SWISSSUITE AI

User Manual

Version 2.9.30.89 · Updated 2026-05-26 · Free & Pro editions · swisswpsecure.com

SwissSuite AI — User Manual

> Architecture: dual-build freemium — see docs/architecture/FREEMIUM_DUAL_BUILD_ARCHITECTURE.md

Version: 2.9.30.89 **Last Updated:** 2026-05-26 **Audience:** WordPress site owners. No coding required.

> **Two editions.** SwissSuite AI ships as two products built from one codebase: **SwissSuite AI** (free, installed from the WordPress.org directory) and **SwissSuite AI Pro** (downloaded from swisswpsecure.com after purchase). The free edition contains only the free local features; the paid features described in this manual as "Pro" — 2FA, geo-blocking, advanced WAF, cloud backup, sync, migration, and all AI features (deep AI scan, AI SEO meta, AI content) — live exclusively in the Pro edition, which you download and install separately. Entering a Pro license key in the free edition prompts you to download Pro.

Table of Contents

---

1. Getting Started

1.1 What SwissSuite Does

SwissSuite AI is an all-in-one WordPress plugin for **security**, **backups**, **migration**, **content sync**, **SEO**, and **AI content rewriting**. It runs entirely inside your WordPress admin — there is nothing to install on your server.

The plugin has three states:

- **No license activated** — the core firewall (basic WAF), the Quick malware scan, manual local backups, essential hardening, and login/spam protection all work. The daily Sentinel Audit can be run on demand, but the **daily Scan Report email** and any AI-powered feature are not available because both require an active license.
- **Free license** — request one from inside the plugin (enter your email, one click). It is **domain-locked** (one site only) and gives you **50,000 AI tokens per month** plus the daily Scan Report email. Tokens are used by AI-powered analysis features (for example, the "Check with AI" action on individual scan findings, and the AI Threat Analysis of recent logs). Tokens are **not** enough to unlock paid-tier features such as Deep AI Malware Scan, SEO meta generation, FAQ generation, or AI content rewriting — those require a paid plan.
- **Pro mode** — unlocked by activating a paid license. Adds Deep AI Malware Scanning, advanced hardening, geo-blocking, cloud backups, scheduled backups, site migration, content sync, SEO automation, and AI content rewriting. The paid token allowance is higher and depends on your plan.

> **What "Free capabilities" really are.** Whether or not you have a license, every site starts with the same six baseline capabilities: `scan_basic`, `reports`, `threat_block_basic`, `dashboard_access`, `backup_local`, `firewall_basic`. Activating a *free* license adds the daily Scan Report email and the monthly AI token allowance, but does **not** add `2fa`, `hardening`, `seo_meta`, or any other paid capability — those are tier-gated. See **Section 9** for the full capability list.

1.2 Installation

Install SwissSuite from the official WordPress.org plugin directory:

1. In your WordPress dashboard, go to **Plugins** → **Add New**.
2. Search for **SwissSuite AI**.
3. Click **Install Now**, then **Activate**.

After activation, a new menu item called **SwissSuite** appears in your WordPress sidebar.

> **Free vs Pro installation.** The **free** edition (SwissSuite AI) installs from the WordPress.org directory as above. To unlock the paid features, purchase a plan at swisswpsecure.com and download the **SwissSuite AI Pro** ZIP from your account, then install it via **Plugins** → **Add New** → **Upload Plugin**. Pro is a full standalone superset — deactivate the free edition and activate Pro (it contains the free features too). Pro updates come from swisswpsecure.com, not WordPress.org, so a wp.org update can never downgrade your Pro install.

System requirements:

- WordPress 5.6 or newer
- PHP 7.4 or newer
- **WordPress 7.0 compatible.** The plugin header lists a conservative "Tested up to" value of 6.7, but the codebase has been adapted for WordPress 7.0: it ships a `SWISSWP_WP7` feature flag that activates 7.0-specific behavior (notably, coexistence with WP 7.0's Real-Time Collaboration sessions and the WP Abilities API for bring-your-own LLM). It runs unchanged on WordPress 6.x.

1.3 First-Time Setup

The first time you open SwissSuite, the **Dashboard** shows a **Critical Next Steps** card. It guides you through the four most important things to do:

1. **Activate (or request) a license** — Open **Settings** → **License** and either paste an existing license key, or scroll down to "No license? Start free" and enter your email. A free, domain-locked license is created and activated instantly.
2. **Run your first scan** — Go to **Security** → **Scan** and click **Run Sentinel Audit**. Results appear within a few seconds.

3. **Create your first backup** — Go to **Backup** → **Backups** and click **Create Backup Now**. Wait until the green "Complete" badge shows.
4. **Turn on 2FA** — Two-Factor Authentication is a paid-tier feature. If your plan includes the `2fa` capability, go to **Settings** → **Security** → **Two-Factor Authentication** and follow the in-page setup. Without 2FA your admin password is the only thing protecting your site.

You can dismiss the Critical Next Steps card at any time by clicking the small "x" in its corner. It comes back automatically if any of the four items become incomplete (for example, your license expires).

1.4 The Sidebar — How You Navigate

The left sidebar shows six main destinations (the order is fixed):

Item	What it opens
Dashboard	Health overview, alerts, recent activity.
Security	The Security Hub — scans, firewall, hardening, logs, quarantine, IP management, history.
SEO	SEO scan, bulk meta generation, On-Page audit, FAQ generation, sitemap (Pro).
AI Content	List of posts/pages/products, rewrite proposals, bulk apply, restore (Pro).
Backup	Backups, Move to New Host (Beta), Sync Two Sites (Beta).
Settings	General, AI Configuration, Security, SEO, License, Maintenance.

If your license does not include a feature, that sidebar item shows a small **lock icon**. Clicking it still opens the page, but the actions inside are disabled with an "Upgrade to unlock" prompt.

Standalone mode. If the plugin detects it is running in a standalone Sentinel-only build, the **SEO** and **AI Content** items are hidden, and the Dashboard route redirects to Security.

The sidebar can be **collapsed** with the small `<` button at the bottom-left. Your preference is remembered in your browser. On mobile, the sidebar is a swipe-out drawer — tap the hamburger icon in the top bar to open it.

When a Pro **trial** is active, a small "Trial" pill appears under the plugin logo. The trial end date itself is shown in **Settings** → **License** (see Section 7.5), not in the sidebar.

1.5 No-License vs Free License vs Pro — at a Glance

Feature	No license	Free license	Pro
Basic Web Application Firewall (WAF)	Yes	Yes	Yes
Login protection (brute-force lockouts)	Yes	Yes	Yes
Spam protection	Yes	Yes	Yes

Feature	No license	Free license	Pro
Quick Malware Scan (signatures only)	Yes	Yes	Yes
Sentinel Audit on demand (heuristic + signatures, zero AI cost)	Yes	Yes	Yes
Daily Scan Report email (automatic daily run + email)	No	Yes	Yes
Monthly AI token allowance	0	50,000	Plan-dependent
"Check with AI" on individual findings	No	Yes (uses tokens)	Yes (uses tokens)
Deep Malware Scan (hash DB + WPScan + Patchstack + AI analysis)	No	No	Yes
Essential hardening (8 options)	Yes	Yes	Yes
Advanced hardening (5 options)	No	No	Yes
Geo-blocking by country	No	No	Yes
Manual IP banning	No	No	Yes
IP allowlist	View only	View only	Edit
Quarantine restore / delete	View only	View only	Edit
Manual local backups	Yes	Yes	Yes
Cloud backups (Google Drive, Dropbox, S3, Backblaze B2, FTP)	No	No	Yes
Scheduled backup automations	No	No	Yes
Backup encryption (AES-256 / XChaCha20)	No	No	Yes
Site Migration (Move to New Host)	No	No	Yes (Beta)
Content Sync (Sync Two Sites)	No	No	Yes (Beta)
SEO scan + meta generation	No	No	Yes
FAQ generation	No	No	Yes
On-Page audit	No	No	Yes
llms.txt + AI-aware sitemap	No	No	Yes
AI content rewriting	No	No	Yes
Two-Factor Authentication (TOTP + backup codes)	No	No	Yes
WordPress.org Update Guard (virtual patching)	Yes	Yes	Yes

> Capability codes (used in the API): `scan_basic`, `reports`, `threat_block_basic`, `dashboard_access`, `backup_local`, `firewall_basic` are always present — they exist whether or not a license is activated, and a free license adds nothing else to that list. Pro adds (depending on plan): `sentinel_pro`, `scan_deep`, `ai_access`, `ai_content`, `threat_block_pro`, `reports_advanced`, `waf`, `advanced_waf`, `geoblocking`, `advanced_malware`, `auto_quarantine`, `files_monitor`, `2fa`, `hardening`, `rate_limiting`, `seo_meta`, `seo_advanced`, `sitemap`, `broken_links`, `page_speed`, `backup_cloud`, `sync_staging`, `blog_generation`, `product_descriptions`, `meta_ai`, `scheduled_backups`, `content_rewrite`. See **Section 9**.

---

2. Dashboard

The Dashboard is the page you land on when you open SwissSuite. It shows the high-level health of your site.

2.1 The Critical Next Steps Card

A teal card at the top of the Dashboard listing tasks you should complete to be secure. Items only appear here if they are still incomplete:

- **No license active** — shows an "Activate License" button.
- **No backup in the last 30 days** — shows "Create Backup".
- **2FA not enabled** (Pro plans only) — shows "Enable 2FA".
- **Critical Sentinel findings unfixed** — shows "Open Security Hub".

Each item is a one-click jump to the right page. You can dismiss the entire card with the small "x" button; it reappears automatically if a new gap is detected.

2.2 The Health Tiles

A row of tiles below the Critical Next Steps card. Exactly which tiles you see depends on your plan, but the main dashboard shows summary information such as:

- **Last Backup** — when the most recent backup completed. Shows "Never" if no backup exists. Color-coded: green (< 7 days), amber (7–30 days), red (> 30 days or never).
- **SEO Health** — a score from 0 to 100 based on the last SEO scan (Pro). "—" means no SEO scan has been run yet.
- High-level firewall and scan status indicators that link to the Security Hub.

> Your remaining **AI token balance** for the month is **not** shown on the main Dashboard. It is shown only in **Settings → License**.

2.3 Recent Activity

Below the tiles, a small list of the last few events: scans completed, backups created, login attempts blocked. Each row links to the relevant page.

---

3. Security Hub

The Security Hub is the largest area of the plugin. It has seven tabs along the top:

`dashboard` · `scan` · `logs` · `quarantine` · `hardening` · `cloud-shield` · `history`

The tab labels are lowercase except for **History** (with a clock icon) and **Cloud Shield** (with a globe icon). The active tab gets a navy underline.

3.1 Dashboard tab (Security overview)

This is the **security summary page** (different from the main app Dashboard in Section 2). It is laid out as a grid of premium status cards, each with its own toggle and short description. The exact set of cards depends on your plan, but typically includes:

- **Smart Firewall** card — toggle to enable/disable the WAF; a "Detection Only Mode" checkbox to log threats without blocking; a list of the active rule packs (Basic WAF shows 5 SQLi + 4 XSS patterns and path traversal; Advanced WAF, when your plan includes it, lists 28+ SQLi patterns, 40+ XSS patterns, 3-layer URL decoding, and double/triple-encoded payload detection).
- **Geo-Lockdown** card (Pro) — country block/allow mode, "Block High-Risk Zones" preset, and a country picker.
- **Update Guard** card — observe/auto-patch status for the WordPress.org virtual-patching feature.
- **Quick-toggles** for Login Protection, Spam Protection, and other firewall sub-features mirror the equivalent controls in the Logs tab.

If your plan does not include a feature, its card shows an "Upgrade for full protection" panel instead of the toggle.

After you run a scan from the Scan tab, a **scan summary card** appears on this Dashboard tab showing the security grade (A / B / C / D / F, only available after a Deep Malware Scan) and a link back to the detailed results.

3.2 Scan tab

The Scan tab has **three scan cards** stacked vertically. Each card has its own "Start" button, its own progress indicator, and its own results panel.

3.2.1 Sentinel Audit (free, daily)

What it does. Runs a four-module heuristic scan locally (no Groq AI calls):

- **M1 — File System Audit** — looks for malware patterns, PHP in uploads, suspicious filenames, and WordPress core file integrity (compares against checksums from wordpress.org).
- **M2 — Permission Audit** — flags world-writable files, executable uploads, SUID bits.
- **M3 — Config Audit** — checks for `WP_DEBUG` left on in production, exposed `debug.log`, backup files in the web root, directory listing enabled.
- **M4 — Environment Audit** — reports WordPress / PHP / server versions, plugins, XML-RPC exposure, REST user enumeration, default `admin` username.

Cost. Zero tokens. Available to everyone, including sites with no license.

Button: Run Sentinel Audit. While running, the button is disabled and shows a spinner. Findings appear in the results panel below.

> The automatic **daily** Sentinel Audit (the one that emails you a report each morning) requires an active license — see **Section 3.2.4**.

3.2.2 Quick Malware Scan

What it does. Scans your WordPress core, themes, plugins, and uploads for known malware signatures using a local pattern library. No AI involved.

Cost. Zero tokens. Available to everyone (with or without a license).

Button: Run Quick Scan. Results show each suspicious file path with action buttons described in Section 3.2.5.

Note. A previous version had a "Deep" mode toggle on this card. It was removed in v2.9.30.74 — to run a deep scan, use the dedicated **Deep Malware Scan** card (Pro).

3.2.3 Deep Malware Scan (Pro)

What it does. An eight-phase asynchronous pipeline (only the phases your license enables run):

1. **Enumerate** — finds candidate files.
2. **Hashing** — computes SHA-256 for each candidate.
3. **VPS hash lookup** — checks each hash against our cloud database (MalwareBazaar + URLhaus, hourly-refreshed).
4. **Local scan** — runs the malware-signature pattern engine.
5. **WPScan API** — if you provided a WPScan API key, queries the vulnerability database for installed plugin / theme slugs and versions.
6. **Patchstack API** — same as above, for the Patchstack feed (if you provided a key).
7. **AI analysis** — sends suspicious findings to Groq AI for a final verdict.
8. **Complete** — assembles the report and a grade (A / B / C / D / F).

Button: Start Deep Scan. The card shows the **current phase name** as the scan progresses (Enumerate → Hashing → VPS lookup → …). You can leave the page — the scan continues in the background, and the result will appear next time you come back. You can also stop a running scan with **Cancel**.

Result panel. In addition to the Quick Scan fields, it shows: - An **AI Grade** badge (A green, B emerald, C amber, D/F red, "?" gray when unavailable). - **Source pills** for each finding — `Hash DB`, `Pattern`, `WPScan`, `Patchstack`, or `AI`. This tells you which data source flagged the file. - **Status pills** — `VPS hash: ok / degraded / unavailable`, `WPScan: ok / degraded / unavailable`, etc. Amber means the source ran but with reduced confidence; gray means the source was not contacted (no API key or feature off). - A warning banner when files were skipped or the budget was exhausted (for example, "Review your ignored paths in Settings → Security → Quarantine").

If you have no WPScan or Patchstack API key, those phases skip cleanly and the scan finishes with whatever data is available.

3.2.4 Daily Scan Report email

A card on the Scan tab labeled **Daily Scan Report**. It shows:

- A **toggle** to enable or disable the daily email
- An **email address** field (defaults to your admin email)
- **Preview Report** button — opens the rendered HTML in a modal so you can see what the next email will look like
- **Send Test Email** button — sends the next scheduled report to the configured address right now

When enabled, the daily cron at midnight site-time runs the day's scan and emails the results. If the email fails to send (for example, your host's `wp_mail()` is misconfigured), a persistent admin notice appears at the top of every WP-Admin page until the next successful send.

> The daily Scan Report email requires an **active license** (free or paid). Without any license activated, you can still run a Sentinel Audit on demand, but you will not get the automatic daily email.

3.2.5 Scan results — what you see

Each finding row in the results panel shows:

- A **severity badge** — `critical` (red), `high` (orange), `medium` (yellow), `low` (gray), `info` (blue)
- A short **title** and a one-line description
- The **module code** for Sentinel findings (e.g. `M1-A`, `M3-B`)
- The **evidence** — usually a file path, a header value, or a version string
- For CVE findings: the **CVE ID**, affected versions, your installed version, and whether your version is verified as vulnerable

Per-finding action buttons (which appear depends on the finding type and your plan):

- **Mark safe** — adds this file path (or finding id, for non-file findings) to your ignore list so future scans skip it.
- **Quarantine** — moves the file to the protected quarantine directory (file findings only).
- **Delete** — permanently removes the file (file findings only).
- **Check with AI** — sends the finding to Groq AI for a deeper verdict (consumes tokens; requires an active license with an AI token allowance).

> There is no "Fix it" button. Earlier documentation referred to one — it was retired. Use the actions above to act on a finding.

A summary banner at the top of the panel shows counts: "3 critical, 5 high, 2 medium, 1 low". A green banner says "All clear" when nothing is found.

3.3 Logs tab

This tab shows the **security event log** and the master toggles for the firewall.

The log table shows recent events with columns: **Time**, **IP**, **Event**, **Severity**, **Blocked?**. Severity rows are color-banded: red (high), amber (medium), gray (low).

3.3.1 Firewall (WAF) toggles

- **Firewall enabled** — master switch. When off, no incoming requests are filtered.
- **Simulation mode** — when on, the firewall **logs** what it would block but **does not** actually block. Use this for one day after enabling, to verify nothing legitimate is caught.
- **Block SQL injection patterns** — toggle for the SQLi rule pack.
- **Block XSS patterns** — toggle for the XSS rule pack.

No-license and free-license sites get a basic ruleset (5 SQLi patterns, 4 XSS patterns, path traversal). Pro plans with `advanced_waf` get the full ruleset (28+ SQLi patterns, 40+ XSS patterns, comment-injection bypass, command injection, common-CVE patterns, advanced anti-bot rules).

3.3.2 Login Protection

- **Login protection enabled** — toggle. Counts failed login attempts per IP.
- **Max retries before lockout** — number input (default 5). After this many failures within 10 minutes, the IP is auto-banned for 30 minutes.

3.3.3 Spam Protection

- **Spam protection enabled** — toggle. Blocks comment/registration spam patterns at the firewall level (before WordPress processes the request).

3.3.4 AI Threat Analysis (Pro)

A button **Analyze last 24h logs with AI** sends a hashed summary of the recent log to Groq AI and returns:

- A **threat verdict** (clean / suspicious / under attack)
- A short prose **summary**
- A **threat level** label
- **Suggested actions** — and if the AI detects coordinated attackers, a list of **Suggested IP bans** with one-click "Ban" buttons.

3.4 Quarantine tab

This tab manages files the plugin has isolated, plus your IP allowlist and blocklist.

3.4.1 Quarantined Files

When the malware scanner detects a malicious file, it **moves** it (it does not delete it) to a protected directory called `wp-content/uploads/swisswpsuite-quarantine/`. That directory has its own `.htaccess` that blocks all web access.

Each quarantined file appears in a table with: - **Original path** - **Quarantined at** (date) - **Size** (human-readable, e.g. "4.2 MB") - **Restore** button (Pro) — moves it back to its original location. - **Delete forever** button (Pro) — permanently removes it.

No-license and free-license sites can view this list but cannot restore or delete.

3.4.2 Ignored Paths (Mark Safe)

A list of file paths and finding IDs you have manually marked as safe. The scanner skips these on future scans.

Two types of entries: - **Path-based** — e.g., `wp-content/themes/my-theme/template-custom.php`. The plugin also stores the SHA-256 of the file at the time you marked it. If the file changes later, the entry is auto-evicted and the file is rescanned (this stops attackers from swapping your safelisted file with malware). - **ID-based** — e.g., `m4-001`, `m3-005`. Used for non-file findings like "WordPress Version Detected" or "Bundled Plugin File Missing", where there is no path to safelist.

Each row has a **Remove** button (Pro).

3.4.3 Blocked IPs

A table of currently blocked IPs. Each row shows: - **IP address** - **Reason** — a short text label describing why the IP is blocked (for example, "Brute-force lockout" or whatever you typed when you blocked it manually) - **Expires** — for time-limited blocks (such as a 30-minute brute-force lockout), the time the block ends. Permanent blocks have no expiry. - **Release** button (Pro) — removes the block immediately. The button is idempotent — clicking it on an already-cleared block is harmless.

Block IP form (Pro) — at the top of the table: - IP input — accepts a single IPv4 or IPv6 address. - Reason input — a short note for your own reference. - **Block** button.

> There are no separate "MANUAL" / "AUTO" badges in this table. The reason column tells you why each IP was blocked.

3.4.4 Allowed IPs (allowlist)

A permanent safelist of IPs that are **never** auto-banned by the brute-force protection. Useful for your office IP, your home IP, or a monitoring service.

- A button shows **your current visitor IP** ("Add my current IP") so you can one-click safelist yourself.
- Add an IP from the input — it accepts IPv4 and IPv6.
- **Remove** button per row (Pro).

When you add an IP that is currently blocked, the block is cleared at the same time.

3.5 Hardening tab

A grid of **hardening options**. Each is a card with the option name, a plain-English explanation, a risk badge (low / high), and a toggle switch. Some options have a small lock icon meaning they require Pro.

3.5.1 Essential hardening (free)

Eight options always visible:

- **Block Legacy Remote Access** (`disable_xmlrpc`) — closes the XML-RPC back door. Only keep off if you use the WordPress mobile app or older Jetpack.
- **Disable File Editor** (`disable_file_editor`) — removes the in-dashboard code editor.
- **Prevent Malware in Uploads** (`block_php_uploads`) — blocks the **execution** of `.php` files placed inside `wp-content/uploads/`. This rule applies broadly to the uploads directory. Some plugins (page builders, caching layers, e-commerce extensions) drop legitimate PHP helper files in or near `uploads/` and may behave incorrectly while this rule is active — there is no built-in per-plugin allowlist. If you notice broken functionality after enabling this option, disable it again or move the affected plugin's helpers out of `uploads/`.
- **Hide WordPress Fingerprints** (`hide_wp_version`) — strips WordPress version from headers, RSS, and HTML; blocks access to `readme.html` and `wp-config-sample.php`.
- **Hide Your Username List** (`block_user_enumeration`) — blocks the `?author=N` enumeration trick.
- **Restrict AI Crawlers to Homepage** (`restrict_llm_crawlers`) — adds a `robots.txt` entry blocking ChatGPT, Claude, Perplexity, Bing AI, and others from crawling beyond your homepage.
- **Restrict Google to Homepage Only** (`restrict_google_indexing`, high-risk) — adds `Disallow: /` for Googlebot and Bingbot for everything except `/`. WARNING: This removes your site from inner-page search results. The toggle shows a confirmation dialog before applying.

3.5.2 Advanced hardening (Pro)

Five more options:

- **Add Browser Security Rules** (`force_security_headers`, high-risk) — sends `X-Frame-Options`, `Content-Security-Policy`, `Strict-Transport-Security`, and friends. May prevent your site from being embedded in other websites. Requires confirmation.
- **Limit What Strangers Can See** (`disable_rest_api_guests`, high-risk) — blocks anonymous REST API access. Can break checkout, contact forms, and many plugins. Requires confirmation.
- **Hide Author Profile Pages** (`disable_author_archives`) — disables author pages (which leak admin usernames). Not recommended for multi-author blogs.
- **Block Aggressive Web Crawlers** (`block_bad_bots`) — blocks scraping bots (Ahrefs, Semrush, MJ12, etc.) at the firewall level. Does NOT affect Google or Bing.
- **Disable Visitor-Triggered Scheduling** (`disable_wp_cron_public`, high-risk) — disables WordPress's default cron-on-pageview behavior and blocks public access to `wp-cron.php`. You **must** set up a real server cron job first or your scheduled tasks (backups, scans) will stop firing. Requires confirmation.
- **Content Source Monitoring** (`enable_csp`) — Report-only Content Security Policy. Doesn't block anything; just collects violation reports.

3.5.3 Conflict / Confirmation dialogs

When you toggle on a high-risk option, the plugin first runs a **pre-toggle check** that scans your active plugins for known conflicts. For example:

- Turning on **Limit What Strangers Can See** while WooCommerce is active triggers a warning that checkout uses the REST API.
- Turning on **Disable Visitor-Triggered Scheduling** triggers a warning that you must add a server cron job first.

The dialog shows: - The conflict title and a plain-English description. - A list of affected plugins (if any). - A **suggested resolution** line. - Two buttons: **Cancel** (default) and a customized confirmation button (e.g. "I understand, enable anyway").

If you click the confirmation button, the option is applied and the dialog closes. The option stays on until you toggle it off.

3.5.4 Apply Recommended Level

A top-right button **Apply Recommended Level**. It calls a server-side helper that recommends a "security level" (Basic / Standard / Strict) based on: - Whether WooCommerce or another e-commerce plugin is active - Whether you have an active subscription/membership plugin - Whether multi-author roles exist

Clicking the button shows a preview dialog with the options that would be turned on, and asks you to confirm. Once you confirm, the plugin enables those options in one batch.

3.6 Cloud Shield tab

A summary tab for advanced cloud-tier protection. Shows your current Cloud Shield mode (Off / Observe / Block) and lets you change it. Cloud Shield is a Pro-only intermediate layer that handles edge-blocking for known-bad IPs maintained by the VPS Command Center.

If your license does not include this feature, the tab shows an "Upgrade to enable" placeholder.

3.7 History tab

A timeline of every scan that has run on your site:

Column	Meaning
Date	When the scan ran.
Type	`Sentinel Audit (L1)`, `Quick Scan`, `Full AI Scan`, or `Deep Malware Scan`.
Grade	A / B / C / D / F (only for AI scans).
Findings	Total findings (also broken down by severity in a tooltip).
Tier	The license tier at the time of the scan (`free`, `pro`, or `none`).

Click any row to open a detail panel that re-renders the full scan results from that point in history. The detail panel has a **Mark Safe** action per finding and a **Re-run** button.

---

4. SEO

(Hidden if you are in Standalone mode. Locked icon if you do not have the `seo_meta` capability.)

The SEO page has four cards.

4.1 SEO health scan

Click **Run SEO Scan**. The plugin examines every published post, page, product, and image:

- Counts how many have a meta title.
- Counts how many have a meta description.
- Counts how many have alt text (for images).
- Computes a **score** out of 100, with a **max achievable score** that excludes thin content (pages too short for AI to improve).

You see: - Per-content-type cards (Posts / Pages / Products / Images) with: total, missing, optimized, and **actionable** (the count that AI can realistically improve). - A **Non-compliant items** list — each row links to the post editor and shows the reason (`missing`, `short_content`, `below_threshold`).

4.2 Bulk meta generation (queue)

Click **Generate Missing Meta**. You can filter by content type, by post status, by category, and by language. The plugin then:

1. Queues every matching item.
2. Submits them as a **Groq batch job** for cheaper bulk processing (uses the `openai/gpt-oss-20b` model).
3. Shows a live progress bar with: total / completed / failed / pending counts, estimated minutes, last error message (if any).
4. Saves the generated titles + descriptions to each post's metadata.

You can **Stop** the queue at any time. Already-generated items are kept.

If WP-Cron is disabled on your site (some hosts disable it), the queue processes inline instead of via cron. A banner warns you about this.

4.3 On-Page Audit

A deeper SEO audit. Click **Run On-Page Audit**. The plugin examines a sample of your top posts and grades them against six factors (titles, descriptions, headings, internal links, images, content length). Returns:

- An overall **score**.
- Per-factor scores with **issues** listed (each with a "fix hint").
- A **Quick Wins** list — the highest-impact actions you can take.

4.4 FAQ generation

Click **Generate FAQs** on a post or page. Groq AI proposes 3–5 frequently-asked questions and answers based on your content, formatted as schema.org FAQPage JSON-LD. You can preview, edit, and apply.

4.5 Sitemap & llms.txt

- **Generate Sitemap** button — creates `sitemap.xml` at the root of your site, including AI-aware metadata (last-modified, image data, alt text).
- **Generate llms.txt** button — creates `/llms.txt`, the new convention that helps language models index your content cleanly. The file lists your key pages with summaries.

---

5. AI Content

(Hidden in Standalone mode. Locked if you do not have `content_rewrite`.)

The AI Content page lets you propose and apply AI-generated rewrites of your titles, descriptions, and short descriptions.

5.1 Content list

A paginated table of every post, page, product, image, and template. Columns: **Name**, **Type**, **Modified**, **Status icon**.

A search box filters by title. A type selector filters by content type. Click a row to open the detail panel.

5.2 Rewrite proposals

Inside an item's detail panel:

- **Original** column on the left — your current title, description, short description.
- **Proposed** column on the right — what the AI would change them to.
- A **Generate** button — calls Groq AI to refresh the proposal.
- **Apply** button — writes the proposal into the post.
- **Skip** button — discards the proposal.

Each item also shows when it was last rewritten (a small icon in the row).

5.3 Bulk apply

A **Bulk Apply** button at the top of the table accepts multiple selected rows and applies their proposals in one batch. Useful after a bulk Generate operation.

5.4 Restore previous version

If you applied a rewrite and want to roll back, the detail panel shows a **History** section with each previous version. Click **Restore** to revert. The plugin saves up to 5 historical versions per item.

---

6. Backup

The Backup page has three sub-sections (selectors at the top): **Backups**, **Move to New Host**, **Sync Two Sites**. The last two are Beta features and only fully unlock when **Settings → General → Beta Features** is turned on.

6.1 Backups section

6.1.1 Backup Control card

A panel with three actions:

- **Create Backup Now** — runs a full backup (database + files). A progress bar shows the current phase (`init`, `db_dump`, `archive_scan`, `archive_chunk`, `encrypt`, `upload_cloud`, `finalize`). The backup engine is **multi-tick** — it splits the work across many HTTP requests so it doesn't time out on shared hosting.
- **Scope** dropdown — **Full** (DB + files), **Database only**, or **Files only**.
- **Destination** dropdown — **Local**, **Google Drive**, **Dropbox**, **S3**, **Backblaze B2**, or **FTP**. Only destinations you have configured appear. Free users see only **Local**.
- **Cancel** button — appears while a backup is running. Stops the engine cleanly and rolls back any partial output.

A status banner appears in these cases: - "Slow backup detected (taking longer than usual)" — if the backup has run > 60 ticks without completing. - "Stuck jobs detected" — if previous backup engine state rows are still marked running for > 2 hours; you can click **Clear stuck jobs** to reset. - "WP-Cron disabled" — backups will not auto-schedule; manual backups still work.

6.1.2 Backup List

A table of every backup the plugin knows about. Each row is a **Backup Set** (one logical backup, possibly split into multiple ZIP files). Columns:

- **Name** — e.g. "Backup 2026-05-22 14:32".
- **Date** — when it completed.
- **Type** — Full / DB / Files.
- **Size** — human-readable total size.
- **Destination** — Local / GDrive / Dropbox / S3 / B2 / FTP.
- **Trigger badge** — Manual / Scheduled / Sentinel (triggered before a risky update).
- **Status badge** — Complete (green) / Failed (red) / Cancelled (gray) / Running (amber).
- Per-row actions: **Download** (local backups only), **Restore**, **Delete**.

When the plugin detects ZIP files on disk that no longer correspond to a Backup Set record, a yellow banner appears at the top of the Backup List with a **Clean up orphaned backup files** button. (The same cleanup action is also reachable from the Settings area as part of the backup-related maintenance controls.)

6.1.3 Backup Automations

A list of scheduled backup tasks. Each automation has:

- **Name** — free-text label you set.
- **Schedule** — Hourly / Twice Daily / Daily / Weekly.
- **Scope** — Full / DB / Files.
- **Destination** — same six options as manual backups.
- **Retention** — how many backups of this automation to keep (older ones auto-delete after each run).
- **Enabled** toggle.
- **Last Run** — time + status (success / failed / running).
- **Next Run** — scheduled time.

- **Run Now** — button to fire this automation immediately.
- **Edit** / **Delete** — modify or remove the automation.

A banner appears if `DISABLE_WP_CRON` is defined — automations won't fire and you need a real server cron job.

6.1.4 Cloud Storage panel

Configuration for each cloud destination. Each destination is its own card:

- **Google Drive** — Connect via OAuth. Click **Connect to Google Drive** → you are redirected to Google → you authorize → you return to the plugin. Status badge shows "Connected as `you@gmail.com`" or "Not connected". A **Disconnect** button revokes the token. You can also supply your own OAuth client ID + secret (for advanced users who want to use a private Google Cloud project instead of the plugin's shared client).
- **Dropbox** — same OAuth flow as Google Drive.
- **Amazon S3** — input fields for **Access Key ID**, **Secret Access Key**, **Bucket Name**, **Region**. **Test Connection** button. Credentials are encrypted at rest.
- **Backblaze B2** — input fields for **Application Key ID**, **Application Key**, **Bucket Name**. **Test Connection** button.
- **FTP / SFTP** — host, port, username, password, base directory. **Test Connection** button.

After a destination is configured, it appears in the Destination dropdown on the Backup Control card.

6.1.5 Restore a backup

Click **Restore** on any row in the Backup List. A confirmation dialog appears that summarizes: - What will be replaced (database, files, or both). - Estimated time. - A red warning that this will overwrite your current site.

After you confirm, the plugin: 1. Snapshots your current security settings (so they survive the import). 2. Downloads the backup (if it's in cloud storage). 3. Restores files (extracts the ZIP over your site). 4. Imports the database in chunks. 5. Re-registers all cron jobs. 6. Restores your security settings from the snapshot. 7. Recomputes your site's identity hash so the license stays valid.

The progress bar shows each step. If a step fails, the plugin logs the exact error and keeps the snapshot so nothing is lost.

6.2 Move to New Host (Migration — Beta)

Available only when **Beta Features** is enabled. Used for moving your site to a different domain or server.

Two modes:

Mode A — Direct (plugin-to-plugin). Both sites have SwissSuite installed. The export side prepares a **passport** (a metadata file describing the backup), generates download tokens for each archive (database SQL, theme, media, plugin files), and presents a one-step "send to destination" flow. The destination plugin pulls each archive in chunks, verifies the SHA-256 checksum, extracts, and imports.

Mode B — Receiver (standalone). Destination has no plugin yet. You download a small `swisswp-receive-XXXX.php` file and upload it to the destination's root. Open the file's URL, paste the export passport, and the receiver does the rest. The receiver auto-expires after 2 hours.

Either mode shows:

- **Preflight check** — disk space, PHP memory, time limit, ZipArchive available, WP-Cron OK, loopback HTTP test, recommended Sentinel mode (safe / standard / turbo) based on server load.
- **Go / No-Go** verdict — green = safe to proceed, red = hard blocker with explanation (e.g. "disk free < 10%").
- **Identity verification** — after import, the plugin compares database fingerprints (table count, post counts, theme, etc.) between source and destination and reports any discrepancies.
- **Include users** toggle — if off, the destination keeps its own user accounts (your admin password on the destination still works). If on, source users overwrite destination users.
- **Same-server optimization** — if the source and destination are detected to be on the same server, the plugin uses direct file copies instead of HTTP transfers (much faster).

6.3 Sync Two Sites (Beta)

Available only when **Beta Features** is enabled. Lets you keep a staging site and a live site in sync without doing full migrations.

- **Connections** — set up a paired site by URL. Both sites must have a sync key (auto-generated). The plugin signs every request with HMAC-SHA256.
- **Schedules** — pick a frequency (Hourly / Daily / Weekly) and a **scope** (posts, pages, products, templates). Each schedule runs on cron.
- **Manual push / pull** — buttons to push selected items to the remote site or pull them from it.
- **Compare** — shows which items differ. Each row links to a **Diff** view that previews the changes before you apply.
- **Inspect** — pulls a single item from the remote and shows its current state side-by-side with yours.
- **Status** — last run, items synced, partial / success / failed indicator.

Sync is **one-way per push** — you choose direction every time. There is no automatic two-way merge.

---

7. Settings

The Settings page has six tabs at the top: **General**, **AI Configuration**, **Security**, **SEO**, **License**, **Maintenance**.

All settings save automatically — there is no "Save Settings" button anywhere in the plugin. Toggles save on change; text fields save on blur.

7.1 General

The General tab has three cards:

- **General Preferences**
- **Automatic Updates** toggle — keep the plugin updated automatically.
- **Beta Features** toggle — unlocks the **Move to New Host** (Migration) and **Sync Two Sites** sub-sections of the Backup page. Off by default.
- **Server Profile** — three selectable cards: **Auto-Detect (Recommended)**, **Standard Hosting** (PHP chunking, tuned for shared hosts like Hostinger / Bluehost), or **VPS / Dedicated** (unlocks high-performance engines such as RSYNC and CLI when the server allows it). Affects chunk sizes and timing for backups and migrations.

The General tab also contains the **Custom SMTP** card (for sending plugin emails through your own SMTP relay). The recipient address for the daily Scan Report is configured separately in Section 3.2.4.

> The General tab does not contain an "API URL" field, a "Custom API URL" toggle, or a "Transfer Strategy" selector. The Command Center API endpoint is fixed and not user-configurable in the UI.

7.2 AI Configuration

A single card called **AI Agent**, with one action:

- **Test AI Connection** button — pings the SwissSuite VPS Bunker proxy to verify connectivity. Authentication is automatic via your active license — no API key is required and no model selector is exposed in the UI.

How AI requests are routed:

1. All AI calls go through the SwissSuite secure VPS proxy (the "Bunker"), which uses your license key to authorize the call.
2. On WordPress 7.0+, if you have configured your own LLM at the WordPress level via the new **WP Abilities API**, SwissSuite will prefer that endpoint and fall back to the VPS proxy when your endpoint is unavailable. You do not need to copy keys into SwissSuite — the plugin asks WordPress which AI provider to use.

7.3 Security

The Security tab is a stack of cards, in this order:

1. **Two-Factor Authentication** (Pro) — status, set-up, backup codes, disable. See **Section 8**.

2. **Backup Encryption** — choose the cipher (AES-256-GCM or XChaCha20-Poly1305), set or change the password, see the key-derivation parameters (PBKDF2 iterations) and the current cipher fingerprint. When a password is set, backup archives are written as `.zip.enc`. **If you lose this password, those backups cannot be recovered.**
3. **WPScan API Key** — optional. Paste your WPScan API token to add WPScan vulnerability lookups to the Deep Malware Scan. The field shows a "key set" badge once saved; you cannot read the saved value back (it is stored encrypted).
4. **Patchstack API Key** — optional. Same idea as WPScan, for the Patchstack vulnerability feed.
5. **Scan Capabilities** - **WordPress Core Integrity Check** toggle — when on, deep scans verify every WordPress core file against the official checksums and report any tampering. - **Abandoned Plugin Detection** toggle — daily check for plugins that WordPress.org has closed or removed (often an early signal of a security compromise or unpatched vulnerability).

> The **daily Sentinel Audit** does not have its own on/off toggle in this tab — it is bound to whether the daily Scan Report is enabled (see Section 3.2.4). The **Scan Report Email** address is also configured in Section 3.2.4 (not duplicated here).

7.4 SEO

A single card called **SEO Settings** with the subtitle "Control how your site appears when shared on social media".

- **Default Social Image** — a Media Library picker for the fallback Open Graph image used when a post has no featured image (your homepage, the blog listing, and posts without thumbnails). Recommended size 1200×630px. Selection and removal save **automatically** the moment you choose or remove an image — there is no Save button. A preview thumbnail is shown when an image is set.

The sitemap.xml and llms.txt files are generated from the **SEO** page (Section 4.5), not from this Settings tab.

7.5 License

- **License Key** field — paste your key here and click **Activate**. Activation contacts the Command Center, validates the key, locks it to your domain, and returns your capabilities + monthly token allowance.
- **No license? Start free** form — enter your email and click **Get Free License**. The Command Center creates a free, domain-locked license, emails you the key, and the plugin auto-activates it. If you reinstall later, the same email recovers the existing license rather than creating a duplicate.
- **Already paid? Manage subscription** — a small link below the activation form that opens the SwissSuite pricing/account page in a new tab.
- **License Status** card — shows tier name, expiry, token balance, monthly limit, and grace-period status (if any).
- **Trial badge** — when a Pro trial is active, a yellow "Trial Ends: " pill appears under the plan name.

- **Refresh License** button — forces a heartbeat to the Command Center to sync your latest plan changes.
- **Deactivate License** button — releases this domain so the key can be activated on another site. Use this **before** uninstalling on a site you are decommissioning.
- **Manage Billing** link (paid plans only) — appears as a small indigo card under the status panel. Opens the Stripe customer portal in a new tab so you can update payment, cancel, or download invoices. The link only shows when your account has a Stripe customer record and your tier is not "Free".

7.6 Maintenance

The Maintenance tab is a stack of cards focused on housekeeping. If your site has `DISABLE_WP_CRON` set in `wp-config.php`, a yellow warning banner appears at the top reminding you that scheduled tasks (backups, scans, sync) won't fire on their own.

- **Maintenance Tools** — four one-click actions, each with a confirmation prompt:
- **Clear Transients** — removes expired temporary data from the database.
- **Delete Post Revisions** — removes old post revision history to save space.
- **Delete Spam Comments** — permanently deletes all comments marked as spam.
- **Optimize Database Tables** — runs SQL `OPTIMIZE` on all site tables to reclaim disk space.
- **Database Cleanup** — six one-click actions for orphaned data:
- **Clean Orphaned Post Meta** — removes metadata left behind by deleted posts.
- **Clean Orphaned Comment Meta** — removes metadata left behind by deleted comments.
- **Empty Trash** — permanently deletes posts and pages currently in the trash.
- **Delete Auto-Drafts** — removes auto-draft posts created when opening the editor without publishing.
- **Clean Orphaned Term Relationships** — removes category/tag associations pointing to posts that no longer exist.
- **Drop Orphaned Tables** — drops database tables left behind by uninstalled plugins. Core tables and tables belonging to active plugins are never touched. **Back up your database first.**
- **Cache Management** — a single **Clear Site Cache** button. The card automatically detects what caching layers are present and shows them inline — for example "WordPress Object Cache · Redis · OPcache: Active". Clearing has a built-in cooldown so you cannot hammer the button.
- **System Logs** — a scrollable, color-coded view of recent debug log entries. The view refreshes **live every 5 seconds** and can also be refreshed on demand with the circular-arrow button. If you contact support, copy and paste the relevant entries.

---

8. Two-Factor Authentication (2FA)

Found in **Settings → Security → Two-Factor Authentication**. 2FA is gated by the `2fa` capability — it is available on Pro plans that include that capability and is **not** part of the free baseline.

Enabling 2FA

1. Click **Set up 2FA**. The plugin generates a TOTP secret.
2. Scan the **QR code** with an authenticator app: Google Authenticator, Authy, 1Password, Bitwarden, Microsoft Authenticator — anything TOTP-compatible.
3. Enter the **6-digit code** from your app into the verification field.
4. Click **Verify**. The plugin shows 10 **backup codes**. Copy them somewhere safe.
5. Click **Done**. 2FA is now required on every login.

Logging in with 2FA

After username + password, you are prompted for the 6-digit code from your app. If you lost your phone, type one of your backup codes instead (each is single-use).

Regenerate backup codes

If you used your backup codes or want a fresh set, open the 2FA section and click **Regenerate Backup Codes**. Old codes are invalidated immediately.

Disable 2FA

Click **Disable 2FA**. You must enter a current code from your app (or a backup code) to confirm. Once disabled, the QR code and secret are deleted.

Important notes

- 2FA only applies to the WordPress admin login screen — not REST API requests (which use nonces) or programmatic logins.
- The TOTP secret is encrypted at rest using your site's `AUTH_KEY` + `SECURE_AUTH_KEY` salts (so even if your database leaks, the secret is unreadable without your `wp-config.php`).

---

9. License, Tokens, and Free Mode

What a license unlocks

- A "capability" is a string flag like `seo_meta`, `backup_cloud`, `geoblocking`. Each Pro feature checks for its capability before letting you use it.
- Every site starts with the **same six baseline capabilities**, with or without a license: `scan_basic`, `reports`, `threat_block_basic`, `dashboard_access`, `backup_local`, `firewall_basic`.
- **Activating a Free license** adds the daily Scan Report email and a 50,000 AI-token allowance per month. It does **not** add any other capabilities — `2fa`, `hardening`, `seo_meta`, AI content rewriting, etc. all require a paid plan.
- **Activating a paid license** adds tier-specific capabilities on top of the baseline.

Plan tiers

- **No license** — baseline only. Quick Scan, Sentinel Audit on demand, essential hardening, basic WAF, manual local backups. No daily report email, no AI tokens.
- **Free** — domain-locked, no payment. Same baseline + daily Scan Report email + 50,000 AI tokens / month.
- **Security tier** ("fortress" plans) — adds `sentinel_pro`, `waf`, `advanced_waf`, `geoblocking`, `advanced_malware`, `auto_quarantine`, `files_monitor`, `2fa`, `hardening`, `rate_limiting`, plus AI access.
- **SEO tier** — adds `seo_meta`, `seo_advanced`, `sitemap`, `broken_links`, `page_speed`.
- **Content tier** — adds `content_rewrite`, `blog_generation`, `product_descriptions`, `meta_ai`.
- **Suite ("swisswpsuite")** — everything.
- **Pro (legacy generic name)** — also maps to the full feature set.

Token economy

- Every AI call (Deep Scan AI analysis, SEO meta generation, content rewriting, FAQ generation, "Check with AI" on findings) deducts tokens from your monthly balance.
- The Sentinel Audit and Quick Malware Scan **do not** use AI and are therefore free.
- Tokens reset on your billing date — they **do not roll over**. Unused tokens are lost.
- The token balance is shown only in **Settings → License** (it is not shown on the main Dashboard). If you run out, AI features show "Out of tokens — upgrade or wait for reset".

Domain locking

- Each license key is bound to one domain (`example.com`). Trying to activate the same key on a different domain returns a **DOMAIN_LOCKED** error with a clear message: "go to the original site, click Deactivate License first".
- If you migrate to a new domain, deactivate on the old site and reactivate on the new one. Deactivation is instant.

Grace period

- If the Command Center is unreachable during a daily license check (network error, 429 rate limit, 5xx errors), the plugin enters a **72-hour grace period** (three days) rather than immediately downgrading. Your features keep working during this window.
- If the Command Center explicitly returns `valid: false`, the plugin downgrades to the no-license baseline immediately — there is no grace period for explicit rejection.
- The grace period applies to any active tier (free or paid) — it covers the case where the Command Center is unreachable, not the case where the server explicitly says the license is invalid.

---

10. Status Indicators, Badges, Colors, and Icons

Indicator	Meaning
Green badge / dot	All good. Last action succeeded.
Amber / yellow badge	Warning. Not broken, but needs attention.
Red badge / dot	Error. Action failed or critical issue present.
Gray badge	Not run, not configured, or feature disabled.
Lock icon next to a sidebar item	Your license does not include this feature.
Lock icon on a toggle	Toggle requires Pro.
Beta badge (amber, flask icon)	Feature is in active testing.
Trial pill under logo	Pro trial is active (the trial end date itself is shown in Settings → License).
`?` grade pill	Scan finished but grade unavailable (AI did not return).
A / B / C / D / F grade	A = excellent, F = critical. From the Deep Malware Scan.
Severity row colors in findings	Red = critical, orange = high, yellow = medium, gray = low, blue = info.
Source pills on findings	`Hash DB` (cloud lookup), `Pattern` (local regex), `WPScan`, `Patchstack`, `AI`.
Status pills on findings	`ok` (green), `degraded` (amber), `unavailable` (gray).
`cron_blocked` banner	`DISABLE_WP_CRON` is on. Scheduled tasks may not fire.
"Slow backup" banner	Backup engine has run > 60 ticks. Often harmless.
Persistent admin notice (yellow) at top of WP-Admin	Last daily report email failed to send. Clears on next success.

11. Troubleshooting

"Network error" when activating a license

Cause: the Command Center is unreachable, or your host blocks outbound HTTPS to `api.swisswpsecure.com`. Fix: 1. **Settings → AI Configuration → Test AI Connection** — if this also fails, your host blocks outbound HTTPS. Contact your host or whitelist the domain. 2. Try again in 5 minutes — the Command Center may be rate-limiting (429). The plugin will treat this as a transient error and enter grace period; your features keep working for up to 72 hours.

"Domain lock" error during activation

Your license key is already activated on another domain. Go to that other site, open **Settings → License**, click **Deactivate License**, then try activating again on this site.

"Failed to send daily report email"

Cause: PHP's `wp_mail()` is failing on your host. Fix: 1. Go to **Settings → General → Custom SMTP** and configure custom SMTP (host, port, username, password, from address). 2. Send a test email. Check the diagnostics output for the exact SMTP error. 3. Common fix: most hosts require an authenticated SMTP relay (Mailgun, SendGrid, your hosting provider's SMTP, or Gmail with app password).

Backup "Stuck" / running forever

Cause: a previous backup tick crashed and the engine state is still marked `running`. Fix: 1. Go to **Backup → Backups** → click **Clear stuck jobs**. 2. Try the backup again. If it stalls in the same phase repeatedly, lower the chunk size by setting **Settings → General → Server Profile** to **Standard Hosting**.

Scan finds malware in the plugin's own files

This was a known bug fixed in v2.9.30.73. Update to the latest version. The fix makes the safe-folder check walk ancestor directories correctly so the plugin's own security classes are not flagged.

Sidebar items are locked even after activating Pro

The capabilities list is cached in `window.swisswpsuiteData`. Hard-reload the page (Ctrl+F5 or Cmd+Shift+R). If still locked, go to **Settings → License → Refresh License** to force a heartbeat with the Command Center.

"All clear" but I think I am hacked

The Sentinel Audit (L1) is heuristic. Run the **Deep Malware Scan** (Pro) for hash-database, vulnerability-feed, and AI confirmation. If the result is still clean and you still suspect a compromise, restore from a clean backup taken before the suspected event.

Restore failed mid-import / site looks broken

The plugin always takes a **safety snapshot** before an import begins. The snapshot is saved to disk and survives even a full database wipe. If a restore fails: 1. Refresh the SwissSuite admin page — the post-import recovery routine auto-runs. 2. If still broken, go to **Backup → Backups** and restore an earlier backup (the snapshot will be used to bring back your security settings).

"Banned IPs wiped after plugin update"

This was a v2.9.28.07 emergency-WAF-unlock bug that was fixed in v2.9.30.85. Update to the latest version. The migration that was wiping bans now has a one-shot guard and never fires again on existing installs.

WP-Cron disabled — features stop firing

If you (or your host) set `DISABLE_WP_CRON` in `wp-config.php`, scheduled backups, daily scans, and daily reports stop firing. The plugin shows a yellow banner at the top of affected pages. Fix: 1. Either remove `DISABLE_WP_CRON` from `wp-config.php`, or 2. Add a real server cron job: `*/5 * * * * curl -s https://yoursite.com/wp-cron.php?doing_wp_cron`.

Other strange behavior

Open **Settings** → **Maintenance** → **System Logs**. Recent entries are shown live (refreshing every 5 seconds), color-coded by severity. Each entry includes timestamp, severity, module, message, memory usage, and load average. If you contact support, copy and paste the relevant entries.

This manual covers SwissSuite v2.9.30.88. For the technical / developer manual, see `docs/manuals/TECHNICAL_MANUAL.md`.