CF Access Service Token Rotation

CF Access Service Token Rotation (docs.alai.no / BookStack)

MC: #99235 (cleanup) — follow-up to Proveo audit #99027 (2026-05-05), deferred from kelsey-hightower subtask 3 on #99027.

Background

`docs.alai.no` (BookStack, Azure VM 4.223.110.181) sits behind Cloudflare Access. All programmatic API calls (BookStack REST API, sync tooling) need two credential pairs:

1. **BookStack API token** — `Authorization: Token <token_id>:<token_secret>` (BookStack user token)
2. **CF Access service token** — `CF-Access-Client-Id` + `CF-Access-Client-Secret` headers (bypasses the CF Access login redirect for non-interactive clients)

Both live in `~/system/config/bookstack.json` (local cache) and, for the BookStack token, in Vaultwarden item **"BookStack API"** (`fe418612-0d17-4e80-9b2e-39ef7c213b61`).

Finding: CF_ACCESS_CLIENT_SECRET leaked in git history

`~/system/config/bookstack.json` was git-tracked with the CF Access client secret **in plaintext** from 2026-02-12 through ~1775 auto-backup commits (repo `~/system`, private, external exposure

minimal per CEO risk assessment 2026-05-05).

CEO decision (2026-05-05): document, do NOT rotate the token immediately.

Status as of 2026-07-29 (MC #99235 cleanup pass):

- `config/bookstack.json` HEAD content had already been redacted in commit `e3e6fe36bd` (2026-07-28 21:00 auto-backup) — `cf_access_client_id` / `cf_access_client_secret` replaced with `[REDACTED — see vault item b42cb5c2]`.
- ⚠ **That vault pointer is wrong.** Vaultwarden item `b42cb5c2-dc9b-4a43-bcc7-4adcfde992b2` is named "*ligthrag monitor deamon service token*" and holds a CF Access pair for a **different** service (`client_id` starting `4248b2c1...`), not the `d9c7d65a...` client_id that was actually in `bookstack.json`'s history. The real BookStack CF Access service-token credential does not currently have a confirmed Vaultwarden home — treat as **not yet rotated, not yet safely stored**, and flag to CEO before relying on that note.
- `config/bookstack.json` and `config/.bookstack-cred-cache.json` were **still git-tracked** (gitignore had no entry) as of this pass, meaning any future edit — including someone restoring a real secret into the file to fix the tool — would re-leak it. Fixed in commits `97552323df` (.gitignore) + `4c69de88f8` (untrack both files; local copies preserved on disk).
- `bookstack-sync.js` was hardened in this pass to ignore `[REDACTED ...]` CF Access placeholders instead of sending them as HTTP headers. Without that guard, sync failed locally with `Invalid character in header content ["CF-Access-Client-Id"]` after the redaction commit.
- The **BookStack API token itself** (`token_secret` field, used for `Authorization: Token`) is still plaintext in the current file and in every historical commit. Same exposure class as the CF secret; not in scope of the original #99027 finding but should be rotated together if/when the CF token is rotated.
- Git **history purge** (removing the secret from all ~1775+ past commits) was NOT done — coordinate with the `~/system` git-history cleanup lineage (MC #105751, filter-repo based) before attempting; do not run filter-repo ad hoc without that runbook's safety steps.

Rotation procedure (when CEO approves)

1. **Generate new service token** in Cloudflare Zero Trust dashboard → Access → Service Auth → Service Tokens → create/rotate the token scoped to `docs.alai.no` (and any other `*.alai.no` host sharing the same Access policy).
2. **Store in Vaultwarden** as a dedicated item (do not reuse an unrelated item like `b42cb5c2`). Recommended: new item "BookStack CF Access" with fields `cf-access-client-id` / `cf-access-client-secret`, matching the field-name pattern `bookstack-sync.js` already expects when a vault item does carry these fields (`loadConfigFromVault()` reads `fields.cf_access_client_id` / `fields.cf_access_client_secret` from the "BookStack API"

item — either add the fields there, or update `~/system/tools/bookstack-sync.js:118-130` to also check the new item name).
3. **Update** `~/system/config/bookstack.json` with the new pair (file is now gitignored — editing it will NOT create a new leak).
4. **Revoke the old token** in Cloudflare Zero Trust once the new one is verified working: `curl -I -H "CF-Access-Client-Id: <new>" -H "CF-Access-Client-Secret: <new>" https://docs.alai.no/api/docs` → expect `200`.
5. **Verify sync still works:** `node ~/system/tools/bookstack-sync.js status` should list pages without `Vault unreachable` or `HTTP 401/403` errors.
6. Update this runbook with the new Vaultwarden item ID once done.

Prevention (already applied, MC #99235)

- `config/bookstack.json` and `config/.bookstack-cred-cache.json` added to `~/system/.gitignore` and untracked from git (commits `97552323df`, `4c69de88f8`).
- Local files remain in place at `~/system/config/`.
- `bookstack-sync.js` only sends CF Access headers when both values are real header-safe strings; redacted placeholders are ignored.
- History purge is a separate, deliberately-deferred step (CEO 2026-05-05 decision) — do not schedule without explicit CEO go-ahead, and do it as part of the git-history cleanup lineage (MC #105751), not standalone.

Revision #3
Created 2026-07-29 00:09:54 UTC by John
Updated 2026-07-29 00:12:35 UTC by John