14.4 Password generator preferences

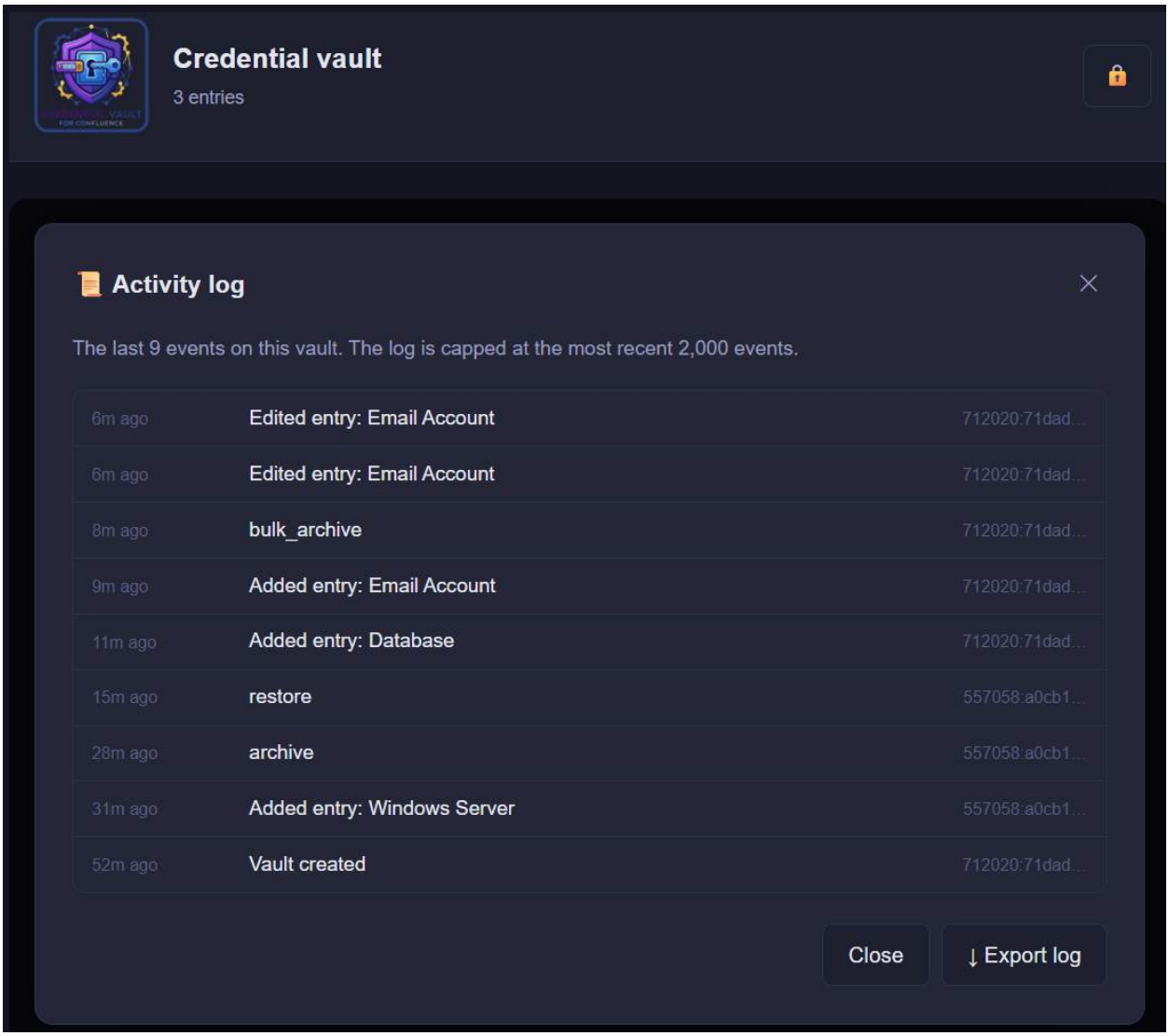
Configure the defaults used by the Generate button on the entry form. See Section 4.2.

15 Activity log

Open Settings > Activity log to see the most recent vault events. The log is PIN-protected on the server - opening it requires your PIN hash, so a user with page access but not the PIN cannot read it.

Events logged include vault_created, pin_change, add, edit, delete (with entry name), archive, restore, bulk_archive, archive_purge (auto-deletes), csv_export, csv_import, ownership_transferred, and restore_password.

Each row shows when, what, and who (display name plus account ID on hover). The log is capped at the most recent 2,000 events per vault to prevent unbounded storage growth. You can export the log to CSV from the modal footer.



16 Locking and auto-lock

16.1 Lock immediately

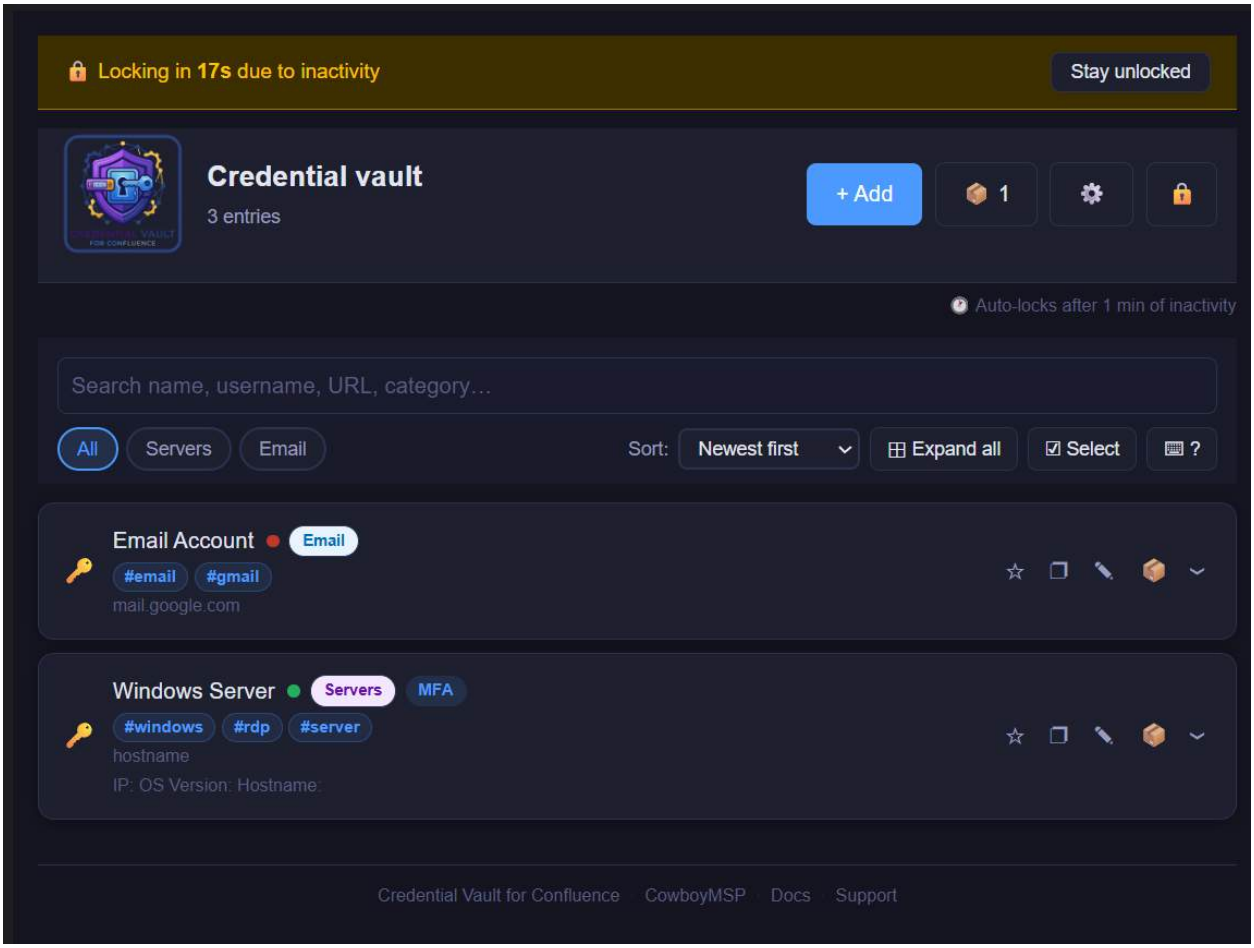
Click the lock icon in the header at any time. All decrypted credentials and the session key are cleared from memory; the lock screen returns.

16.2 Auto-lock

The vault automatically locks after the configured idle timeout (default 10 minutes). Idle means no mouse movement, keystrokes, scrolls, or touch events.

A 60-second countdown banner is shown before the lock fires, with a Stay unlocked button. For the 1-minute setting the warning starts at 20 seconds.

The vault also locks when you navigate away from the Confluence page or refresh it.



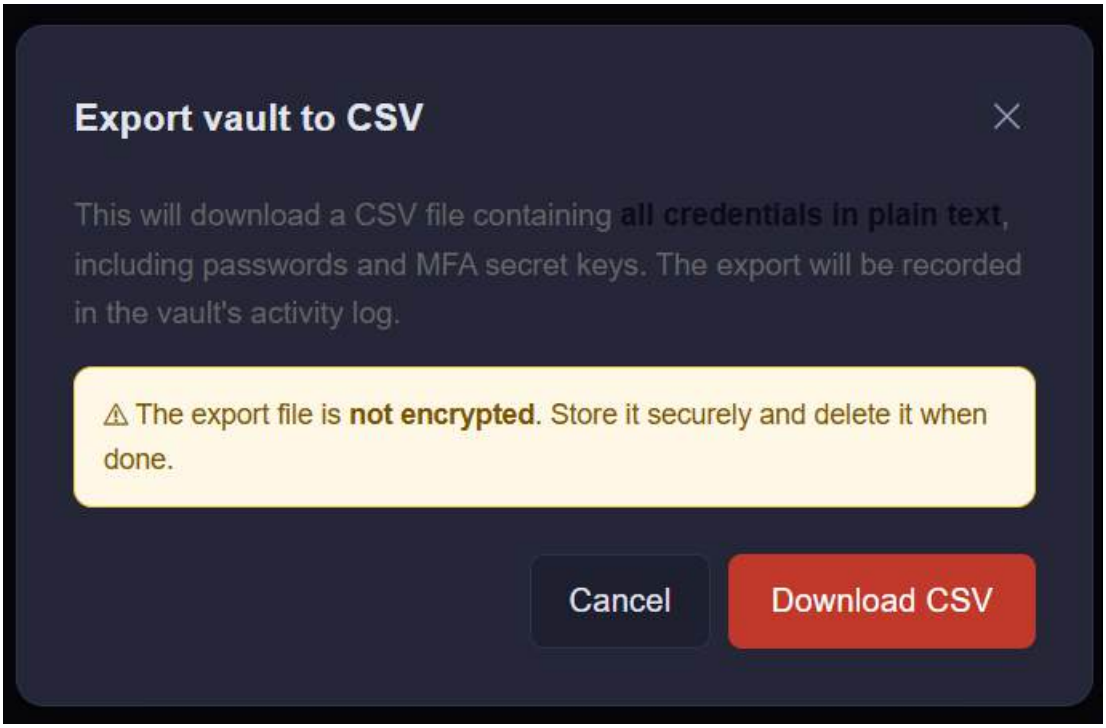
17 Import and export

17.1 Export to CSV (owner only)

9. Open Settings > Export to CSV.
10. Read the security warning carefully.
11. Click Download CSV to confirm.

The export is generated entirely in your browser. The file is downloaded directly. Every export is recorded in the Activity log so other team members can see who exported and when.

Security notice: the exported CSV is not encrypted. Treat it like a master password list. Store it in a secure location and delete it once you have finished using it. Tags and password history are not currently included in the export.



17.2 CSV columns

Column	Contents
Name	Entry name.
Category	Entry category, if set.
URL	Login URL, if set.
Username	Username or email.
Password	Password in plain text.
MFA Secret (TOTP Key)	Raw base32 TOTP secret.
Notes	Notes field.
Created	Date the entry was created.
Modified	Date the entry was last edited.
Last Used	Date the entry was last opened.

17.3 Importing MFA secrets into another app

The MFA Secret column contains the raw base32 key. This can be entered into any standard authenticator app:

- Google Authenticator - plus icon, then "Enter a setup key", paste the key.
- Authy - Add account, "Enter key manually", paste the key.
- Microsoft Authenticator - plus icon, "Other account", "Enter code manually".

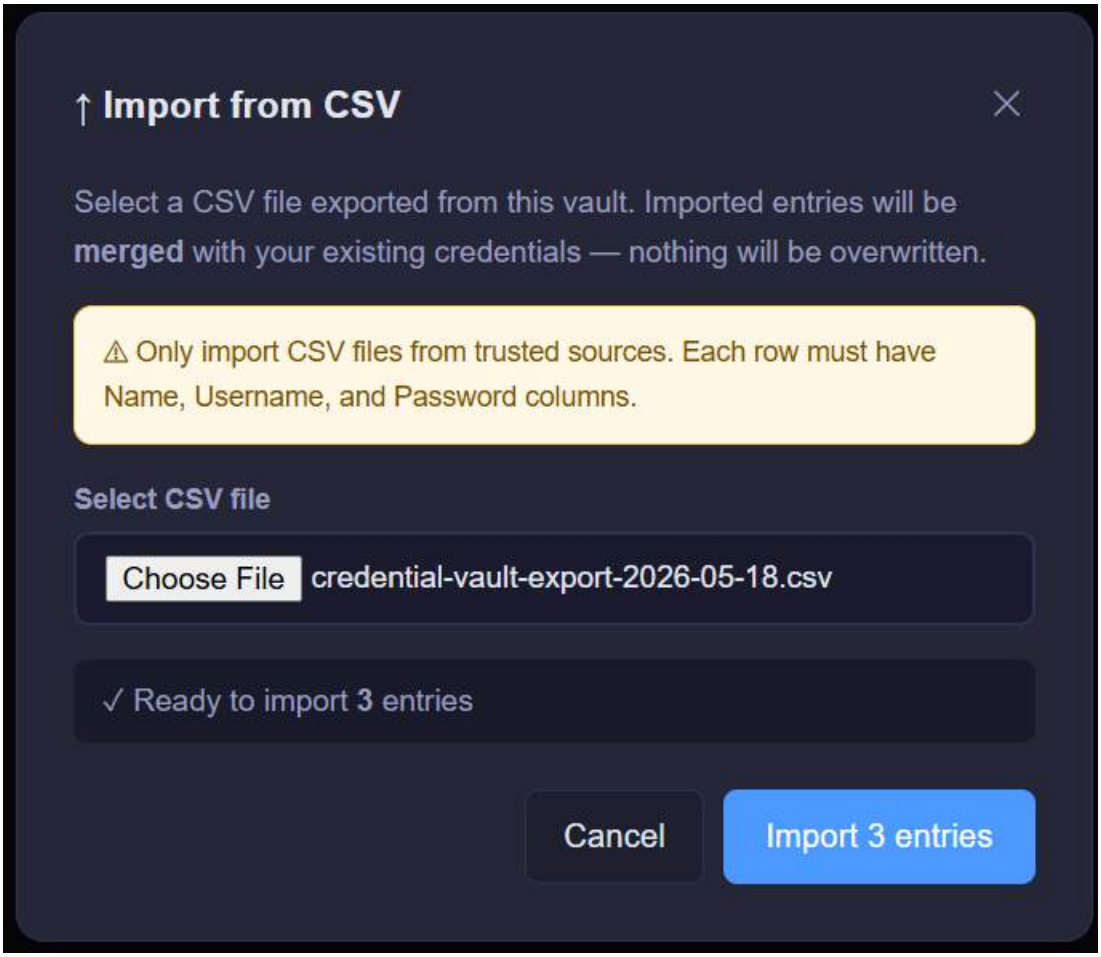
- 1Password - Edit the item, Add field, "One-Time Password", paste the key.
- Bitwarden - Edit the item, TOTP, paste the key.

17.4 Import from CSV (owner only)

12. Open Settings > Import from CSV.
13. Click Select CSV file and pick a file exported from Credential Vault.
14. The vault parses the file and shows the entry count.
15. Click Import N entries to merge them into the vault.

Imported entries are merged with existing credentials - nothing is overwritten. The CSV must include at least the Name, Username, and Password columns. Unsafe URL protocols (javascript:, data:, vbscript:, file:) are blanked out silently during import; the credential itself is still saved.

On the free tier, an import is blocked if it would push you above the 3-entry limit.



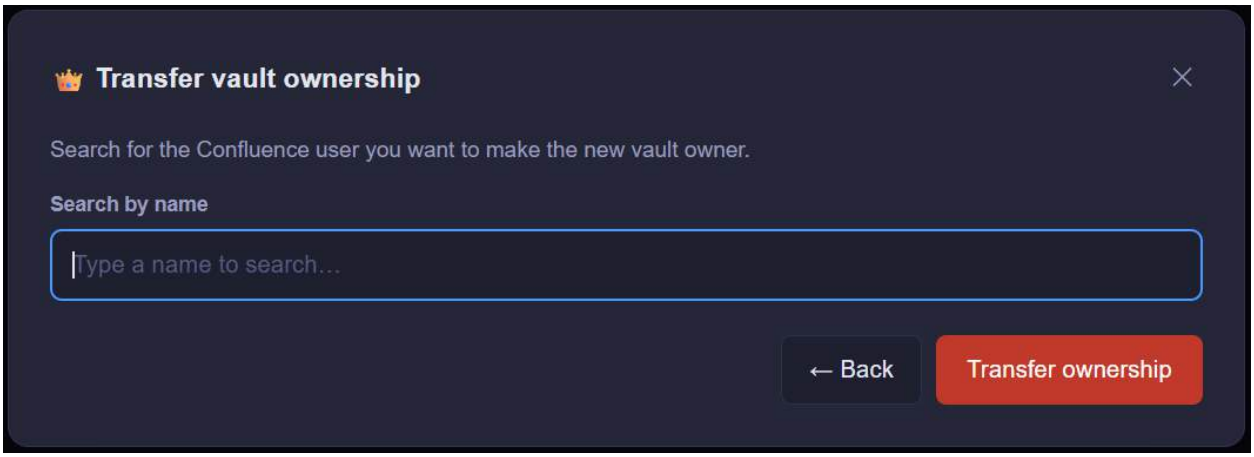
18 Transfer vault ownership

The vault owner can hand off ownership to another Atlassian user on the same site - useful for staff handovers, account closures, or rotating duties.

16. Open Settings > Transfer vault ownership.

17. Read the warning carefully - the change cannot be undone by you.
18. Click Continue, search for the new owner by name (Confluence user search), and select them.
19. Click Transfer ownership.

You lose owner-only rights immediately. The new owner can permanently delete entries from the Archive, change the vault PIN, idle timeout, and archive retention, import and export CSV, manage shared templates and categories, and transfer ownership again. The event is recorded in the Activity log as ownership_transferred.



19 Recovery if you forget your PIN

There is no server-side recovery. Your PIN is never stored - only a salted SHA-256 hash is kept for verification. Without the correct PIN, the AES-GCM encrypted data cannot be decrypted.

19.1 Before you are locked out

- If the owner is still logged in, open Settings > Change PIN and set a new PIN you will remember.
- The owner can export credentials via Settings > Export to CSV as a backup before locking.

19.2 If you have already forgotten your PIN

Unfortunately, the encrypted credentials cannot be recovered. This is intentional - it means nobody else can recover them either, including Atlassian and CowboyMSP. The owner can recreate the vault on a new page and re-enter the credentials from any backup.

19.3 Prevention for the future

- Store your vault PIN in your personal password manager (1Password, Bitwarden, LastPass, etc.).
- Keep a printed or written copy in a secure physical location.
- Always heed the "write this down" warning on first setup and PIN changes.
- Owners should export to CSV periodically and store the file securely.

20 Plans and licensing

Capability	Free	Paid
Credential entries	Up to 3	Unlimited
PIN encryption (AES-GCM 256)	Yes	Yes
Change PIN	Yes	Yes
MFA / TOTP generation	Yes	Yes
Password generator	Yes	Yes
Have I Been Pwned breach check	Yes	Yes
Categories, tags, search, sort	Yes	Yes
Pin to top, duplicate, archive	Yes	Yes
Password history (last 5)	Yes	Yes
Templates (built-in, admin, personal)	Yes	Yes
Activity log (last 2,000 events)	Yes	Yes
Auto-lock with countdown	Yes	Yes
Light / Auto / Dark theme	Yes	Yes
CSV import and export	Yes	Yes
Transfer ownership	Yes	Yes
QR re-add to authenticator	Yes	Yes
30-day free trial	No	Yes
Licence required	No	Atlassian Marketplace

When you reach the 3-entry free-tier limit, a yellow banner is shown in the vault header. The + Add button is disabled until a licence is active. Existing entries can still be viewed, copied, edited, and archived - you just cannot add new ones.

21 Keyboard shortcuts

When the vault is unlocked and no modal is open, the following keyboard shortcuts work:

Key	Action
/ (forward slash)	Focus the search input.
N	Open the templates picker to add a new entry (disabled at free-tier limit).
Esc	Collapse all expanded entries.

A small "kbd ?" button is shown next to the sort dropdown - click it to reveal the same list inline.

22 Frequently asked questions

Can Atlassian read my credentials?

No. Credentials are encrypted in your browser using AES-GCM 256-bit before they are sent to Forge storage. Only encrypted blobs reach Atlassian's servers. Without your PIN, the data cannot be decrypted by Atlassian, CowboyMSP, or anyone else.

What happens if I forget my PIN?

Your credentials cannot be recovered without the PIN. See Section 19 - Recovery. Always store your PIN in a personal password manager.

Can I change my PIN without losing data?

Yes. Open Settings > Change PIN. All entries are re-encrypted with the new PIN immediately. Owner only.

How does the breach check work?

Only the first 5 characters of a SHA-1 hash of your password are sent to the Have I Been Pwned API (k-anonymity). Your actual password and the full hash never leave your browser.

Can I use the vault on mobile?

Yes. The vault works in any modern browser, including Confluence's mobile browser experience.

Why does the MFA code sometimes show dashes?

The MFA secret stored for that entry is invalid or incorrectly formatted. Edit the entry and verify the secret is a valid base32 string with no spaces. You can paste a full otpauth:// URI - the vault parses digits, period, and algorithm from it.

How do I give someone else access to the vault?

Give them the Confluence page URL and the vault PIN. They need Confluence page view access and the PIN to decrypt.

Can I have multiple vaults?

Yes - each Confluence page with the macro added has its own independent vault, PIN, entries, templates, and settings.

Is the CSV export encrypted?

No. The CSV is plain text for portability. Delete it after use. Every export is recorded in the Activity log.

What happens to deleted entries?

They go to the Archive (soft delete). The vault owner can permanently delete archived entries from there. Archived entries are also auto-deleted after the retention window you choose in Settings (default 90 days).

Can I recover an old password if I changed it?

Yes, if it is one of the last 5 passwords for that entry. Click the clock icon next to the password field in the expanded card to open Password history, then click Restore on any row.

What's the difference between Categories and Tags?

Categories come from a fixed list managed by the vault owner. Tags are freeform per-entry labels typed by the user. Both are searchable.

How do I hand the vault over when someone leaves?

The current owner opens Settings > Transfer vault ownership and picks the new owner from the Confluence user search. The handover is immediate and audited.

Why is the Change PIN option greyed out for me?

You are a regular user, not the vault owner. PIN, auto-lock, archive retention, import, export, templates, and categories are owner-only. View, copy, add, edit, and archive remain available to everyone with the PIN.

23 Security summary

Property	Detail
Encryption	AES-GCM 256-bit, client-side only.
Key derivation	PBKDF2 with 200,000 iterations, per-vault random salt.
PIN hash	Salted SHA-256. The PIN itself is never stored or transmitted.
TOTP generation	HMAC-SHA-1 (default), SHA-256, or SHA-512 via Web Crypto API, entirely in-browser.
Breach checking	k-anonymity via Have I Been Pwned (5-char SHA-1 prefix only).
Storage	Encrypted blobs in Atlassian Forge KV Storage.
External egress	Only api.pwnedpasswords.com is allow-listed in the manifest.
Auto-lock	Configurable 1-60 minutes idle, with 60-second pre-lock warning.
Activity log	PIN-gated read, capped at 2,000 events per vault.
Concurrency	Optimistic version checks and stale-PIN-hash detection on save.
Data scope	Per Confluence page; shared among users with page access.
Page-context safety	Vault operations hard-fail without a page context (no cross-page bleed).
URL protocol allow-list	Dangerous schemes (javascript, data, vbscript, file) are blocked.

Credential Vault for Confluence - built on Atlassian Forge by CowboyMSP
Support: support@cowboymsp.com - Web: https://cowboymsp.com