Getting Started

Learn how to install Steel Security, run your first scan, and secure your site in minutes.

Steel Security Documentation

Welcome to the official documentation for **Steel Security** — a high-signal WordPress security auditing and hardening plugin built for real-world environments.

Steel Security helps you quickly identify critical risks, understand their impact, and apply safe, reversible hardening without breaking your site.

Getting Started

New to Steel Security? Start here to get up and running in minutes.

- Installing the Plugin
- Activating Steel Security
- Running Your First Scan
- Understanding the Dashboard

Using the Plugin

Learn how to navigate and use Steel Security effectively.

- Dashboard Overview
- Scan Risk Score Explained
- Hardening Posture Score Explained
- Reviewing Findings
- Applying Hardening Safely

Licensing & Activations

Manage your licenses and connected sites.

- How Licensing Works

- Activating a Site
- Activating a Site
- Moving a License to a New Site
- Managing Licenses in the Portal

Hardening Reference

Detailed explanations of each hardening control and how they behave across environments.

- Uploads PHP Execution Protection
- Directory Listing Protection
- Security Headers Reference
- wp-config Hardening
- Server-Specific Considerations

Findings Reference

Understand what each scan result means and how to respond.

- Debug Mode Enabled
- SQL Dump in Web Root
- Backup Archive in Web Root
- phpinfo File in Web Root
- Default Admin User

Troubleshooting

Having an issue? Start here.

- Activation Failed
- Could Not Connect to License Server
- Scan Does Not Complete

- Hardening Could Not Be Applied
- cPanel and Shared Hosting Notes

How Steel Security Is Different

Steel Security is built around a simple philosophy:

> Focus on high-signal risks, provide safe hardening, and respect real-world hosting environments.

- No noisy, low-value alerts
- Clear separation of **Scan** vs **Hardening**
- Safe, reversible changes
- Server-aware implementation (Apache, IIS, Nginx)
- Designed for developers, agencies, and serious site owners

Recommended Workflow

If you're unsure where to begin, follow this flow:

1. Install and activate the plugin
2. Run your first scan
3. Review high-risk findings
4. Apply hardening where appropriate
5. Re-scan to confirm improvements
6. Monitor regularly

Need More Help?

- Explore the sections above
- Check troubleshooting guides
- Review detailed reference pages

Review all documentation at: https://docs.steelsecurity.com/books

---

Steel Security — Security clarity without the noise.

What Steel Security Is

What Steel Security Is

Welcome to Steel Security

What Steel Security Does

Steel Security is a high-signal WordPress security auditing and hardening plugin designed to surface real risks quickly and help you address them safely.

Instead of overwhelming you with noise, Steel Security focuses on identifying meaningful security issues such as exposed files, misconfigurations, and unsafe defaults — then provides clear, actionable guidance to resolve them.

Steel Security is built for real-world environments where uptime matters, and where security changes must be applied carefully and reversibly.

Why Steel Security Is Different

Most security plugins try to do everything — malware scanning, firewalls, monitoring — often at the cost of clarity and performance.

Steel Security takes a different approach:

- Focus on **high-value, high-signal findings**
- Separate **Scan** (what's wrong) from **Hardening** (what you can safely change)
- Provide **clear explanations**, not just alerts
- Support **safe, reversible changes**
- Respect **real-world hosting environments** (Apache, IIS, Nginx, shared hosting)

This makes Steel Security especially useful for developers, agencies, and site owners who want control and clarity.

What Steel Security Does Not Do

Steel Security is not a malware scanner or firewall.

It does not attempt to:

- continuously scan files for malware signatures
- block traffic or act as a web application firewall
- replace server-level security tools

Instead, it focuses on identifying and resolving **structural security risks** that are often overlooked but highly impactful.

Core Concepts

Understanding Steel Security starts with two key ideas:

Scan

The Scan identifies potential risks in your WordPress installation.

These include:

- exposed sensitive files
- debug configurations
- insecure defaults
- leftover artifacts (backups, dumps, test files)

Each finding includes context so you understand both the risk and the recommended response.

Hardening

Hardening allows you to apply protective changes to reduce risk.

These changes are:

- **targeted** (only what is needed)
- **safe** (designed to avoid breaking your site)
- **reversible** (you can roll them back if needed)

Examples include:

- blocking PHP execution in uploads
- disabling directory listing
- applying security headers
- tightening configuration exposure

When to Use Steel Security

Steel Security is most valuable when:

- launching or auditing a new site
- taking over an existing site
- preparing for production or client handoff
- performing routine security reviews
- cleaning up after migrations or backups

It is also useful as an ongoing check to ensure nothing unsafe has been introduced over time.

Steel Security Pro

Steel Security includes both a free core plugin and a Pro upgrade.

The Pro version expands functionality with additional:

- advanced checks and findings
- enhanced hardening controls
- deeper insights and guidance
- licensing and multi-site management capabilities

If you are managing multiple sites or require more advanced control, Pro is recommended.

What to Do Next

If you're just getting started:

1. Install and activate the Steel Security plugin
2. Run your first scan
3. Review the highest-risk findings
4. Apply hardening where appropriate
5. Re-scan to confirm improvements

From there, explore the rest of the documentation to deepen your understanding and refine your security posture.

Related

- Installing the Steel Security Plugin
- Activating Steel Security
- Running Your First Scan
- Understanding the Dashboard

Installation

Installation

System Requirements

What This Covers

This page outlines the minimum and recommended requirements for running Steel Security effectively.

Steel Security is designed to work in real-world hosting environments, including shared hosting, while still providing meaningful security insights and safe hardening options.

Minimum Requirements

Steel Security requires a standard, modern WordPress environment.

- WordPress 6.0 or newer
- PHP 8.0 or newer
- MySQL 5.7+ or MariaDB equivalent
- Ability to install and activate WordPress plugins

Most managed WordPress hosts and modern shared hosting environments will meet these requirements.

Recommended Environment

For the best experience and full feature support:

- WordPress 6.4+
- PHP 8.2+
- MySQL 8.0+ or MariaDB 10.6+
- HTTPS enabled
- Access to your hosting control panel (cPanel, Plesk, or equivalent)

This ensures compatibility with all checks and hardening features, and improves performance and reliability.

Supported Hosting Environments

Steel Security is designed to function across a wide range of hosting setups:

- Shared hosting (including cPanel environments)
- VPS and dedicated servers
- Managed WordPress hosting platforms

Where server-level access is limited, Steel Security will still provide guidance and apply changes where possible.

Web Server Compatibility

Steel Security is server-aware and adapts its behavior based on your environment.

Supported servers include:

- Apache
- Nginx
- Microsoft IIS

Some hardening features may behave differently depending on server capabilities and configuration.

File System Access

Steel Security requires standard WordPress-level file access.

- Ability to read WordPress files and directories
- Ability to write to specific locations when applying hardening

If your file system is locked down or read-only, some hardening features may not be available.

Outbound Connectivity

Steel Security connects to the licensing system for activation and validation.

Your server must be able to:

- make outbound HTTPS requests
- resolve external domains

If outbound connections are blocked, activation and licensing features will not function.

Permissions and Security Restrictions

Some hosting environments impose restrictions that may affect functionality.

These may include:

- disabled PHP functions
- restricted file permissions
- limited access to server configuration

Steel Security will continue to operate where possible and will provide guidance when a feature cannot be applied automatically.

Performance Considerations

Steel Security is designed to be lightweight and efficient.

- Scans are targeted and do not continuously run in the background
- No persistent high-load processes
- No traffic filtering or firewall overhead

This makes Steel Security suitable for both small sites and larger deployments.

When Requirements Are Not Met

If your environment does not meet certain requirements:

- some checks may be skipped
- some hardening features may be unavailable
- guidance may be provided instead of automated fixes

Steel Security will not attempt unsafe changes or force incompatible behavior.

Related

- Installing the Plugin
- Running Your First Scan
- Server and Hosting Issues

Installing the Plugin

What This Covers

This guide walks you through installing the Steel Security plugin on your WordPress site.

Steel Security installs like any standard WordPress plugin and does not require any special configuration to get started.

Before You Begin

Ensure your site meets the minimum system requirements:

- WordPress 6.0 or newer
- PHP 8.0 or newer
- Administrator access to your WordPress dashboard

If you're unsure, see the **System Requirements** page for full details.

Install via WordPress Admin (Recommended)

This is the fastest and most common method.

1. Log in to your WordPress admin dashboard
2. Navigate to **Plugins → Add New**
3. Search for **Steel Security**
4. Click **Install Now**
5. Click **Activate**

Once activated, Steel Security will appear in your admin menu.

Install via Plugin Upload

Use this method if you have downloaded the plugin manually.

1. Log in to your WordPress admin dashboard
2. Navigate to **Plugins → Add New**
3. Click **Upload Plugin**
4. Select the Steel Security `.zip` file
5. Click **Install Now**
6. Click **Activate**

After Installation

Once the plugin is activated:

- Steel Security will be available in your WordPress admin menu
- You can access the dashboard immediately
- No configuration is required before running your first scan

At this point, Steel Security is ready to use.

What to Expect

On first access:

- Steel Security may prompt you to activate your license
- You will be able to run your first scan immediately
- No automatic changes are made to your site

Steel Security does not modify your site until you explicitly apply hardening actions.

Common Issues

Plugin does not appear after activation

- Ensure activation completed successfully
- Refresh the admin dashboard

- Check for plugin conflicts

Installation fails

- Verify your PHP and WordPress versions meet requirements
- Check file upload limits if using manual upload
- Confirm your hosting environment allows plugin installation

---

Permission errors

- Ensure WordPress has permission to install plugins
- Check file ownership and permissions on your server

When to Use Each Installation Method

- Use **WordPress Admin install** for most cases
- Use **manual upload** if you have a direct download or restricted plugin access

---

What to Do Next

After installation:

1. Activate your Steel Security license **Note:** License activation is only required for Steel Security Pro.
2. Run your first scan
3. Review findings and next steps

Related

- System Requirements
- Activating Steel Security
- Running Your First Scan

Installation

Activating Steel Security

What This Covers

This guide explains how to activate Steel Security and connect your site to your account.

Do You Need to Activate?

Steel Security can be used without activation in its free version.

Pro Feature: Requires an active Steel Security license.

If you are using Steel Security Pro features, activation is required.

How to Activate Steel Security

1. In your WordPress admin, navigate to **Steel Security → Dashboard**
2. Locate the **License / Activation** section
3. Enter your Steel Security account credentials or license key
4. Click **Activate**

Once successful, your site will be linked to your Steel Security account.

What Happens During Activation

- Your site is connected to your Steel Security account
- Pro features become available (if applicable)
- Secure communication with the licensing system is enabled

No changes are made to your site during activation.

What to Expect After Activation

- Activation status is visible in the dashboard
- Pro features are enabled
- The plugin will validate your license automatically

Common Issues

Activation Failed

- Verify your credentials or license key
- Ensure your license is active
- Confirm your site has internet access

Unable to Connect to License Server

- Check outbound HTTPS connectivity
- Review firewall or hosting restrictions

What to Do Next

After activation:

1. Run your first scan
2. Review findings
3. Begin applying hardening

Related

- Running Your First Scan
- Licensing and Activations

First Scan

First Scan

Running Your First Scan

What This Covers

This guide explains how Steel Security performs your first scan and what to expect when viewing results.

The scan is the first step in identifying security risks and establishing a baseline for your site.

Before You Begin

Ensure:

- Steel Security is installed and activated
- You have access to the Steel Security dashboard
- (Optional) Your license is activated if using Pro features

How to Run Your First Scan

Steel Security runs a scan automatically when you open the Scan page.

To start your first scan:

1. In your WordPress admin, navigate to **Steel Security → Dashboard**
2. Click **Open Scan**

—or—

1. Navigate directly to **Steel Security → Scan**

Once the Scan page loads, the scan will begin automatically.

What the Scan Checks

Steel Security focuses on high-value findings, including:

- exposed sensitive files (e.g. backups, dumps, configuration artifacts)
- debug and development settings
- insecure defaults
- leftover or forgotten files in the web root

The scan is designed to prioritize **meaningful risks**, not noise.

What to Expect

When the Scan page loads:

- A scan begins automatically
- Results are displayed within a few seconds
- A **Scan Risk Score** summarizes overall risk

Steel Security does not make any changes to your site during the scan.

Understanding the Results

Each finding represents a potential risk.

For each item, you will see:

- what was detected
- why it matters
- recommended next steps

Focus first on:

- high-risk findings
- exposed files
- configuration issues

What the Scan Does Not Do

Steel Security does not:

- scan for malware signatures
- run continuously in the background
- modify your site automatically

This ensures the scan is fast, safe, and predictable.

Running Additional Scans

To run another scan:

- Re-open the **Scan** page
- Reload the Scan page

A new scan will be triggered automatically each time.

After Your First Scan

Once you have reviewed the results:

1. Identify the highest-risk findings
2. Apply hardening where appropriate
3. Return to the Scan page to confirm improvements

Common Issues

Scan Does Not Start

- Ensure you are on the **Scan** page (not just the dashboard)
- Refresh the page
- Check for plugin or JavaScript conflicts

No Findings Detected

This is normal.

- Your site may already be well-configured

- No obvious risks were found

Unexpected Results

- Review the explanation provided with each finding
- Some findings may reflect intentional configurations
- Only apply changes you understand

Tips for Best Results

- Run scans after updates, migrations, or restores
- Re-scan after applying hardening
- Use scans as a regular audit tool

What to Do Next

After your first scan:

1. Review the Dashboard overview
2. Understand your Scan Risk Score
3. Begin applying hardening controls

Related

- Understanding the Dashboard
- Scan Risk Score Explained
- Applying Hardening Safely

Dashboard Essentials

Dashboard Essentials

Understanding the Dashboard

What This Covers

This guide explains the Steel Security dashboard and how to interpret the information it provides.

The dashboard gives you a high-level view of your site's security posture and helps you prioritize next steps.

What the Dashboard Shows

The dashboard provides a summary of your site’s current security state.

It is designed to answer three key questions:

- What risks exist on this site?
- How severe are those risks?
- What should I do next?

Key Sections

Scan Summary

The Scan Summary reflects the results of your most recent scan.

It includes:

- total findings detected
- breakdown by severity (if applicable)
- overall **Scan Risk Score**

This gives you a quick understanding of your current risk level.

Scan Risk Score

The Scan Risk Score represents the overall risk level of your site based on detected findings.

- Higher scores indicate greater risk
- Lower scores indicate a more secure configuration

The score is intended as a **guideline**, not a perfect measurement.

Focus on the underlying findings rather than the number alone.

Recent Findings

This section highlights the most relevant issues detected during the last scan.

Each finding includes:

- a description of the issue
- why it matters
- recommended next steps

Use this section to quickly identify what needs attention.

Hardening Overview

The dashboard also summarizes available hardening opportunities.

This may include:

- protections that can be applied
- current hardening status
- areas where improvements can be made

Hardening actions are optional and should be applied thoughtfully.

How to Use the Dashboard

A typical workflow:

1. Review your Scan Risk Score

2. Identify high-risk findings
3. Open the Scan page for detailed results
4. Apply hardening where appropriate
5. Re-scan to confirm improvements

The dashboard helps you decide where to focus, not perform the work itself.

What the Dashboard Does Not Do

The dashboard does not:

- run scans automatically
- make changes to your site
- apply hardening actions

It is a **summary and navigation layer**, not an action layer.

When to Check the Dashboard

Use the dashboard:

- after running a scan
- after applying hardening
- after updates, migrations, or restores
- as part of routine maintenance

Common Questions

Why does the dashboard not update automatically?

The dashboard reflects the most recent scan results.

To refresh the data, return to the **Scan** page to trigger a new scan.

What should I focus on first?

Start with:

- high-risk findings
- exposed files
- configuration issues

These typically represent the most immediate concerns.

Is a low score “secure”?

A low score indicates fewer detected risks, but no system is ever completely risk-free.

Use the score as a guide, not a guarantee.

Tips

- Use the dashboard to prioritize, not diagnose
- Always review the full Scan results before making changes
- Apply hardening incrementally and verify results

What to Do Next

After reviewing the dashboard:

1. Open the Scan page for detailed findings
2. Review individual issues
3. Begin applying hardening controls

Related

- Running Your First Scan
- Scan Risk Score Explained
- Applying Hardening Safely

Reviewing Findings

What This Covers

This guide explains how to review and interpret the findings from a Steel Security scan.

Understanding your findings is the key step before applying any hardening changes.

Where to View Findings

Findings are available on the **Scan** page.

To access them:

1. Navigate to **Steel Security → Scan**
2. A scan will run automatically
3. Review the list of findings once the scan completes

Each finding represents a potential security risk or configuration issue.

What a Finding Represents

A finding indicates something on your site that may:

- expose sensitive information
- weaken security
- reflect an unsafe or outdated configuration
- indicate leftover or unnecessary files

Not all findings require immediate action, but all should be understood.

Information Provided for Each Finding

Each finding includes:

- **What was detected**
- **Why it matters**
- **Recommended next steps**

This context is designed to help you make informed decisions, not just react to alerts.

How to Prioritize Findings

Start by focusing on:

High-Risk Findings

These typically include:

- exposed backup or database files
- configuration leaks
- publicly accessible sensitive data

These should be addressed as soon as possible.

Configuration Issues

Examples include:

- debug mode enabled
- unnecessary exposure of system information

These may not be immediately critical but should be corrected.

Informational Findings

Some findings may be:

- informational
- intentional based on your setup

Review these carefully before taking action.

When to Take Action

You should consider taking action when:

- the finding exposes sensitive data
- the risk is publicly accessible
- the issue is not required for your workflow

If a finding is intentional, you may choose to leave it as-is.

Applying Fixes

Some findings can be addressed using Steel Security hardening features.

Others may require:

- manual file removal
- configuration updates
- hosting-level changes

Always review the recommendation before applying changes.

Safe Approach to Fixing Issues

Follow this workflow:

1. Review the finding and understand the risk
2. Confirm whether the issue is intentional
3. Apply the recommended fix or hardening
4. Re-run the scan to verify resolution

Avoid applying multiple changes at once without verification.

What Not to Do

- Do not blindly apply all fixes

- Do not remove files without understanding their purpose
- Do not assume all findings are critical

Steel Security is designed to inform, not automate decisions.

Common Questions

Why am I seeing findings on a new site?

Many WordPress installations include:

- default files
- leftover artifacts
- development configurations

These are common and should be reviewed and cleaned up.

Can I ignore a finding?

Yes, if:

- the behavior is intentional
- the risk is understood and accepted

However, you should document or remember why it was ignored.

Why does a finding still appear after fixing it?

- Ensure the change was applied correctly
- Return to the **Scan** page to trigger a new scan
- Confirm the issue is fully resolved

Tips

- Focus on quality, not quantity of fixes
- Address high-risk issues first
- Make changes incrementally

- Re-scan after each set of changes

What to Do Next

After reviewing your findings:

1. Identify the most important issues
2. Begin applying hardening controls
3. Re-scan to confirm improvements

Related

- Running Your First Scan
- Understanding the Dashboard
- Applying Hardening Safely
- Hardening Reference

Basic Hardening Workflow

Basic Hardening Workflow

Applying Hardening Safely

What This Covers

This guide explains how to review and interpret the findings from a Steel Security scan.

Understanding your findings is the key step before applying any hardening changes.

Where to View Findings

Findings are available on the **Scan** page.

To access them:

1. Navigate to **Steel Security → Scan**
2. A scan will run automatically
3. Review the list of findings once the scan completes

Each finding represents a potential security risk or configuration issue.

What a Finding Represents

A finding indicates something on your site that may:

- expose sensitive information
- weaken security
- reflect an unsafe or outdated configuration
- indicate leftover or unnecessary files

Not all findings require immediate action, but all should be understood.

Information Provided for Each Finding

Each finding includes:

- **What was detected**
- **Why it matters**
- **Recommended next steps**

This context is designed to help you make informed decisions, not just react to alerts.

How to Prioritize Findings

Start by focusing on:

High-Risk Findings

These typically include:

- exposed backup or database files
- configuration leaks
- publicly accessible sensitive data

These should be addressed as soon as possible.

Configuration Issues

Examples include:

- debug mode enabled
- unnecessary exposure of system information

These may not be immediately critical but should be corrected.

Informational Findings

Some findings may be:

- informational
- intentional based on your setup

Review these carefully before taking action.

When to Take Action

You should consider taking action when:

- the finding exposes sensitive data
- the risk is publicly accessible
- the issue is not required for your workflow

If a finding is intentional, you may choose to leave it as-is.

Applying Fixes

Some findings can be addressed using Steel Security hardening features.

Others may require:

- manual file removal
- configuration updates
- hosting-level changes

Always review the recommendation before applying changes.

Safe Approach to Fixing Issues

Follow this workflow:

1. Review the finding and understand the risk
2. Confirm whether the issue is intentional
3. Apply the recommended fix or hardening
4. Re-run the scan to verify resolution

Avoid applying multiple changes at once without verification.

What Not to Do

- Do not blindly apply all fixes

- Do not remove files without understanding their purpose
- Do not assume all findings are critical

Steel Security is designed to inform, not automate decisions.

Common Questions

Why am I seeing findings on a new site?

Many WordPress installations include:

- default files
- leftover artifacts
- development configurations

These are common and should be reviewed and cleaned up.

Can I ignore a finding?

Yes, if:

- the behavior is intentional
- the risk is understood and accepted

However, you should document or remember why it was ignored.

Why does a finding still appear after fixing it?

- Ensure the change was applied correctly
- Return to the **Scan** page to trigger a new scan
- Confirm the issue is fully resolved

Tips

- Focus on quality, not quantity of fixes
- Address high-risk issues first
- Make changes incrementally

- Re-scan after each set of changes

What to Do Next

After reviewing your findings:

1. Identify the most important issues
2. Begin applying hardening controls
3. Re-scan to confirm improvements

Related

- Running Your First Scan
- Understanding the Dashboard
- Applying Hardening Safely
- Hardening Reference