Plugin Guide

Understand how Steel Security works and how to use its features effectively.

Dashboard

Dashboard

Dashboard Overview

What This Covers

This page provides a detailed overview of the Steel Security dashboard and its components.

The dashboard acts as a central summary of your site's security posture and provides quick access to key areas of the plugin.

Dashboard Purpose

The dashboard is designed to:

- summarize scan results
- highlight areas of concern
- provide quick navigation to actions
- give a high-level view of your security posture

It is not intended to perform actions directly, but to guide your next steps.

Scan Summary

The Scan Summary provides a snapshot of your most recent scan.

It typically includes:

- number of findings
- severity distribution (if applicable)
- overall **Scan Risk Score**

This section helps you quickly assess the current state of your site.

Scan Risk Score

The Scan Risk Score reflects the overall risk level based on detected findings.

- Higher scores indicate greater risk
- Lower scores indicate fewer or less severe issues

The score is best used as a **trend indicator**, not a definitive measure.

Hardening Overview

The Hardening section provides visibility into available and applied protections.

This may include:

- active hardening controls
- available improvements
- overall hardening posture

This section helps identify opportunities to reduce risk.

Navigation and Actions

The dashboard provides quick access to key areas:

- **Open Scan** — view detailed findings and trigger a scan
- **Hardening sections** — apply or review protections
- Additional plugin features depending on configuration

The dashboard is intended as a starting point, not the place where changes are made.

Data Freshness

The dashboard reflects the results of the most recent scan.

To update the data:

1. Navigate to **Steel Security → Scan**
2. A new scan will run automatically
3. Return to the dashboard to view updated results

Using the Dashboard Effectively

A typical workflow:

1. Review the Scan Risk Score
2. Identify areas of concern
3. Open the Scan page for detailed findings
4. Apply hardening as needed
5. Re-scan and return to the dashboard

Limitations

The dashboard does not:

- run scans automatically
- apply changes
- provide full detail for each finding

Use it as a summary and navigation tool.

Tips

- Use the dashboard for quick assessment
- Always review detailed findings before acting
- Revisit after changes to confirm improvements

Related

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

Scan

Scan

Scan Risk Score Explained

What This Covers

This guide explains how the Scan Risk Score is calculated and how to interpret it.

The Scan Risk Score provides a quick summary of your site's overall risk level based on detected findings.

What the Scan Risk Score Represents

The Scan Risk Score is an aggregated measure of risk based on the findings from your most recent scan.

It reflects:

- the presence of security issues
- the severity of those issues
- the potential exposure of sensitive data

The score is intended to give you a **high-level view**, not a complete assessment.

How to Interpret the Score

In general:

- A **higher score** indicates greater risk
- A **lower score** indicates fewer or less severe issues

However, the score should always be interpreted alongside the actual findings.

What Influences the Score

The Scan Risk Score is affected by:

- severity of findings
- number of findings
- type of exposure (e.g. public access vs internal configuration)

High-impact issues contribute more heavily than minor or informational findings.

Why the Score Is Not Everything

The Scan Risk Score is a guide, not a guarantee.

For example:

- A single high-risk issue may be more important than multiple minor ones
- Some findings may be intentional based on your setup
- Not all risks are equal in real-world impact

Always review individual findings before taking action.

How to Use the Score Effectively

Use the Scan Risk Score to:

- quickly assess overall risk
- track improvements over time
- identify when attention is needed

Do not use it as the sole basis for decisions.

Improving Your Score

To improve your Scan Risk Score:

1. Address high-risk findings first
2. Apply relevant hardening controls
3. Remove unnecessary or exposed files
4. Re-run the scan to confirm improvements

Changes to your configuration will be reflected in the score after the next scan.

When the Score Does Not Change

If your score remains the same after making changes:

- confirm the issue was fully resolved
- return to the Scan page to trigger a new scan
- review whether the finding still applies

Common Questions

Is a low score “secure”?

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

Use the score as a guideline, not a guarantee.

Why is my score high?

Common reasons include:

- exposed backup or database files
- debug settings enabled
- publicly accessible sensitive information

These should be reviewed and addressed where appropriate.

Can I ignore the score?

You should not ignore the score entirely, but you should prioritize **understanding findings** over chasing a number.

Tips

- Focus on high-impact issues first
- Use the score to track progress, not define success
- Re-scan regularly after making changes

What to Do Next

After reviewing your Scan Risk Score:

1. Open the Scan page
2. Review individual findings
3. Apply hardening where appropriate

Related

- Reviewing Findings
- Applying Hardening Safely
- Understanding the Dashboard

Working with Scan Findings

What This Covers

This guide explains how to work with scan findings within Steel Security.

It focuses on how to interpret, navigate, and act on findings efficiently as part of your workflow.

Where Findings Are Managed

Scan findings are managed on the **Scan** page.

To access them:

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

This is the primary location for reviewing and acting on detected issues.

Understanding the Findings List

The Scan page presents findings as a structured list.

Each entry represents a specific issue and includes:

- a description of the problem
- context explaining the risk
- recommended next steps

Findings are designed to be **actionable and easy to interpret**.

Working Through Findings Efficiently

A typical workflow:

1. Start with the highest-risk findings
2. Open each finding to review details
3. Determine whether action is required
4. Apply a fix or hardening control if appropriate
5. Re-scan to confirm resolution

Work through findings methodically rather than all at once.

Prioritization Strategy

When reviewing findings, prioritize:

High-Risk Issues

- exposed sensitive files
- publicly accessible data
- configuration leaks

These should be addressed first.

Moderate Issues

- debug settings
- unnecessary exposure
- non-critical misconfigurations

These should be reviewed and corrected where appropriate.

Informational Findings

- expected or intentional configurations

These may not require action but should still be understood.

Taking Action on Findings

Depending on the finding, actions may include:

- applying a hardening control
- removing or securing a file
- updating configuration settings
- making server-level changes

Always review the recommendation before taking action.

Using Hardening with Findings

Some findings can be resolved directly through Steel Security hardening features.

When available:

- review the hardening option
- confirm it is appropriate for your site
- apply the change
- re-scan to verify

Hardening provides a safe and structured way to address common issues.

Handling Intentional Findings

Not all findings indicate problems that need to be fixed.

You may choose to leave a finding unresolved if:

- it is required for your workflow
- the risk is understood and accepted
- the exposure is controlled

Be intentional with these decisions.

Re-Scanning After Changes

After addressing findings:

1. Reload the **Scan** page

2. A new scan will run automatically
3. Confirm that the issue no longer appears

This step is important to validate that changes were successful.

Avoiding Common Mistakes

- Do not apply fixes without understanding them
- Do not attempt to resolve everything at once
- Do not remove files without verifying their purpose

Work incrementally and verify each step.

When a Finding Persists

If a finding remains after applying a fix:

- confirm the change was applied correctly
- check for caching or server-level behavior
- verify the issue has been fully resolved

Some issues may require manual intervention beyond the plugin.

Tips

- Focus on high-impact issues first
- Work in small, controlled steps
- Re-scan frequently
- Use findings as an ongoing audit tool

What to Do Next

After working through your findings:

1. Apply additional hardening where appropriate
2. Monitor your Scan Risk Score

3. Continue periodic scans to maintain security

Related

- Reviewing Findings
- Applying Hardening Safely
- Scan Risk Score Explained
- Hardening Reference

Hardening

Hardening

Hardening Posture Score Explained

What This Covers

This guide explains the Hardening Posture Score and how to interpret it.

The Hardening Posture Score reflects the level of protective measures applied to your site through Steel Security.

What the Hardening Posture Score Represents

The Hardening Posture Score measures how well your site is protected based on applied hardening controls.

It reflects:

- active protections
- coverage of available hardening options
- overall defensive posture

Unlike the Scan Risk Score, which identifies issues, this score represents **what has been secured**.

How to Interpret the Score

In general:

- A **higher score** indicates more protections are in place
- A **lower score** indicates opportunities to improve security

The score helps you understand how much of your site’s potential hardening has been applied.

What Influences the Score

The Hardening Posture Score is affected by:

- number of applied hardening controls
- importance of each control
- coverage across different security areas

Some protections contribute more than others based on their impact.

Scan vs Hardening: Key Difference

Steel Security separates **risk detection** from **risk reduction**.

- **Scan Risk Score** → What risks exist
- **Hardening Posture Score** → What protections are in place

Improving your security posture requires addressing both.

Why the Score Is Not Everything

The Hardening Posture Score is a guide, not a target.

For example:

- Not all hardening controls are appropriate for every site
- Some protections may conflict with functionality
- A “perfect” score is not always desirable

Focus on applying **relevant and safe protections**, not maximizing the score.

How to Improve Your Score

To improve your Hardening Posture Score:

1. Review available hardening controls

2. Apply relevant protections
3. Test your site after each change
4. Re-run scans to confirm impact

Improvements will be reflected after changes are applied.

When Not to Apply a Control

You may choose not to apply a control if:

- it conflicts with your site’s functionality
- it is not relevant to your environment
- the risk is already mitigated in another way

Steel Security is designed to support informed decisions, not enforce changes.

When the Score Does Not Change

If your score does not increase:

- confirm the control was applied successfully
- ensure the change is supported by your server
- review whether the control contributes to the score

Common Questions

Should I aim for a perfect score?

Not necessarily.

A high score is beneficial, but only when the applied protections are appropriate for your site.

Why is my score low?

Common reasons include:

- no hardening controls applied
- limited server capabilities
- skipped or unsupported protections

Can I ignore the score?

You should use it as a guide, but not as the sole measure of security.

Understanding your environment is more important than achieving a number.

Tips

- Apply protections gradually
- Prioritize high-impact controls
- Test after each change
- Use the score to track progress over time

What to Do Next

After reviewing your Hardening Posture Score:

1. Review available hardening controls
2. Apply relevant protections
3. Re-test your site
4. Continue improving your security posture

Related

- Scan Risk Score Explained
- Applying Hardening Safely
- Hardening Reference

Quarantine

Quarantine

How Quarantine Works

What This Covers

This guide explains how the Steel Security quarantine system works and how it helps safely isolate potentially risky files.

Quarantine provides a controlled way to remove files from active use without permanently deleting them.

What Quarantine Does

Quarantine moves a file out of its original location into a secure, non-public storage area.

This means:

- the file is no longer accessible via the web
- it cannot be executed or loaded by WordPress
- it is preserved for review or restoration

This allows you to safely handle suspicious or unnecessary files.

When Quarantine Is Used

Quarantine is typically used when:

- a scan identifies a potentially sensitive or risky file
- you want to remove a file without deleting it permanently
- you are unsure whether a file is safe to remove

It provides a safe alternative to immediate deletion.

How the Process Works

When a file is quarantined:

1. The file is moved from its original location
2. It is stored in a protected directory within your site
3. Access to the file is restricted
4. A record is kept to allow restoration

The original file path is preserved for reference.

What Happens After Quarantine

After a file is quarantined:

- it will no longer appear in scans as an exposed file
- any functionality depending on that file may change
- the file remains available for restoration

You should verify your site after quarantining any file.

Safety Considerations

Quarantine is designed to be safe, but you should still:

- understand what the file does before quarantining
- avoid quarantining core or required files
- test your site after making changes

When in doubt, proceed cautiously.

Where Quarantined Files Are Stored

Quarantined files are stored in a protected location within your WordPress environment.

This location:

- is not publicly accessible
- prevents direct execution of files
- is managed by Steel Security

This ensures quarantined files cannot pose a risk while stored.

Quarantine vs Deletion

Quarantine is not the same as deletion.

Quarantine	Deletion
Reversible	Permanent
Safe for testing	No recovery
Preserves file	Removes file entirely

Quarantine is recommended when you are unsure about a file.

Limitations

- Quarantine does not analyze file contents for malware
- Some files may be required for site functionality
- Manual review may still be necessary

Steel Security focuses on safe handling, not automatic classification.

Common Questions

Will quarantining a file break my site?

It can, if the file is required.

Always test your site after quarantining any file.

Can I view quarantined files?

Yes, files remain stored and can be restored if needed.

Are quarantined files secure?

Yes.

They are stored in a protected location and are not accessible via the web.

Tips

- Use quarantine when you are unsure about a file
- Avoid deleting files immediately
- Always test after quarantining
- Review findings before taking action

What to Do Next

After quarantining a file:

1. Test your site functionality
2. Confirm no issues are introduced
3. Decide whether to keep the file quarantined or restore it

Related

- Restoring Quarantined Files
- Working with Scan Findings
- Safe Rollback Practices

Restoring Quarantined Files

What This Covers

This guide explains how to restore files that have been placed in quarantine.

Restoring allows you to return a file to its original location if it is needed for your site to function correctly.

When to Restore a File

You may need to restore a file if:

- your site functionality is affected after quarantining
- a plugin or theme stops working
- you determine the file is safe and required

Restoration returns the file to its original state and location.

How Restoration Works

When a file is restored:

- it is moved back to its original path
- its original filename is preserved
- it becomes active again within your site

This effectively reverses the quarantine action.

How to Restore a File

1. Navigate to the Steel Security quarantine section
2. Locate the file you want to restore

3. Select the restore option
4. Confirm the action

The file will be returned to its original location immediately.

What to Expect After Restoring

After restoring a file:

- any related functionality should return
- the file may reappear in scan results if it still represents a risk
- your Scan Risk Score may change

This is expected and reflects the current state of your site.

Verifying a Restoration

After restoring a file:

1. Test the affected part of your site
2. Confirm functionality is working as expected
3. Return to the Scan page and re-run a scan

This ensures both functionality and security are understood.

When Not to Restore

Do not restore a file if:

- it is clearly unnecessary or outdated
- it exposes sensitive data
- it was intentionally removed for security reasons

Only restore files you understand and trust.

Common Issues

File Restored but Issue Persists

- confirm the correct file was restored
- check for caching or server-level delays
- verify no additional files were affected

File Reappears in Scan Results

This is expected.

The underlying issue has not changed, only the file’s location.

You may need to:

- remove the file permanently
- secure it properly
- accept the risk if intentional

Restoration Fails

- check file permissions
- ensure the original path still exists
- verify hosting restrictions are not blocking the action

Tips

- Restore one file at a time
- Test immediately after restoring
- Avoid repeated quarantine/restore cycles without understanding the issue

---

What to Do Next

After restoring a file:

1. Review why the file was flagged
2. Decide whether to secure or remove it permanently
3. Continue monitoring your scan results

Related

- How Quarantine Works
- Safe Rollback Practices
- Working with Scan Findings

Configuration

Configuration

Configuration and Defaults

What This Covers

This page explains how Steel Security handles configuration and why it does not include traditional plugin settings.

Steel Security is designed to minimize configuration and provide safe, effective defaults out of the box.

No Settings by Design

Steel Security does not include a traditional settings panel.

This is intentional.

The plugin is designed to:

- reduce complexity
- avoid misconfiguration
- provide consistent, reliable behavior

Most functionality is controlled through actions, not settings.

How Steel Security Is Configured

Instead of settings, Steel Security operates through:

- scan results
- hardening controls
- quarantine actions

This means:

- you act based on findings
- you apply protections intentionally

- you make decisions with context

Why There Are No Settings

Traditional settings often:

- introduce unnecessary complexity
- allow unsafe configurations
- create inconsistent behavior across environments

Steel Security avoids this by using:

- sensible defaults
- controlled actions
- environment-aware behavior

What You Can Control

While there are no global settings, you still have full control over:

- which hardening controls are applied
- which files are quarantined or restored
- how findings are handled

This keeps control focused on **decisions that matter**.

Benefits of This Approach

- fewer configuration mistakes
- faster onboarding
- consistent behavior across sites
- reduced need for ongoing management

This approach is especially beneficial for:

- agencies managing multiple sites
- developers working across environments
- users who prefer simplicity

When Configuration May Still Be Needed

Some actions may still involve environment-specific decisions, such as:

- server-level configurations
- file permissions
- hosting restrictions

These are handled outside of Steel Security where appropriate.

Common Questions

Why can’t I customize scan behavior?

Steel Security focuses on high-signal checks that are relevant across most environments.

Reducing configurability helps ensure consistent and meaningful results.

Will settings be added in the future?

Steel Security prioritizes clarity and safety over configurability.

New options will only be introduced where they provide clear value without increasing complexity.

How do I change how Steel Security behaves?

Behavior is controlled through:

- applying or reverting hardening
- managing quarantined files
- responding to scan findings

Tips

- Trust the default behavior
- Focus on findings and actions rather than configuration
- Avoid overcomplicating your security workflow

What to Do Next

Now that you understand how Steel Security is configured:

1. Run a scan
2. Review findings
3. Apply hardening as needed

Related

- Working with Scan Findings
- Applying Hardening Safely
- Safe Rollback Practices

Safe Rollback Practices

What This Covers

This guide explains how to safely manage and reverse changes made through Steel Security.

Rollback is a critical part of using hardening features responsibly and ensures you can recover quickly if something does not behave as expected.

Why Rollback Matters

Security changes can affect how your site behaves.

Even well-designed protections may:

- interfere with specific plugins or themes
- impact custom configurations
- behave differently across hosting environments

Rollback ensures that any change can be safely reversed if needed.

How Steel Security Supports Rollback

Steel Security is designed to apply hardening in a **controlled and reversible way** wherever possible.

This means:

- changes are applied intentionally
- original states are preserved where applicable
- controls can be disabled or reverted

This approach allows you to experiment safely without risking long-term issues.

When to Use Rollback

You should consider rolling back a change if:

- your site functionality breaks
- a feature stops working as expected
- you observe unexpected behavior after applying hardening

Always investigate the most recent change first.

Safe Rollback Workflow

Follow this process to safely revert changes:

1. Identify the most recent hardening control applied
2. Navigate to the relevant hardening section
3. Disable or revert the control
4. Test your site functionality
5. Confirm the issue is resolved

Work one change at a time to isolate the cause.

Verifying a Rollback

After reverting a change:

- test key areas of your site
- confirm expected behavior is restored
- return to the Scan page to validate results

This ensures both functionality and security are understood.

Rollback vs Manual Changes

Some findings may require manual fixes outside of Steel Security.

In these cases:

- Steel Security cannot automatically revert changes
- you will need to restore files or configurations manually

Always keep backups when making manual changes.

Limitations

Rollback is designed to be safe and predictable, but:

- not all changes can be automatically reversed
- server-level configurations may behave differently
- hosting restrictions may limit reversibility

Steel Security will only offer rollback where it is safe to do so.

Best Practices

- Apply one change at a time
- Test immediately after each change
- Keep a recent backup of your site
- Use a staging environment when possible
- Document changes if managing multiple sites

Common Questions

What if I’m not sure what caused the issue?

- Revert the most recent change first
- Test after each rollback
- Continue step-by-step until the issue is resolved

Can I undo all changes at once?

It is not recommended.

Reverting changes individually helps identify the cause and prevents unnecessary rollback of safe improvements.

Does rollback affect my scan results?

Yes.

Reverting a change may cause a finding to reappear in the next scan.

This is expected and reflects the current state of your site.

Tips

- Think of hardening as reversible improvements, not permanent changes
- Use rollback as a safety net, not a fallback for careless changes
- Prioritize understanding before applying controls

What to Do Next

After confirming a rollback:

1. Review the related finding again
2. Determine if an alternative solution is needed
3. Continue applying safe, appropriate hardening

Related

- Applying Hardening Safely
- Working with Scan Findings
- Hardening Reference