



TW Security Toolkit User Guide

Prepared by: Technology Wisdom

Version 1.0

Table of Contents

1. Introduction.....	4
2. Features.....	4
3. Installation Guide.....	5
3.1. Method 1 — Upload Plugin ZIP.....	5
3.2. Method 2 — Manual Installation.....	6
4. Setup Guide.....	6
4.1. Getting Started.....	6
4.2. Authentication & Login Security.....	7
4.2.1. Login Alert & Tracker.....	7
4.2.2. Secure Login Path.....	8
4.2.3. Failed Login & Brute Force Protection.....	9
4.2.4. IP Blacklist.....	10
4.2.5. Login OTP & Role Policies.....	11
4.2.6. Login History by User.....	13
4.3. Content Workflow.....	14
4.3.1. Post Modifier Tracker.....	14
4.3.2. Post Approval Notifier.....	15
4.3.3. CPT Revisions.....	17
4.3.4. Link Expiration.....	19
4.4. Site Protection.....	20
4.4.1. Disable File Editor.....	20
4.4.2. File Change Detection.....	21
4.4.3. Security Health Check.....	22
4.4.4. Upload Guard.....	24
4.5. Monitoring & Alerts.....	25
4.5.1. Complete Audit Log.....	25
4.5.2. Suspicious Activity Detection.....	26
4.5.3. Email & Slack / Discord Notifications.....	28
4.5.4. Scheduled Security Reports.....	29
4.5.5. Automated Emails.....	30
5. How to View Stats?.....	31
6. Frequently Asked Questions (FAQs).....	33
7. Troubleshooting.....	35
7.1. Dashboard Shows Little or No Activity.....	35
7.2. Secure Login Path Not Working.....	35
7.3. Brute Force Lockouts.....	35
7.4. Health Check Cannot Run.....	35
7.5. File Change Alerts After Updates.....	35

7.6. Notifications Not Arriving.....	36
8. Best Use Cases.....	36
8. Conclusion.....	36

1. Introduction

The TW Security Toolkit helps site owners protect WordPress logins, harden the site, control content workflows, and monitor important security activity from one place.

The plugin is designed for:

- WordPress sites that need stronger login protection
- Sites that want to hide the default login URL
- Teams that need content approvals and edit tracking
- Stores and blogs that must limit risky uploads
- Agencies and site owners who want a clear security score and alerts

Using this plugin, site owners can:

- Hide the default WordPress login page behind a custom URL
- Track successful logins and send login alert emails
- Block repeated failed logins and lock risky IPs
- Block selected visitor IPs
- Require an email one-time code (OTP) at login
- Disable the theme and plugin file editors
- Limit uploads by size, type, and image dimensions
- Track who last edited posts and pages
- Expire links by date or click count
- Control revisions for custom post types
- Notify admins when content is published
- Hold drafts until an administrator approves them
- Run a security health check and improve the security score
- Watch important files for unexpected changes
- Keep a full audit log of key site actions
- Detect suspicious activity
- Send alerts by email, Slack, or Discord
- Receive daily, weekly, or monthly security reports

Important: Activating the plugin does **not** turn any tool on automatically. Every tool stays Off until you turn it On from the Dashboard or Settings.

2. Features

1. **Login Alert & Tracker:** Record each user's last login time and optionally email the site admin after a successful login.

2. **Secure Login Path:** Hide the default WordPress login URL ([wp-login.php](#)) behind a custom slug such as [/mylogin](#).
3. **Failed Login & Brute Force Protection:** Lock an IP after too many failed password attempts within a set time window.
4. **IP Blacklist:** Block selected visitor IPs with a 403 Access denied response.
5. **Login OTP & Role Policies:** Require a 6-digit email code after password login, with optional role-based limits.
6. **Login History by User:** Review successful logins, failed logins, and logouts with filters for user, IP, status, and date.
7. **Post Modifier Tracker:** Show who last modified posts, pages, products, and public custom post types.
8. **Post Approval Notifier:** Email the administrator when another user publishes content.
9. **Draft Approval:** Hold writer posts as drafts until an administrator publishes them.
10. **CPT Revisions:** Enable or disable WordPress revisions per custom post type.
11. **Link Expiration:** Expire content by date/time and/or max clicks, then move it to Draft.
12. **Disable File Editor:** Block Theme File Editor and Plugin File Editor in wp-admin.
13. **File Change Detection:** Watch core, admin, includes, themes, plugins, and mu-plugins for unexpected file changes.
14. **Security Health Check:** Run a scan, get a score out of 100, and follow clear fix recommendations.
15. **Upload Guard:** Limit uploads by file size, MIME type, and image dimensions per role (including Guest).
16. **Complete Audit Log:** Record important site actions and export filtered results as CSV or PDF.
17. **Suspicious Activity Detection:** Detects unusual patterns such as rapid failed logins or new administrator accounts.
18. **Email & Slack / Discord Notifications:** Send security alerts to email and webhook channels.
19. **Scheduled Security Reports:** Send daily, weekly, or monthly email summaries.
20. **Security Dashboard:** View score, security level, top IPs, and recent activity in one overview.

3. Installation Guide

3.1. Method 1 — Upload Plugin ZIP

1. Log in to your WordPress admin dashboard.
2. Go to Plugins > Add New.
3. Click Upload Plugin.
4. Select the Security Toolkit plugin ZIP file.
5. Click Install Now.
6. After installation, verify your plugin license and click the Activate Plugin button to complete the activation process.

Quick Tip: You can download your plugin ZIP file at any time via the following:

- The **purchase confirmation email** has been sent to your inbox.
- Your personal **Freemius account** dashboard.

3.2. Method 2 — Manual Installation

1. Place the plugin Zip file in: /wp-content/plugins/
2. Extract the plugin ZIP file.
3. Log in to WordPress Admin.
4. Go to Plugins.
5. After file upload, verify your plugin license and click the Activate Plugin button to complete the activation process.

4. Setup Guide

4.1. Getting Started

Access Plugin Settings:

- Log in to WordPress Admin.
- Navigate to: **TW Security Toolkit > Dashboard**
- Use **Settings** or each module's **Configure** tab to turn tools On and save options.

Default Behavior:

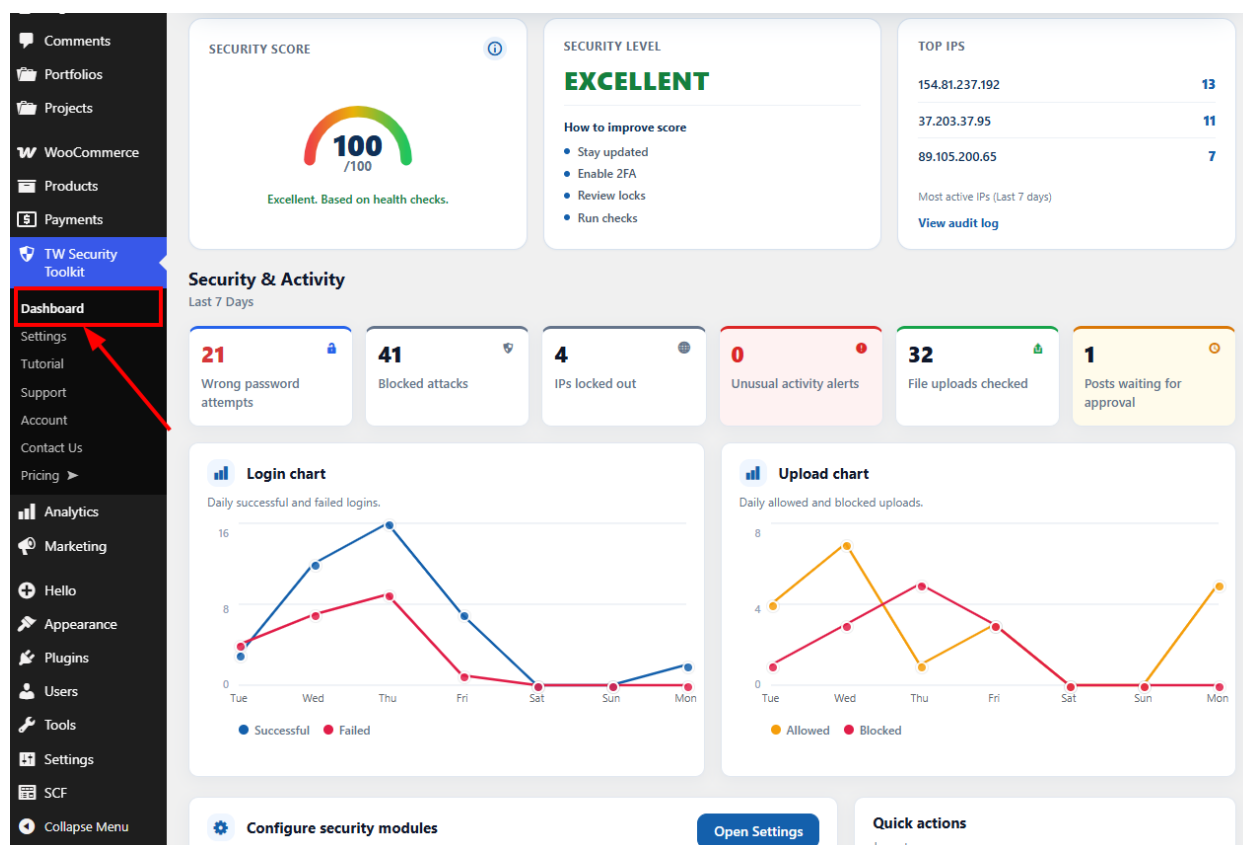
By default:

- All tools remain Off after activation.
- No login, upload, file, or content restrictions are applied until you turn a tool On and save its settings.
- The Dashboard shows an overview only after related tools start recording activity.

Recommended first steps:

1. Open the Dashboard and review the Security Score / Security Level cards.
2. Turn On **Audit Log** so activity can appear in reports and detail pages.
3. Turn On the login tools you need (Secure Login Path, Brute Force, Login Alert).
4. Run **Security Health Check** and follow the recommendations.

Backend Screenshot:



4.2. Authentication & Login Security

Access this module from:

- **TW Security Toolkit > Authentication**
- Or open each feature from Settings / Configure

4.2.1. Login Alert & Tracker

Login Alert & Tracker records last login times and can email the site admin after successful logins.

How It Works

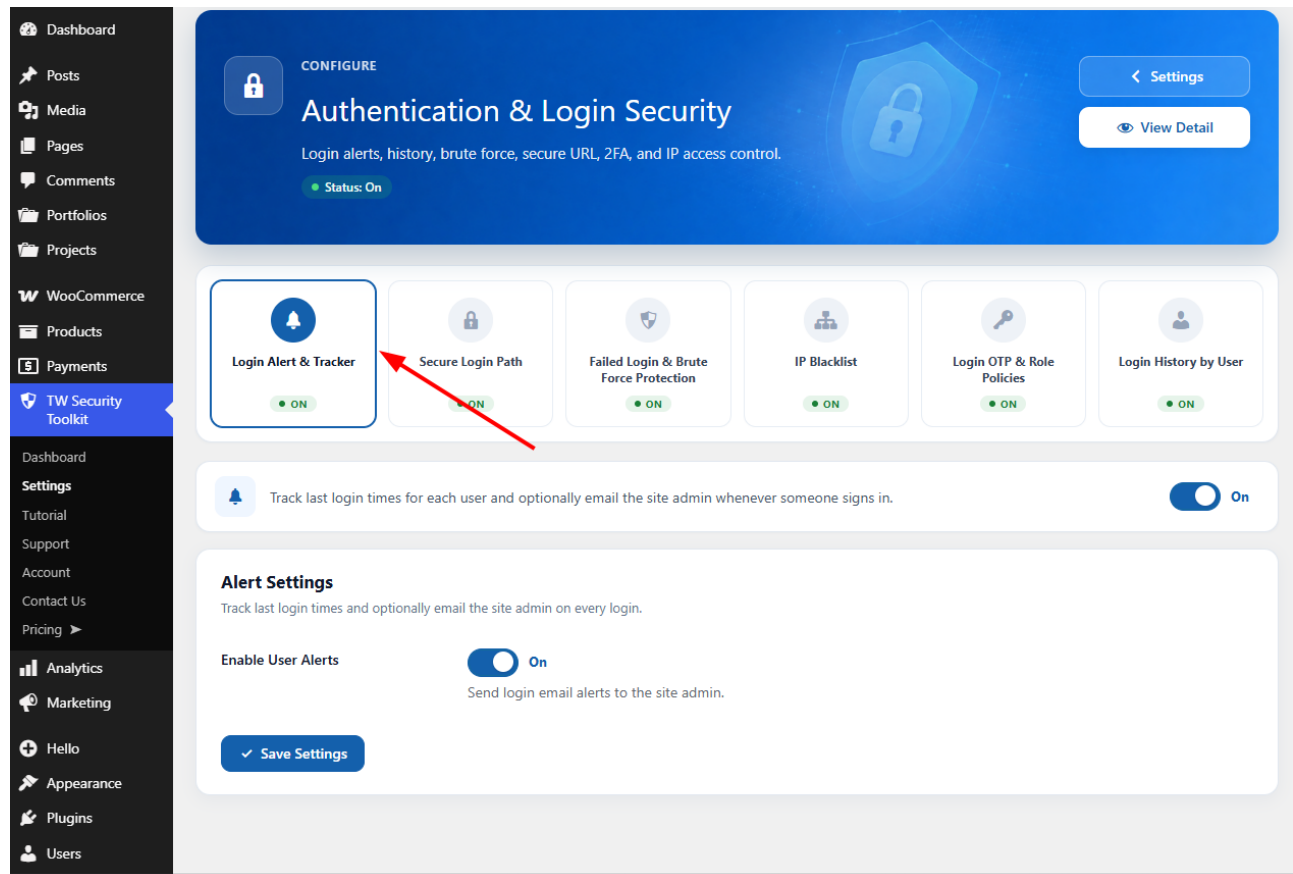
When enabled:

- Each successful login updates the user's last login time.
- An optional alert email can be sent to the site admin.
- A **Last Login** column appears in the Users list.

Steps to Enable

1. Turn **Login Alert & Tracker** On.
2. Enable login email alerts if needed.
3. Save settings.

Backend Screenshot:



4.2.2. Secure Login Path

Secure Login Path hides the default WordPress login URL behind a custom slug.

This helps reduce automated attacks that target `/wp-login.php` and `/wp-admin`.

How It Works

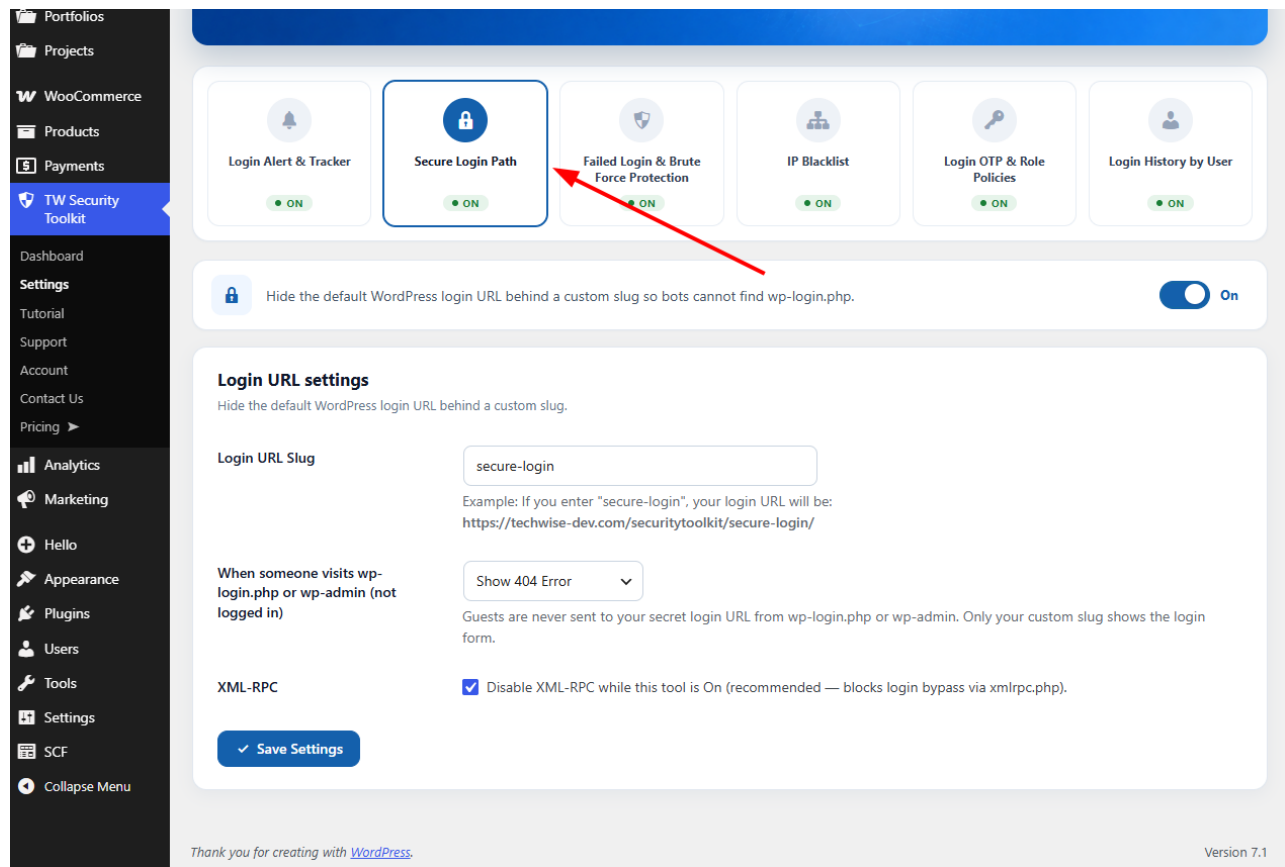
When enabled:

- Guests who open `wp-login.php` or `wp-admin` see a 404 page or are redirected to the home page (your choice).
- Only your custom login slug shows the login form.
- Guests are never redirected to the secret login URL.

Steps to Enable

1. Turn **Secure Login Path** On.
2. Set the custom login slug.
3. Choose old-URL behavior (404 or redirect home).
4. Save settings.
5. Go to **Settings > Permalinks > Save Changes**.
6. Bookmark the new login URL in a safe place.

Backend Screenshot:



4.2.3. Failed Login & Brute Force Protection

Brute Force Protection locks an IP after too many failed password attempts.

How It Works

When enabled:

- Failed logins are counted per IP inside your chosen time window.
- When the limit is reached, the IP is locked for the lockout period.

- A successful login clears the fail counter for that IP.
- Currently locked IPs can be unlocked from Settings.

Steps to Enable

1. Turn **Failed Login & Brute Force Protection** On.
2. Set max attempts, time window, and lockout length.
3. Save settings.
4. Review locked IPs and unlock any trusted address if needed.

Careful: If your own IP is locked, unlock it from Settings.

Backend Screenshot:

The screenshot displays the TW Security Toolkit interface. On the left, a dark sidebar contains navigation links: Media, Pages, Comments, Portfolios, Projects, WooCommerce, Products, Payments, TW Security Toolkit (active), Dashboard, Settings, Tutorial, Support, Account, Contact Us, Pricing, Analytics, Marketing, Hello, Appearance, Plugins, Users, Tools, Settings, and SCF. The main content area features a row of six security settings cards, each with an icon, title, and status (ON/OFF). A red arrow points to the 'Failed Login & Brute Force Protection' card, which is highlighted with a blue border. Below this row is a toggle switch for 'Monitor failed logins and automatically lock IPs after too many attempts so brute-force attacks are blocked.', currently set to 'On'. The 'Lockout settings' section follows, with a description 'Automatically lock IPs after too many failed login attempts.' and three input fields: 'Max failed attempts' (2), 'Window (minutes)' (15), and 'Lockout (minutes)' (2). A 'Save Settings' button is located below these fields. The 'Currently locked IPs' section contains a table with the following data:

IP	Unlocks at	
182.178.252.141	2026-09-15 05:02:54	<button>Unlock</button>

4.2.4. IP Blacklist

IP Blacklist blocks visitors whose IP addresses appear on your list.

How It Works

When enabled:

- Listed visitor IPs receive a 403 Access denied response.
- Logged-in administrators are never blocked.
- You cannot blacklist your own current IP.

Steps to Enable

1. Turn **IP Blacklist** On.
2. Turn **Block listed IPs** On.
3. Paste one IP per line.
4. Save settings.

Example format:

203.0.113.10
198.51.100.22
192.0.2.55

Backend Screenshot:

The screenshot displays the TW Security Toolkit interface. On the left is a dark sidebar with navigation links: WooCommerce, Products, Payments, TW Security Toolkit (highlighted), Dashboard, Settings, Tutorial, Support, Account, Contact Us, Pricing, Analytics, Marketing, Hello, Appearance, Plugins, Users, Tools, Settings, SCF, and Collapse Menu. The main content area has a top row of six feature toggles: Login Alert & Tracker, Secure Login Path, Failed Login & Brute Force Protection, IP Blacklist (highlighted with a red box and a red arrow), Login OTP & Role Policies, and Login History by User. Below these is a toggle for 'Block visitors by IP address with a blacklist you manage from this page.' which is turned 'On'. A 'How to use' section explains that the tool blocks visitors whose IP addresses appear on the blacklist, while logged-in administrators are never blocked. It provides instructions on how to use the tool and an example format for the blacklist: '203.0.113.10 / 198.51.100.22 / 192.0.2.55'. The 'IP blacklist' section shows a text input field labeled 'Blacklist IPs' containing the IP address '23.106.249.52', with a red arrow pointing to it. A note at the bottom states 'One IP per line. Your current IP cannot be blacklisted.'

4.2.5. Login OTP & Role Policies

Login OTP adds a second step after password login using a 6-digit email code.

How It Works

When enabled:

- After a correct password, an OTP email is sent.
- The user must enter the code on the login form.
- You can require OTP for all users, administrators only, or selected roles.
- Optional role policies can limit extra actions (for example uploads).
- Administrators are never limited by the optional role policies.

Steps to Enable

1. Turn **Login OTP & Role Policies** On.
2. Choose the Email OTP scope.
3. Optionally enable role policies.
4. Save settings.
5. Test login: password → email code → enter code.

Backend Screenshot:

The screenshot displays the WordPress dashboard with the TW Security Toolkit settings. The left sidebar contains the following menu items: Dashboard, Posts, Media, Pages, Comments, Portfolios, Projects, WooCommerce, Products, Payments, TW Security Toolkit (highlighted), Dashboard, Settings, Tutorial, Support, Account, Contact Us, Pricing, Analytics, Marketing, Hello, Appearance, Plugins, Users, and Tools. The main content area shows the 'Login OTP & Role Policies' settings. The 'Login OTP & Role Policies' widget is highlighted with a blue border and a red arrow. Below it, the 'Email OTP at login' section is visible, showing a toggle switch for 'Require an email one-time code at login, plus optional per-role limits for uploads, plugins, and idle sessions.' The 'Email OTP at login' section includes a description: 'After a correct password, a 6-digit code is emailed to the user. They enter it on the WordPress login page to finish signing in.' The 'Who gets Email OTP' section has three radio button options: 'All users (recommended)', 'Administrators only', and 'Selected roles only' (selected). Below this, the 'Used when "Selected roles only" is chosen:' section lists roles with checkboxes: Administrator, Editor, Author, Contributor, Subscriber, Customer, and Shop manager (checked). The 'Extra role policies' section is also visible, showing a table with roles and a toggle for 'Disable uploads'.

Role	Disable uploads
Editor editor	☐
Author author	☐

4.2.6. Login History by User

Login History shows successful, failed, and logout events in one place.

How It Works

When enabled:

- Login-related events are listed with user, IP, status, and date.
- You can filter by username, IP, status, and date range.

Steps to Enable

1. Turn **Login History by User** On.
2. Review Login History table to monitor login activity.
3. Optionally use filters to review login activity.

Backend Screenshot:

The screenshot displays the TW Security Toolkit interface. On the left is a dark sidebar with navigation links: Dashboard, Posts, Media, Pages, Comments, Portfolios, Projects, WooCommerce (Products, Payments), TW Security Toolkit (highlighted), and a section for Analytics, Marketing, Hello, Appearance, Plugins, and Users. The main content area features a top row of six toggle switches: Login Alert & Tracker (ON), Secure Login Path (OFF), Failed Login & Brute Force Protection (ON), IP Blacklist (ON), Login OTP & Role Policies (ON), and Login History by User (ON, highlighted with a red box and a red arrow). Below this is a section titled 'Review login, failed attempt, and logout history per user or IP, then filter results by date and status.' with a toggle switch set to 'On'. Underneath are filter fields for User, IP, Status (set to 'All'), From, and To dates, followed by a 'Filter' button. The 'Login history' section shows '98 login events' and a table with the following data:

Time	Type	Priority	User	IP	Message
2026-09-15 05:03:36	login_success	info	securitytoolkit_admin_abdullah_2	23.106.249.52	User securitytoolkit_admin_abdullah_2 logged in.
2026-09-15 05:01:12	login_failed	warning	securitytoolkit_admin_abdullah_2	182.178.252.141	Failed login attempt for securitytoolkit_admin_abdullah_2.
2026-09-15 05:00:54	login_failed	warning	securitytoolkit_admin_abdullah_2	182.178.252.141	Failed login attempt for securitytoolkit_admin_abdullah_2.
2026-09-15 05:00:43	login_failed	warning	securitytoolkit_admin_abdullah_2	182.178.252.141	Failed login attempt for securitytoolkit_admin_abdullah_2.
2026-09-15 04:52:40	login_success	info	securitytoolkit_admin_abdullah	182.178.252.141	User securitytoolkit_admin_abdullah logged in.
2026-09-15 04:52:31	logout	info	securitytoolkit_admin	182.178.252.141	User securitytoolkit_admin logged out.
2026-09-14 09:37:37	logout	info	securitytoolkit_hussain	182.178.252.141	User securitytoolkit_hussain logged out.
2026-09-14 09:34:27	login_success	info	securitytoolkit_hussain	182.178.252.141	User securitytoolkit_hussain logged in.
2026-09-14 09:32:52	login_success	info	securitytoolkit_admin_abdullah	182.178.252.141	User securitytoolkit_admin_abdullah logged in.

4.3. Content Workflow

Access this module from:

- **TW Security Toolkit > Content Workflow**

4.3.1. Post Modifier Tracker

Post Modifier Tracker shows who last modified content in the admin lists.

How It Works

When enabled:

- The last modifier is stored when content is updated.
- List tables show a Last Modified column with date, time, and user.

Steps to Enable

1. Turn **Post Modifier Tracker** On.
2. Open Posts, Pages, or custom post type lists.
3. Review the Last Modified column.

Backend Screenshot:

Post Modifier Tracker ON

Post Approval Notifier ON

CPT Revisions ON

Link Expiration ON

Show who last modified posts, pages, products, and custom types directly in the admin lists. On

How it works

1 New posts and pages created LAST 24 HOURS

1 Posts and pages updated LAST 24 HOURS

Content change activity Open Audit Log

Recent content create/update events from the audit log.

Time	Type	Priority	User	IP	Message
2026-09-15 05:19:36	content_updated	info	securitytoolkit_admin_abdullah	182.178.252.141	portfolio "Portfolio 5" was updated.
2026-09-15 05:18:44	content_created	info	securitytoolkit_admin_abdullah	182.178.252.141	portfolio "Portfolio 5" was created.
2026-09-11 04:45:55	content_updated	info	securitytoolkit_admin_abdullah_2	89.105.200.65	securitytoolkit_admin_abdullah_2 updated page "Page 1".
2026-09-11 04:39:16	content_updated	info	securitytoolkit_admin_abdullah_2	89.105.200.65	securitytoolkit_admin_abdullah_2 updated project "Project 1".

Portfolios Add Portfolio

All (6) | Mine (1) | Published (4) | Drafts (2)

Bulk actions Apply All dates Filter Search Portfolios

6 items

Title	Categories	Date	Last Modified
☐ Test Portfolio	—	Published 2026/09/15 at 5:18 am	September 15, 2026 5:42 am by Abdullah Dilshad
☐ Portfolio 1	—	Published 2026/09/10 at 5:03 am	September 10, 2026 5:04 am by Abdullah TW
☐ Title	Categories	Date	Last Modified

6 items

4.3.2. Post Approval Notifier

Post Approval Notifier emails the administrator when another user publishes content.

How It Works

When enabled:

- Publish events can trigger a customized email.

- You can choose post types and excluded roles.
- Optional Draft Approval can hold writer posts until an admin publishes them.

Steps to Enable

1. Turn **Post Approval Notifier** On.
2. Open **Configure**.
3. Enable publish alerts and/or Draft Approval.
4. Choose post types and excluded roles.
5. Save settings.

Backend Screenshot:

The screenshot shows the WordPress dashboard with the TW Security Toolkit plugin settings. The left sidebar contains the following menu items: Posts, Media, Pages, Comments, Portfolios, Projects, WooCommerce, Products, Payments, TW Security Toolkit (highlighted), Dashboard, Settings, Tutorial, Support, Account, Contact Us, Pricing, Analytics, Marketing, Hello, Appearance, and Plugins. The main content area displays four status cards: Post Modifier Tracker (ON), Post Approval Notifier (ON, highlighted with a red box and a red arrow), CPT Revisions (ON), and Link Expiration (ON). Below these cards is a toggle switch for 'Email the site administrator when other users publish content, with optional draft approval before posts go live.' (ON). The 'Admin Notifications' section is expanded, showing options to 'Notify site admin when' (checked for 'Post is published') and 'Excluded User Roles' (Editor, Author, Contributor, Subscriber, Customer, Shop manager). The 'Plugin Information' section on the right provides details about the plugin's functionality and lists available variables for email notifications.

Post Approval Notifier (ON)

Email the site administrator when other users publish content, with optional draft approval before posts go live. **ON**

Admin Notifications

Choose when the site administrator receives an email. Administrators never trigger these alerts.

Notify site admin when ☒ Post is published

This applies when Draft Approval is off. Approval drafts always notify the site administrator once.

Excluded User Roles

- ☐ Editor
- ☐ Author
- ☐ Contributor
- ☐ Subscriber
- ☐ Customer
- ☐ Shop manager

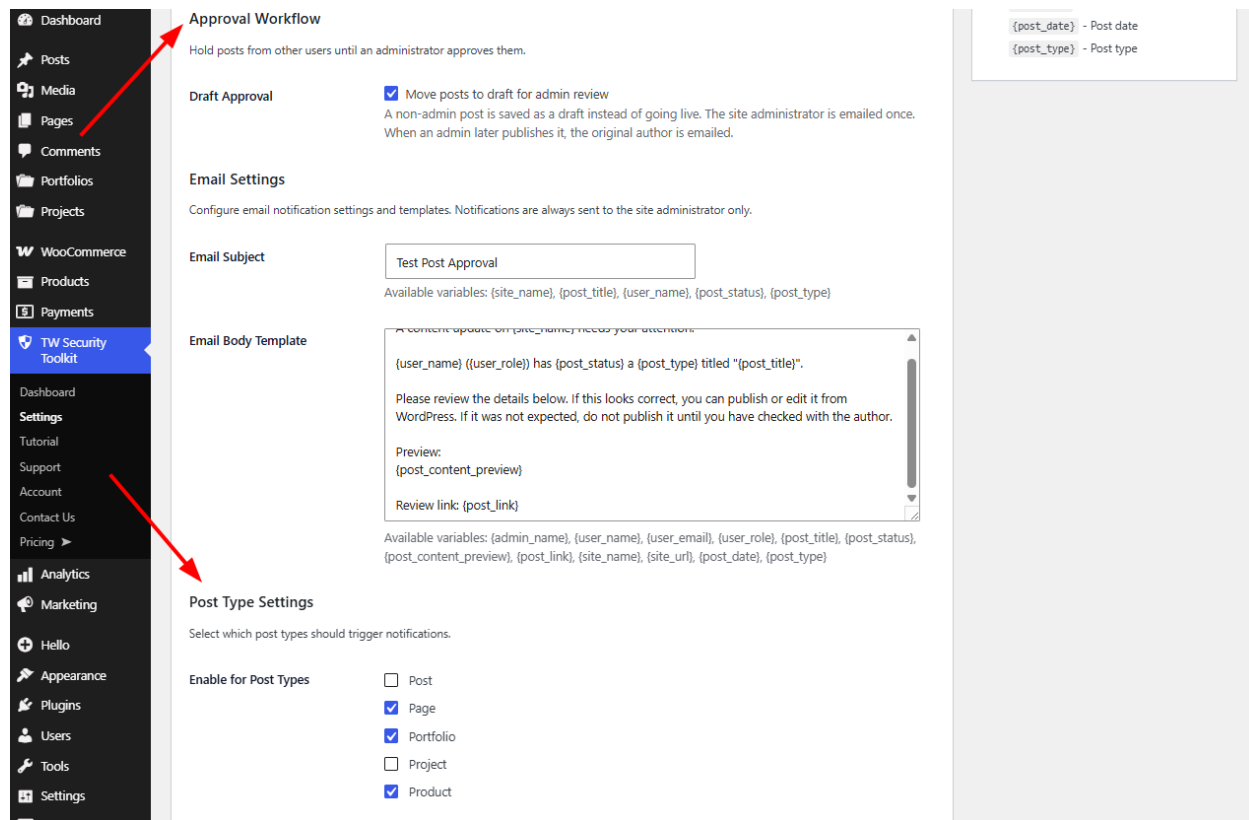
People with these account types will not cause an email alert. Site administrators are always skipped and cannot be turned on.

Plugin Information

This tool emails the site admin when other users publish posts. Administrators never trigger these emails. Optional draft approval can hold writer posts until you publish them.

Available Variables:

- {admin_name} - Administrator name
- {user_name} - User who published/submitted
- {user_email} - User email
- {user_role} - User role
- {post_title} - Post title
- {post_status} - Post status
- {post_content_preview} - Post content preview
- {post_link} - Edit post link
- {site_name} - Site name
- {site_url} - Site URL



4.3.3. CPT Revisions

CPT Revisions lets you enable or disable WordPress revisions for custom post types.

How It Works

When enabled:

- Nothing changes until you save settings.
- Built-in Post/Page and WooCommerce products are not listed.
- Only checked custom post types keep revisions.

Steps to Enable

1. Turn **CPT Revisions** On.
2. Check the custom post types that should keep revisions.
3. Save settings.

Backend Screenshot:

Dashboard

Posts

Media

Pages

Comments

Portfolios

Projects

WooCommerce

Products

Payments

TW Security Toolkit

Dashboard

Settings

Tutorial

Support

Account

Contact Us

Pricing >

Analytics

Marketing

Hello

Appearance

Plugins

Users

CONFIGURE

Content Workflow

Approvals, revisions, post edit tracking, and link expiration.

Status: On

< Settings

View Detail

Post Modifier Tracker

ON

Post Approval Notifier

ON

CPT Revisions

ON

Link Expiration

ON

Enable or disable WordPress revisions for each custom post type from one settings screen.

On

Revision toggles

Enable or disable WordPress revisions for each public custom post type.

Custom Post Type	Enable Revisions
Portfolio portfolio	☒
Project project	☐

Save Settings

< + ↶ ↷ ≡

Test Portfolio · Portfolio

🔗

🖨

📄

Save

⋮

Portfolio

Block

×

Test Portfolio

⋮

Set featured image

5 words, 1 minute read time.

Last edited a second ago.

Status ☒ Published

Publish September 15, 2026 5:18 am UTC+0

Slug test-portfolio

Template Default template

Revisions 5

Move to trash

Categories

Link Expiration

Expiration Time: mm/dd/yyyy --:-- --

Max clicks (0 = unlimited): 0

4.3.4. Link Expiration

Link Expiration expires content by date/time and/or maximum clicks.

How It Works

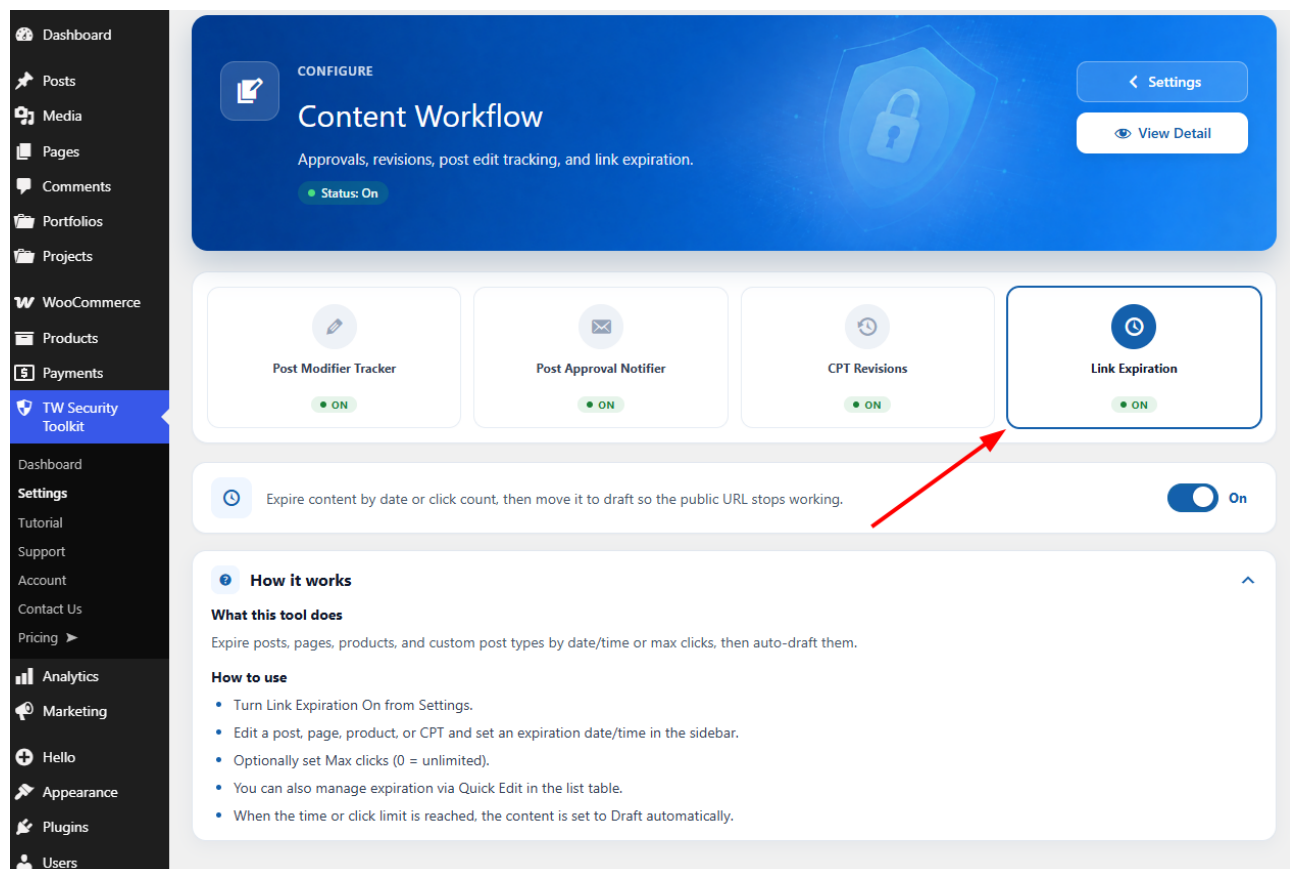
When enabled:

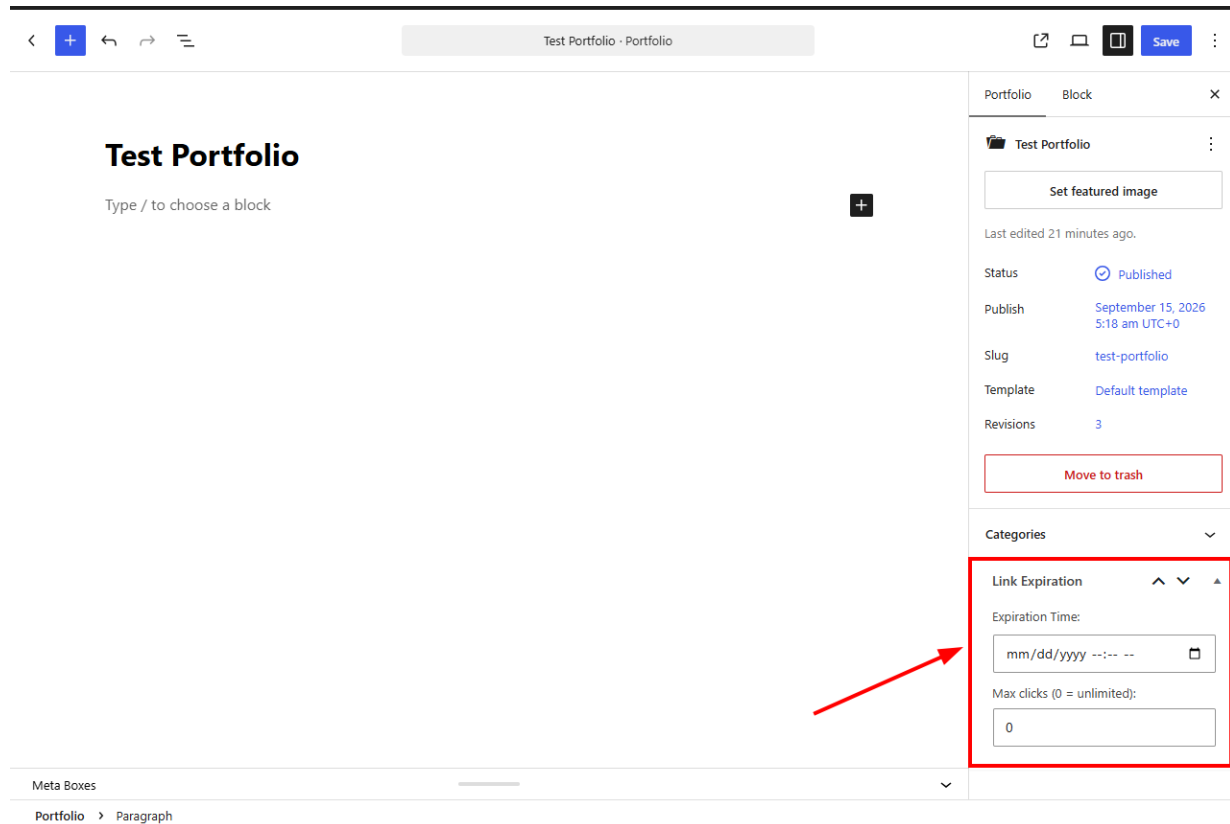
- Expiration rules are stored with the content.
- When the time or click limit is reached, the content moves to Draft.
- The public URL stops working (404).
- You can manage rules from the editor sidebar or Quick Edit.

Steps to Enable

1. Turn **Link Expiration** On.
2. Edit a post or page.
3. Set expiry date/time and/or Max clicks (0 = unlimited clicks).
4. Update the content.

Backend Screenshot:





4.4. Site Protection

Access this module from:

- **TW Security Toolkit > Site Protection**

4.4.1. Disable File Editor

Disable File Editor blocks the Theme File Editor and Plugin File Editor.

How It Works

When enabled:

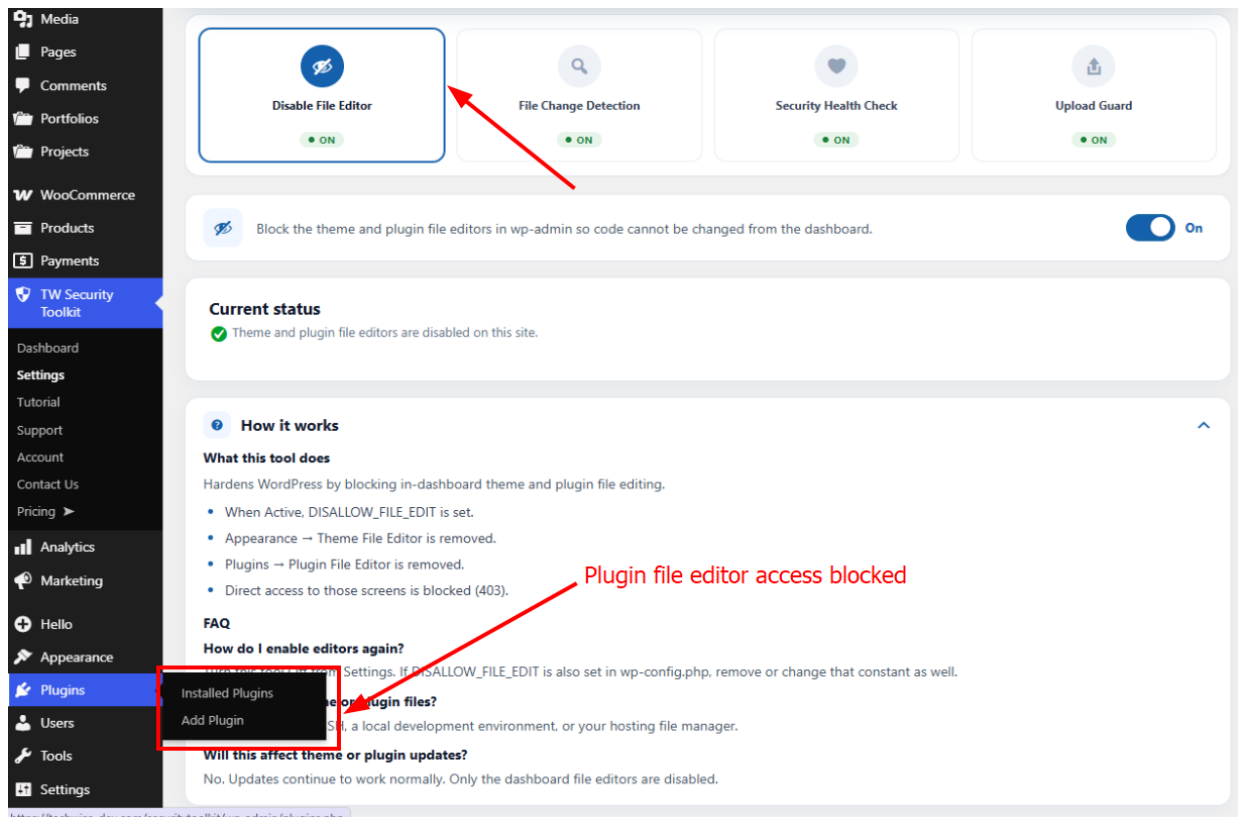
- Theme and plugin file editors are disabled in wp-admin.
- Related menu items are removed.
- Direct access attempts are blocked.

Steps to Enable

1. Turn **Disable File Editor** On.
2. Now You will see theme and plugin file editor are blocked

3. No extra settings are required.

Backend Screenshot:



4.4.2. File Change Detection

File Change Detection watches important WordPress files for unexpected changes.

How It Works

When enabled:

- A baseline of file hashes is stored.
- Automatic scans run on a schedule, and you can also scan manually.
- Status can show OK, Changed, or Unknown.
- After intentional updates, accept the current hashes to reset the baseline.

Steps to Enable

1. Turn **File Change Detection** On.
2. Run **Scan now**.
3. Accept the baseline hashes.

4. Re-scan after major updates and accept hashes again when changes are expected.

Backend Screenshot:

The screenshot displays the WordPress dashboard with the TW Security Toolkit sidebar. The 'File Change Detection' widget is highlighted with a red box and a red arrow. Below it, the 'File integrity' section shows a status of 'OK' and a list of watched areas including WordPress core, themes, and plugins. The 'Recent file change events' table shows two critical events from 2026-09-15.

Time	Type	Priority	User	IP	Message
2026-09-15 06:00:47	file_changed	critical	—	0.0.0.0	File change detected (20 files). Sample: .htaccess, error_log, wp-content/plugins/tw-security-toolkit/assets/css/support-page.css, wp-content/plugins/tw-security-toolkit/assets/css/admin.css, wp-content/plugins/tw-security-toolkit/assets/css/support-page-portal.css, wp-content/plugins/tw-security-toolkit/assets/js/dashboard.js, wp-content/plugins/tw-security-...
2026-09-15 05:00:29	file_changed	critical	—	0.0.0.0	File change detected (20 files). Sample: .htaccess, error_log, wp-content/plugins/tw-security-toolkit/assets/css/support-page.css, wp-content/plugins/tw-security-toolkit/assets/css/admin.css,

4.4.3. Security Health Check

Security Health Check scans your site and shows a score with recommendations.

How It Works

When enabled:

- You can run a security scan from Configure.
- Results show severity, status, and recommended fixes.
- The Dashboard Security Score uses the latest health check when available.
- Optional blocking can help protect public access to sensitive files such as `readme.html` and `license.txt`.

Steps to Enable

1. Turn **Security Health Check** On.

2. Optionally enable **Block sensitive files**.
3. Click **Run check**.
4. Fix recommended items, then run the check again.

Note: The **Run check** button stays disabled until Security Health Check is turned On.

Backend Screenshot:

The screenshot displays the TW Security Toolkit backend interface. On the left is a dark sidebar with navigation links: Pages, Comments, Portfolios, Projects, WooCommerce, Products, Payments, TW Security Toolkit (highlighted), Dashboard, Settings, Tutorial, Support, Account, Contact Us, Pricing, Analytics, Marketing, Hello, Appearance, Plugins, Users, Tools, Settings, SCF, and Collapse Menu. The main content area has a top row of four toggle cards: Disable File Editor (ON), File Change Detection (ON), Security Health Check (ON, highlighted with a red box and a red arrow), and Upload Guard (ON). Below these is a summary bar with a heart icon, a description, and a toggle switch set to 'On'. The summary bar contains four boxes: '89/100 Current security health score', '0 Critical issues found', '2 Statuses needing attention', and '2026-09-15 06:14:16 Last health check time'. The 'Settings' section follows, with a description and a 'Block sensitive files' toggle set to 'On'. A 'Save Settings' button is present. The 'Run security scan' section at the bottom has a description and a 'Run check' button, which is highlighted with a red arrow.

Pages
Comments
Portfolios
Projects
WooCommerce
Products
Payments
TW Security Toolkit
Dashboard
Settings
Tutorial
Support
Account
Contact Us
Pricing >
Analytics
Marketing
Hello
Appearance
Plugins
Users
Tools
Settings
SCF
Collapse Menu

Disable File Editor
ON

File Change Detection
ON

Security Health Check
ON

Upload Guard
ON

Scan your site for common security gaps and get a score plus recommended fixes you can act on. ☒ On

89/100
Current security health score

0
Critical issues found

2
Statuses needing attention

2026-09-15 06:14:16
Last health check time

Settings
Block public access to common sensitive files (readme.html, license.txt, wp-config backups, debug.log) using managed .htaccess rules. Files are not deleted.

Block sensitive files ☒ On
Requires Apache with .htaccess support (works on XAMPP). Turning Off removes only the toolkit-managed rules.

✓ Save Settings

Run security scan
Checks updates, known vulnerabilities, hardening settings, exposed files, and toolkit protection status.

✓ Run check

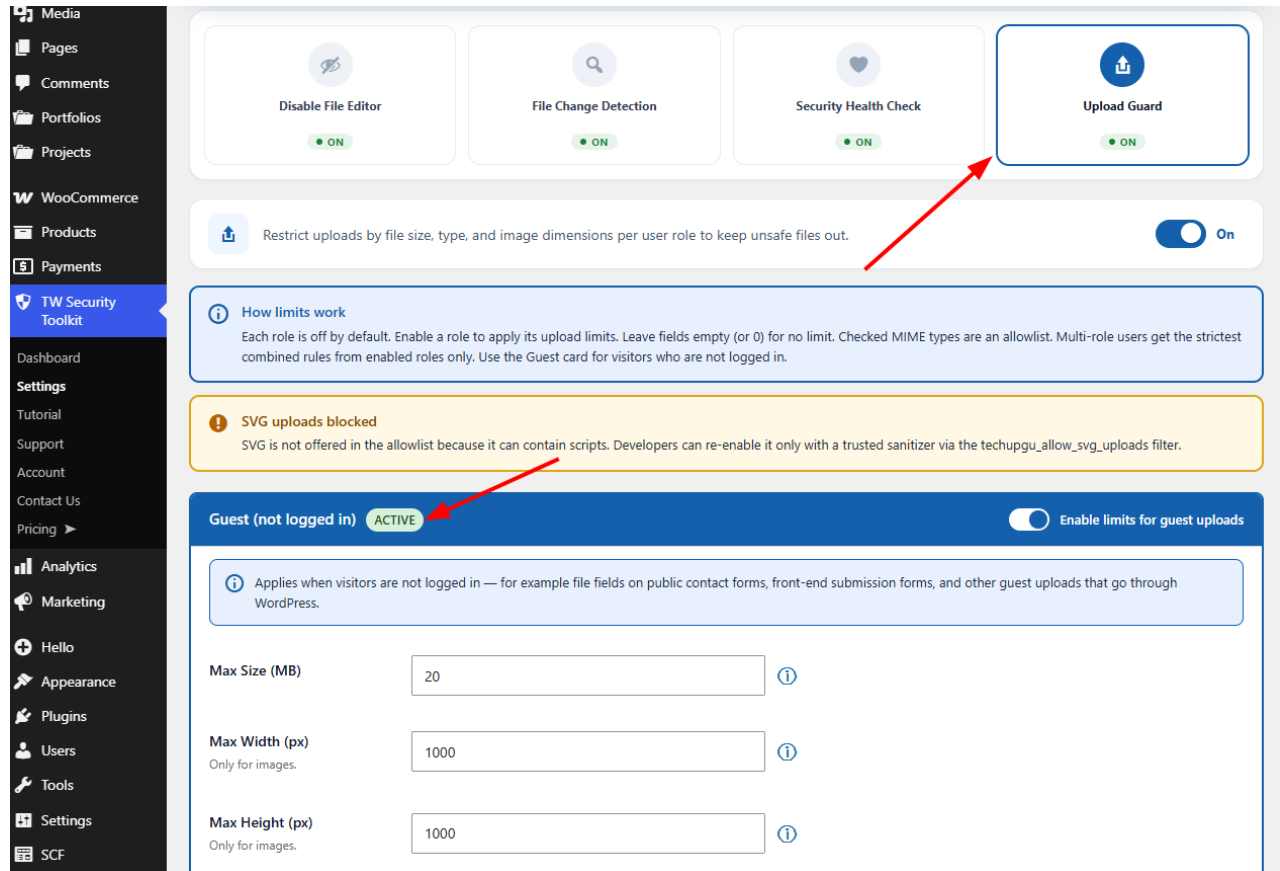
Check	Severity	Status	Recommendation
HTTPS / SSL enabled	Critical	OK	—
WP_DEBUG disabled on production	Critical	OK	—
Theme/plugin file editor disabled	Recommended	OK	—
PHP version supported (8.2.33)	Critical	OK	—
Administrator accounts limited (4)	Recommended	OK	—
No default "admin" username	Critical	OK	—
Custom database prefix (wp9k_)	Recommended	OK	—
Inactive plugins kept low (5)	Info	OK	—
WordPress core is up to date	Critical	OK	—
Plugins up to date (0 pending)	Recommended	OK	—
Themes up to date (0 pending)	Recommended	OK	—
No known vulnerabilities found (core + active plugins/themes)	Critical	OK	—
No obvious sensitive files exposed	Recommended	OK	—
3 unresolved suspicious alerts	Recommended	Needs attention	Review Activity & Audit Center and mark expected actions (for example an admin activating a plugin) so they leave the suspicious list.
Two-Factor Authentication (2FA) is On	Recommended	OK	—
Brute force protection is On	Recommended	OK	—
File change detection is On	Recommended	OK	—
Secure Login Path is On	Info	Needs attention	Turn on Secure Login Path to hide wp-login.php.
IP Blacklist tool is On	Info	OK	—

4.4.4. Upload Guard

How It Works

- Checks apply to Media Library uploads and guest uploads where supported.
- Rules can be set per role, including Guest.
- Empty or 0 values mean no limit for that field.
- Multi-role users follow the strictest combined rules from enabled roles.

Backend Screenshot:



4.5. Monitoring & Alerts

Access this module from:

- TW Security Toolkit > Monitoring & Alerts

4.5.1. Complete Audit Log

Complete Audit Log records important site actions in a searchable admin table.

How It Works

When enabled:

- Key events are stored and listed with filters.
- You can filter by type, date range, and search text.
- Exports to CSV or PDF respect the current filters.

Typical events include:

- Successful / failed logins and logouts
- Post and page updates
- Plugin and theme activate, deactivate, and update actions
- User create, role change, and delete actions
- IP locks, IP blocks, and other high-value security events

Steps to Enable

1. Turn **Complete Audit Log** On.
2. Open the Audit Log screen.
3. Use filters to review activity.
4. Export CSV or PDF when needed.

Backend Screenshot:

The screenshot displays the TW Security Toolkit backend interface. On the left is a dark sidebar menu with options: Media, Pages, Comments, Portfolios, Projects, WooCommerce, Products, Payments, TW Security Toolkit (highlighted), Dashboard, Settings, Tutorial, Support, Account, Contact Us, Pricing, Analytics, Marketing, Hello, Appearance, Plugins, Users, Tools, Settings, and SCF. The main content area has a top row of five toggle switches, all set to 'ON': Complete Audit Log, Suspicious Activity Detection, Email & Slack/Discord Notifications, Scheduled Security Reports, and Automated Emails. Below this is a section for 'Log important WordPress security events in one place, then export the results as CSV or PDF reports.' with a toggle switch set to 'On'. A red box highlights the filter section below, which includes a 'Type' dropdown (set to 'All types'), 'From' and 'To' date pickers (set to 09/10/2026 and 09/15/2026), a search bar, and buttons for 'Filter', 'Export CSV', and 'Export PDF'. Below the filter section is the 'Audit events' table, which shows 179 events. The table has columns: Time, Type, Priority, User, IP, Message, and Actions. The first event is a 'file_changed' event with 'critical' priority, occurring on 2026-09-15 at 06:00:47. The second event is a 'content_updated' event with 'info' priority, occurring on 2026-09-15 at 05:42:43. The third event is a 'content_updated' event with 'info' priority, occurring on 2026-09-15 at 05:19:36. The fourth event is a 'content_created' event with 'info' priority, occurring on 2026-09-15 at 05:18:44.

Time	Type	Priority	User	IP	Message	Actions
2026-09-15 06:00:47	file_changed	critical	—	0.0.0.0	File change detected (20 files). Sample: .htaccess, error_log, wp-content/plugins/tw-security-toolkit/assets/css/support-page.css, wp-...	View detail
2026-09-15 05:42:43	content_updated	info	securitytoolkit_admin_abdullah	182.178.252.141	portfolio "Test Portfolio" was updated.	—
2026-09-15 05:19:36	content_updated	info	securitytoolkit_admin_abdullah	182.178.252.141	portfolio "Portfolio 5" was updated.	—
2026-09-15 05:18:44	content_created	info	securitytoolkit_admin_abdullah	182.178.252.141	portfolio "Portfolio 5" was created.	—

4.5.2. Suspicious Activity Detection

Suspicious Activity Detection watches for unusual security patterns.

How It Works

When enabled, the tool can detect:

- Failed logins over a threshold in a short window
- Administrator login from a new IP (optional)
- New administrator accounts
- Plugin activations
- File editors enabled while Disable File Editor is Active

Matched events are logged and can also be sent through Notifications when that tool is On.

Steps to Enable

1. Turn **Suspicious Activity Detection** On.
2. Review detection options.
3. Save settings.

Backend Screenshot:

The screenshot shows the TW Security Toolkit interface. On the left is a dark sidebar with navigation links: Posts, Media, Pages, Comments, Portfolios, Projects, WooCommerce, Products, Payments, TW Security Toolkit (highlighted), Dashboard, Settings, Tutorial, Support, Account, Contact Us, Pricing, Analytics, Marketing, Hello, Appearance, Plugins, Users, and Tools. The main content area has a top row of five toggle switches, all set to 'ON': Complete Audit Log, Suspicious Activity Detection (highlighted with a blue border and a red arrow), Email & Slack/Discord Notifications, Scheduled Security Reports, and Automated Emails. Below this is a section for 'Suspicious Activity Detection' with a toggle switch set to 'On' and a description: 'Watch for unusual behavior on the site and send instant alerts when something looks suspicious.' This section is also pointed to by a red arrow. Underneath is the 'Detection settings' section, which includes: 'Failed login threshold' set to 3, 'Window (minutes)' set to 10, and 'New admin IP' set to 'On' with a sub-note 'Alert when an administrator logs in from a new IP'. A 'Save Settings' button is at the bottom of this section. The bottom section is 'Recent suspicious events', which contains a table with two entries. The table has columns: Time, Type, Priority, User, IP, Message, and Actions. Both entries are marked as 'suspicious' and 'critical'.

Time	Type	Priority	User	IP	Message	Actions
2026-09-15 05:03:36	suspicious	critical	securitytoolkit_admin_abdullah_2	23.106.249.52	Admin securitytoolkit_admin_abdullah_2 logged in from new IP 23.106.249.52.	Mark as expected
2026-09-15 05:01:12	suspicious	critical	securitytoolkit_admin_abdullah_2	182.178.252.141	Rapid failed logins from IP 182.178.252.141 (user securitytoolkit_admin_abdullah_2).	Mark as expected

4.5.3. Email & Slack / Discord Notifications

Notifications send security alerts when important events happen.

How It Works

When enabled:

- Alerts can go to Email, Slack webhook, and/or Discord webhook.
- Only official webhook URLs are supported for Slack and Discord.
- You can choose a minimum severity, such as warning and above or critical only.

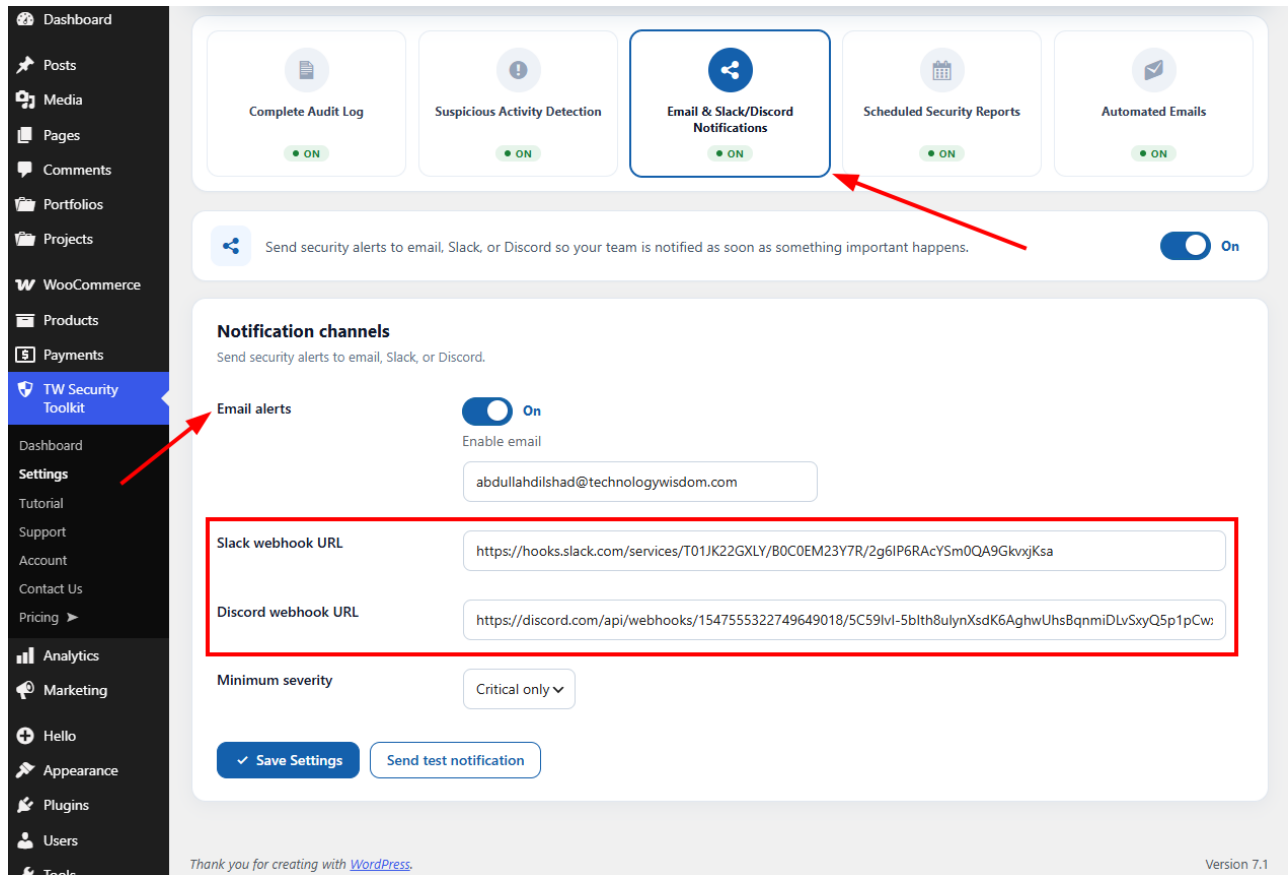
Typical triggers include:

- IP locks
- Suspicious activity
- File changes
- OTP failures
- Other high-severity events

Steps to Enable

1. Turn **Notifications** On.
2. Enable email and/or paste webhook URLs.
3. Choose severity settings.
4. Save settings.
5. Optionally send a test notification.

Backend Screenshot:



4.5.4. Scheduled Security Reports

Scheduled Reports send a summary email on a daily, weekly, or monthly schedule.

How It Works

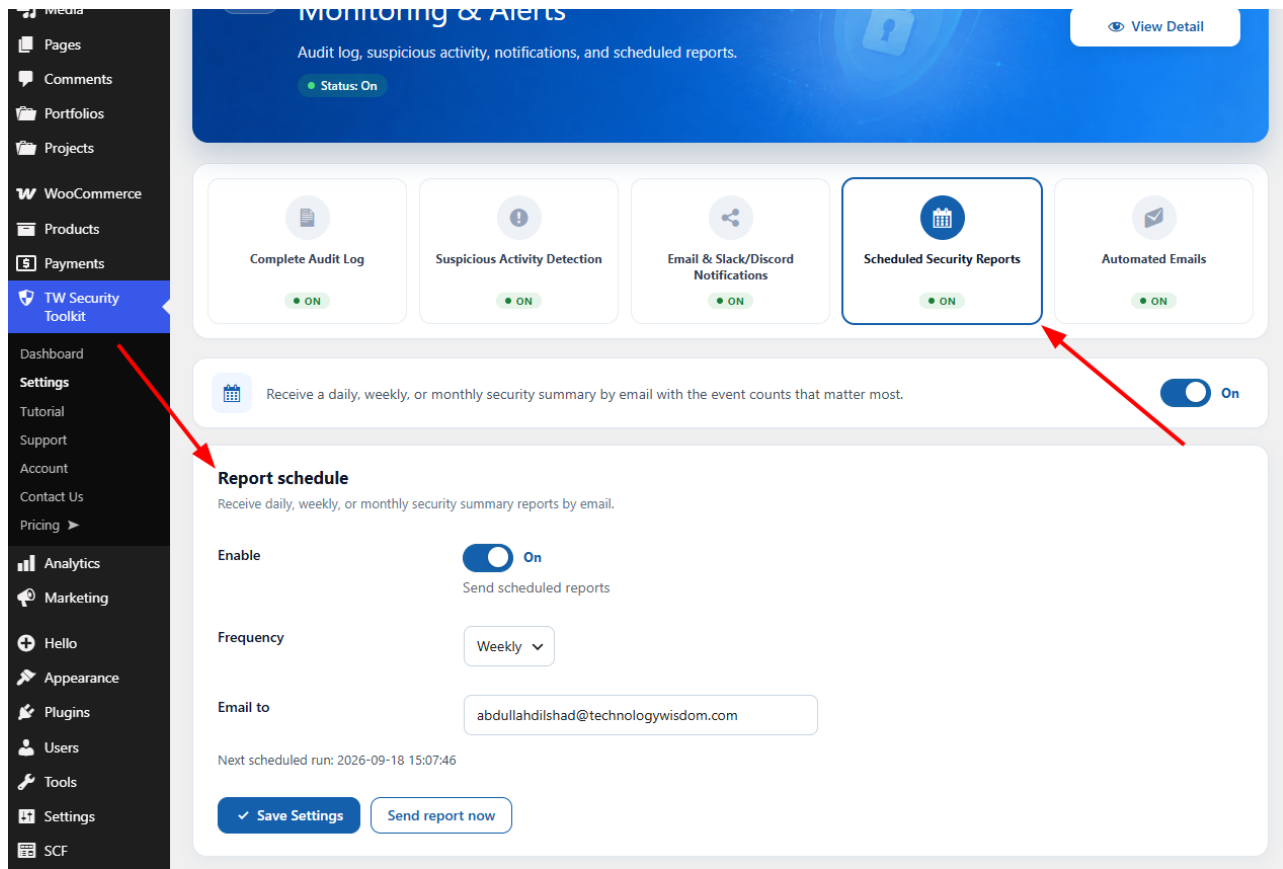
When enabled:

- Reports can include logins, suspicious events, file changes, and health score.
- WordPress cron handles the schedule.
- You can send a report immediately for testing.
- On low-traffic sites, cron runs when the site is visited.

Steps to Enable

1. Turn **Scheduled Security Reports** On.
2. Choose frequency and recipient Email.
3. Save settings.
4. Optionally click **Send report now**.

Backend Screenshot:



4.5.5. Automated Emails

Automated Emails lets you control each email the toolkit can send, one by one.

This is useful when you want a security feature to stay On, but you do not want every related email.

How It Works

When you open this tab:

- You see a list of every automated email the plugin can send.
- Every email starts **On** by default.
- Turning one email **Off** stops that message only.
- Related security features can stay On even if their email is Off.
- Examples include locked IP alerts, suspicious activity alerts, file change alerts, login alerts, login verification codes, and post approval emails.

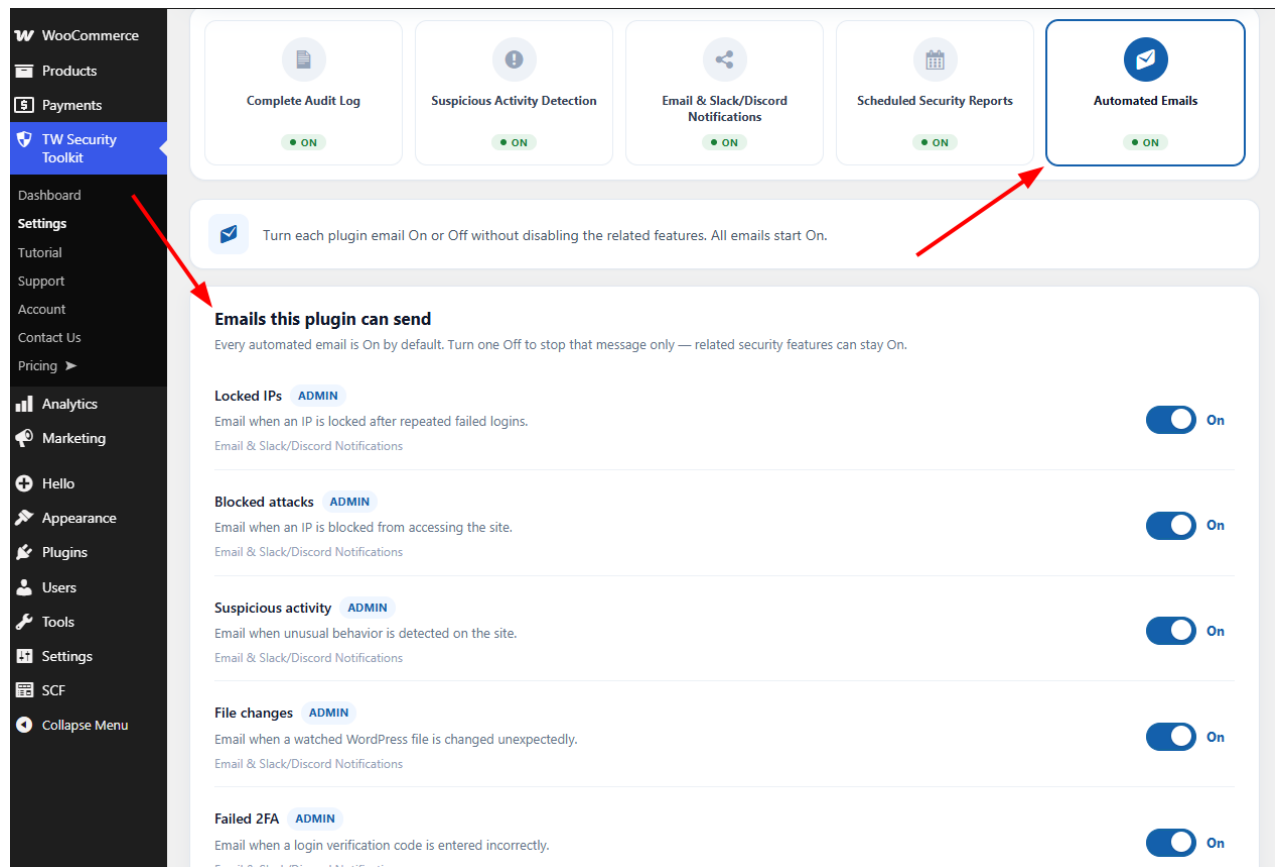
Steps to Enable / Manage

1. Turn **Automated Emails On**.
2. Review the list of emails this plugin can send.

3. Turn **Off** any message you do not want.
4. Leave the rest ON.

Note: Turning Off the **Login verification code** email will block Email OTP logins, because users will not receive the one-time code.

Backend Screenshot:



5. How to View Stats?

Each security module includes a View Detail page.

Use View Detail when you want to review activity for that module only — not the whole toolkit.

What you can see on a View Detail page:

- A short “How it works” overview for the module
- Time filters such as Last 24 hours, Last 7 days, Last 30 days, or All time
- Module stats for the selected period
- Charts and recent activity related to that module

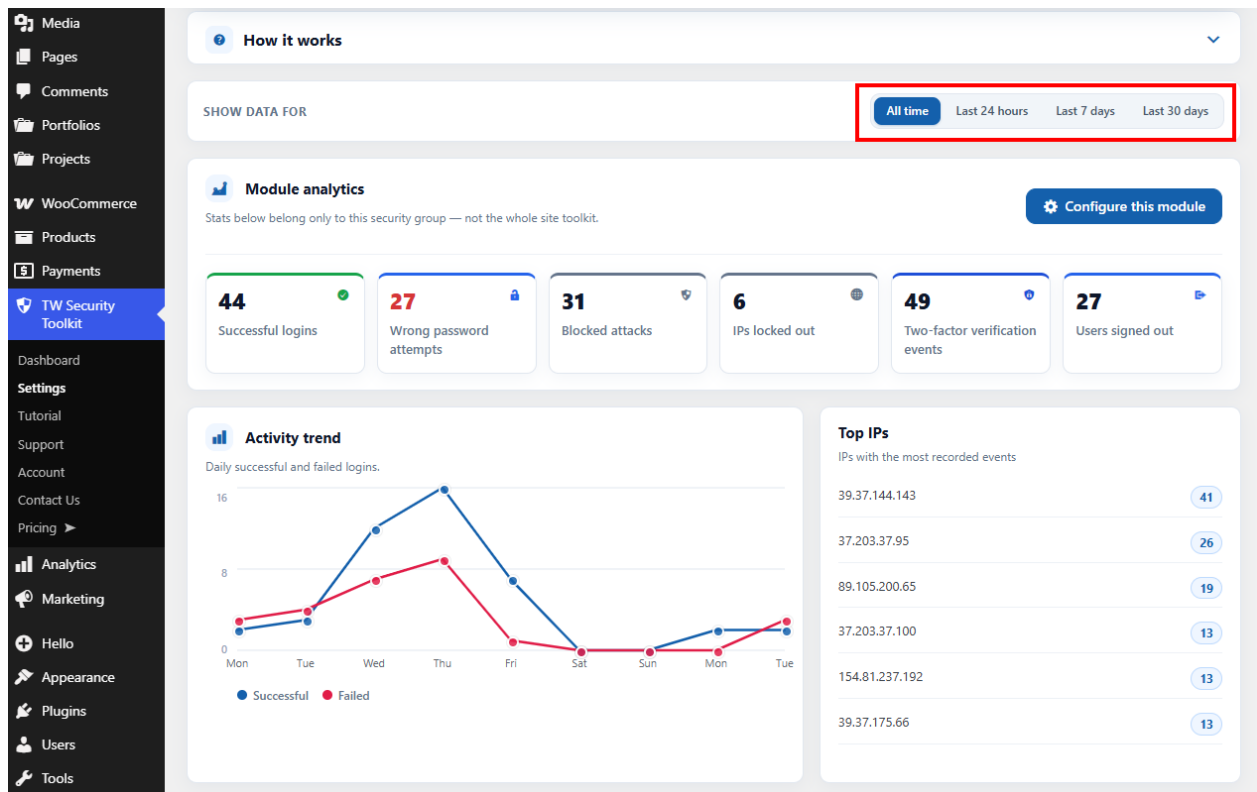
- A quick link back to Configure for the same module

Example: Authentication View Detail

1. Go to TW Security Toolkit > Authentication.
2. Click View Detail.
3. Choose a time range.
4. Review login-related stats, charts, and recent activity for Authentication only.

Other modules work the same way. Open the module, click View Detail, and review activity for that group.

Backend Screenshot:



Pages

Comments

Portfolios

Projects

WooCommerce

Products

Payments

TW Security Toolkit

Dashboard

Settings

Tutorial

Support

Account

Contact Us

Pricing

Analytics

Marketing

Hello

Appearance

Plugins

Users

Tools

Settings

SCF

Collapse Menu

Activity in this module

View all

TIME	TYPE	PRIORITY	USER	IP	MESSAGE
2026-09-15 05:03:36	login_success	info	securitytoolkit_admin_abdullah_2	23.106.249.52	User securitytoolkit_admin_abdullah_2 logged in.
2026-09-15 05:01:12	login_failed	warning	securitytoolkit_admin_abdullah_2	182.178.252.141	Failed login attempt for securitytoolkit_admin_abdullah_2.
2026-09-15 05:00:54	ip_locked	critical	securitytoolkit_admin_abdullah_2	182.178.252.141	IP 182.178.252.141 locked after failed logins for securitytoolkit_admin_abdullah_2.
2026-09-15 05:00:54	login_failed	warning	securitytoolkit_admin_abdullah_2	182.178.252.141	Failed login attempt for securitytoolkit_admin_abdullah_2.
2026-09-15 05:00:43	login_failed	warning	securitytoolkit_admin_abdullah_2	182.178.252.141	Failed login attempt for securitytoolkit_admin_abdullah_2.
2026-09-15 04:52:40	login_success	info	securitytoolkit_admin_abdullah	182.178.252.141	User securitytoolkit_admin_abdullah logged in.
2026-09-15 04:52:31	logout	info	securitytoolkit_admin	182.178.252.141	User securitytoolkit_admin logged out.
2026-09-14 09:37:37	logout	info	securitytoolkit_hussain	182.178.252.141	User securitytoolkit_hussain logged out.
2026-09-14 09:34:27	login_success	info	securitytoolkit_hussain	182.178.252.141	User securitytoolkit_hussain logged in.
2026-09-14 09:32:52	login_success	info	securitytoolkit_admin_abdullah	182.178.252.141	User securitytoolkit_admin_abdullah logged in.
2026-09-14 09:32:21	logout	info	securitytoolkit_admin_abdullah	182.178.252.141	User securitytoolkit_admin_abdullah logged out.
2026-09-11 13:09:41	logout	info	securitytoolkit_hussain	39.37.159.111	User securitytoolkit_hussain logged out.
2026-09-11 11:56:52	logout	info	securitytoolkit_admin	39.37.159.111	User securitytoolkit_admin logged out.
2026-09-11 11:53:11	login_success	info	securitytoolkit_hussain	39.37.159.111	User securitytoolkit_hussain logged in.

6. Frequently Asked Questions (FAQs)

Does activating the plugin turn all tools On?

No. Every tool stays Off until you turn it On from the Dashboard or Settings.

Where do I manage the tools?

Use **TW Security Toolkit > Dashboard** for the overview, then open each module (**Authentication**, **Content Workflow**, **Site Protection**, **Monitoring & Alerts**) to Configure or View Detail.

Do I need coding knowledge?

No. All features can be configured from the WordPress admin dashboard.

What happens if I forget my Secure Login Path URL?

Deactivate the plugin through FTP or your host file manager. The default **wp-login.php** URL will work again.

Can administrators be blocked by IP Blacklist?

No. Logged-in administrators are never blocked, and you cannot blacklist your own current IP.

Does Login OTP work for all users?

You choose the scope: all users, administrators only, or selected roles.

Are administrators limited by role policies?

No. Administrators are excluded from the optional role policy limits.

Does Upload Guard work for guests?

Yes. You can enable Guest rules in addition to logged-in roles.

What happens when a Link Expiration rule is reached?

The content moves to Draft and the public URL stops working.

Does CPT Revisions affect Posts and Pages?

No. Built-in Post/Page and WooCommerce products are not listed. Only custom post types you select are managed.

Why is the Run check button disabled?

Security Health Check must be turned On first. When it is Off, Run check stays disabled.

How do I improve the Security Score / Security Level?

Run Health Check, fix the recommended items, then run the check again.

When should I accept File Change Detection hashes?

After intentional core, theme, or plugin updates, accept the current hashes so expected changes do not keep triggering alerts.

Can I export Audit Log data?

Yes. You can export audit log data as CSV or PDF.

Can alerts go to Slack or Discord?

Yes. Add official webhook URLs in Notifications settings.

Will Scheduled Reports always be sent on time?

They use WordPress cron. On low-traffic sites, cron runs when someone visits the site.

What happens when I deactivate the plugin?

Scheduled cron jobs for advanced tools are cleared. Settings remain until uninstalled.

What happens when I uninstall the plugin?

The events table, options, and related user meta are cleaned up.

If free companion TW plugins are installed, what happens when I activate TW Security Toolkit?

The toolkit can automatically deactivate the matching free plugins because those features are already included.

7. Troubleshooting

7.1. Dashboard Shows Little or No Activity

Check:

- Related tools are turned On (especially Audit Log and login tools)
- Users have performed actions after tools were enabled
- You are looking at the correct time range (for example Last 7 Days)

7.2. Secure Login Path Not Working

Check:

- Secure Login Path is On
- Settings were saved
- You visited **Settings > Permalinks > Save Changes**
- You are using the correct custom login slug

7.3. Brute Force Lockouts

Check:

- Max attempts and lockout settings
- Locked IP list in Configure
- Unlock your own IP if needed

7.4. Health Check Cannot Run

Check:

- Security Health Check is turned On
- The Run check button is no longer disabled
- You have administrator ([manage_options](#)) access

7.5. File Change Alerts After Updates

Check:

- Recent core, theme, or plugin updates
- Accept current hashes after intentional changes
- Run a fresh scan

7.6. Notifications Not Arriving

Check:

- Notifications tool is On
- Email / webhook settings are saved
- Webhook URLs are official Slack or Discord URLs
- Send a test notification
- Server mail delivery is working for email alerts

8. Best Use Cases

- Business websites that need stronger login protection
- Agency-managed WordPress sites
- Membership or multi-author sites that need publish approvals
- Sites that must hide the default login URL
- Stores and content sites that need upload limits
- Sites that require file integrity monitoring
- Teams that want email, Slack, or Discord security alerts
- Owners who want a clear security score and weekly reports
- Sites replacing several free security helpers with one toolkit

8. Conclusion

TW Security Toolkit provides a flexible solution for login protection, site hardening, content workflow control, and security monitoring. With tools for Secure Login Path, brute force protection, OTP, upload limits, health checks, file change detection, audit logging, alerts, and scheduled reports, site owners can improve WordPress security without complex setup.

Turn on only the tools you need, review the Dashboard regularly, and follow Health Check recommendations to keep your Security Score strong.